Verena Schochlow, Stephan Neumann, Kristoffer Braun, Melanie Volkamer

Bewertung der GMX/Mailvelope-Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-verschlüsselte E-Mail-Kommunikation hat seit den Veröffentlichungen von Edward Snowden erneut an Bedeutung gewonnen. Obwohl die entsprechenden Möglichkeiten seit mehr als zwei Jahrzehnten gegeben sind, sind die technischen Umsetzungen für Endanwender häufig schwer zugänglich. Ein wesentlicher Grund dafür ist, wie Studien belegen, deren Nutzerschnittstelle. Mit Mailvelope versuchen die Anbieter GMX und WEB.DE derzeit, Ende-zu-Ende-verschlüsselte E-Mail-Kommunikation in ihren gewohnten Benutzerschnittstellen zu integrieren. Zur Bewertung dieses Ansatzes wurden ein *Cognitive Walkthrough* durchgeführt und die Sicherheit des Ansatzes bewertet.

Verena Schochlow

ist Wissenschaftliche Mitarbeiterin bei der Forschungsgruppe Arbeits- und Ingenieurpsychologie (FAI) der TU Darmstadt

E-Mail: schochlow@psychologie.tu-darmstadt.de

Stephan Neumann

ist Wissenschaftlicher Mitarbeiter an der Technischen Universität Darmstadt. Er forscht in der Arbeitsgruppe Security, Usability, and Society (SECUSO) an dem Thema sichere Internetwahlen und sichere E-Mail-Kommunikation.

E-Mail: stephan.neumann@secuso.org

Kristoffer Braun

ist Studentische Hilfskraft an der Technischen Universität Darmstadt. Er forscht in der Arbeitsgruppe Security, Usability, and Society (SECUSO). Hier schreibt er auch seine Masterarbeit.

E-Mail: kristoffer.braun@secuso.org

Melanie Volkamer

ist Professorin für Usable Privacy and Security an der Universität Karlstad (Schweden) und Juniorprofessorin an der Technischen Universität Darmstadt. Sie leitet dort die Arbeitsgruppe Security, Usability, and Society (SECUSO).

E-Mail: melanie.volkamer@secuso.org

1 Einleitung

Eine der bedeutendsten digitalen Kommunikationskanäle stellt die E-Mail dar; über 80% der Deutschen nutzen das Internet zum Versenden und Empfangen von E-Mails, Tendenz steigend.[1] Nicht zuletzt die Snowden-Enthüllungen haben der Allgemeinheit die technischen Möglichkeiten zur digitalen Massenüberwachung aufgezeigt und zahlreiche Fragen zur Sicherheit und Privatsphäre digitaler Kommunikation aufgeworfen. Ziel kryptographischer Ansätze ist die E-Mail-Kommunikation ausschließlich zwischen Sender und Empfänger offenzulegen, also auch E-Mail-Anbietern den Zugriff auf E-Mail-Inhalte unmöglich zu machen.

Obwohl technische Lösungen bzw. Standards existieren (z. B. S/MIME, OpenPGP), die eine solche Ende-zu-Ende-Verschlüsselung (E2E) der E-Mail-Kommunikation ermöglichen, sind diese Endanwendern häufig nicht zugänglich, wie zahlreiche Studien belegen [1, 2]. In den letzten Jahren wurden eine Reihe von Browsererweiterungen zur E2E-verschlüsselten E-Mail-Kommunikation im Browser entwickelt, z. B. WebPG, mymail-crypt und Mailvelope, die eine nutzerfreundliche E2E-Verschlüsselung für zahlreiche webbasierte E-Mail-Dienste versprechen.[2] Erste Studien belegen jedoch, dass auch derartige Browsererweiterungen die Benutzbarkeitsprobleme früherer technischer Lösungen nicht ausreichend adressieren [3, 4].

Ein weiterer Vorstoß in Richtung benutzbarer E2E-verschlüsselter E-Mail-Kommunikation wird derzeit von Mailvelope in direkter Kooperation[3] mit GMX und WEB.DE (beides Marken der 1&1

1 http://de.statista.com/statistik/daten/studie/204272/umfrage/nutzung-des-internets-fuer-versenden-empfangen-von-e-mails-in-deutschland/ (abgerufen am 29.03.2016)

2 https://www.mailvelope.com/de/help (abgerufen am 29.03.2016)

3 https://www.mailvelope.com/de/coop_gmx (abgerufen am 29.03.2016)

Mail & Media GmbH und beide Partner der Initiative „E-Mail made in Germany") unternommen. So wird insbesondere der aus Nutzersicht kritische Schlüsselaustausch und die Sicherung der Schlüsseldaten über die Integration von Mailvelope in die bestehende Infrastruktur der E-Mail-Anbieter vereinfacht. Dieser Schritt der E-Mail-Anbieter könnte zukünftig Nutzern den Weg zur E2E-Verschlüsselung ihrer E-Mail-Kommunikation erleichtern.

Dieser Beitrag bewertet die Integration der Browsererweiterung Mailvelope in die bestehende Infrastruktur des E-Mail-Anbieters GMX aus Sicht der „benutzbaren Sicherheit" und beschränkt sich daher auf den GMX-Webdienst; dedizierte E-Mail-Clients (z.B. Microsoft Outlook, Mozilla Thunderbird) werden nicht betrachtet.

Zunächst werden die Grundlagen der Integration von Mailvelope in GMX vorgestellt; dabei wird die GMX-Terminologie verwendet. Anschließend werden die Ergebnisse eines *Cognitive Walkthrough* (CW) präsentiert und diskutiert. Im Rahmen des CW wurde die Benutzbarkeit folgender relevanter Nutzeraufgaben evaluiert: Einrichtung der verschlüsselten Kommunikation[4], Senden verschlüsselter E-Mails und Entschlüsseln verschlüsselter E-Mails. Zuletzt werden die wesentlichen Sicherheitsaspekte der Integration von Mailvelope in die Infrastruktur des E-Mail-Anbieters GMX beleuchtet.

2 Grundlagen der Integration von Mailvelope in GMX

Im Folgenden werden die Grundlagen der E2E-verschlüsselten E-Mail-Kommunikation anhand der drei wesentlichen Funktionen beschrieben: (1) Einrichtung der verschlüsselten Kommunikation, (2) Senden einer verschlüsselten E-Mail und (3) Entschlüsselung einer verschlüsselten E-Mail.

2.1. Einrichtung der verschlüsselten Kommunikation

Die verschlüsselte E-Mail-Kommunikation bei GMX basiert auf einer E2E-Verschlüsselung mit dem Verschlüsselungsstandard OpenPGP. Dieser verwendet ein hybrides, also eine Kombination aus einem asymmetrischen und einem symmetrischen, Verschlüsselungssystem. Ein Absender erzeugt für jede Nachricht einen symmetrischen Sitzungsschlüssel, welcher mit dem öffentlichen Schlüssel des Empfängers verschlüsselt wird. Die Nachricht wird anschließend mit dem Sitzungsschlüssel verschlüsselt und abgeschickt. Der Empfänger entschlüsselt den Sitzungsschlüssel mit seinem privaten Schlüssel und anschließend die Nachricht mit dem entschlüsselten Sitzungsschlüssel.

Um die verschlüsselte E-Mail-Kommunikation einzurichten, müssen drei Schritte befolgt werden. Als Erstes ist es notwendig, dass der Nutzer die Browsererweiterung Mailvelope installiert. Dabei handelt es sich um ein Open Source Projekt, das unter anderem auf dem OpenPGP.js-Projekt basiert, einer Open Source JavaScript-Implementierung des OpenPGP-Standards.

Bei der Einrichtung der verschlüsselten Kommunikation wird der Nutzer im zweiten Schritt dazu aufgefordert, ein so genanntes Schlüsselpasswort[5] mit mindestens vier Zeichen zu vergeben, welches seinen privaten Schlüssel schützen soll. Nach der Eingabe erzeugt Mailvelope lokal auf dem Computer des Nutzers je einen 4096 Bit langen privaten und öffentlichen RSA-Schlüssel, die sowohl zum Ver-/Entschlüsseln und Signieren/Verifizieren von E-Mails verwendet werden.[6] Beide Schlüssel werden anschließend lokal (auf dem Rechner des Nutzers) in der Schlüsselverwaltung von Mailvelope gespeichert; dabei wird der private Schlüssel mit dem Schlüsselpasswort des Nutzers verschlüsselt. Jeder Eintrag enthält Details zu den eigenen und den gespeicherten öffentlichen Schlüsseln Dritter, beispielsweise den Fingerabdruck und das Erstellungsdatum.

Im dritten und letzten Schritt der Einrichtung kann der Nutzer eine so genannte Sicherung einrichten. Diese soll ermöglichen, dass er bei Verlust der Schlüssel eine Möglichkeit hat, diese und damit die verschlüsselte E-Mail-Kommunikation wiederherzustellen. Außerdem kann damit das Verfahren besonders einfach auf anderen Geräten wie beispielsweise Laptops oder Smartphones des Nutzers eingerichtet werden. Stimmt der Nutzer der Sicherung zu, werden sein Schlüsselpasswort und sein Schlüsselpaar, bestehend aus dem privaten und öffentlichen Schlüssel, in einem Paket mit AES-256 und einem zufälligen AES-Schlüssel verschlüsselt, und auf die Server von GMX hochgeladen.

Diese symmetrische Verschlüsselung geschieht lokal, auf dem Computer des Nutzers. Der private Schlüssel ist zu keinem Zeitpunkt unverschlüsselt auf den Servern von GMX. Anschließend erhält der Nutzer innerhalb von Mailvelope den AES-Schlüssel in Form eines 26-stelligen Wiederherstellungscodes, mit dem er bei Bedarf die verschlüsselte Kommunikation wiederherstellen kann. GMX empfiehlt diesen Code sicher und außerhalb des Computers aufzubewahren. Es ist nachträglich möglich weitere Sicherungen zu erstellen; dabei wird die vorherige Sicherung auf den Servern von GMX gelöscht und eine neue mit passendem Wiederherstellungscode hochgeladen. Ältere Codes werden dadurch ungültig. In den GMX-Einstellungen besteht die Möglichkeit, die Sicherung nachträglich von den GMX-Servern zu entfernen. Wenn sich der Nutzer entscheidet, keine Sicherung einzurichten und das Schlüsselpasswort verloren geht, können verschlüsselte E-Mails nicht mehr entschlüsselt werden. Die verschlüsselte Kommunikation muss erneut eingerichtet werden. Dazu muss sich der Nutzer an den GMX-Support wenden.

Nach der Einrichtung wird der öffentliche Schlüssel des Nutzers standardmäßig im Schlüssel-Verzeichnis von GMX abgelegt, aus dem die öffentlichen Schlüssel anderer Nutzer abgerufen werden können. Dort werden ebenso die in Kooperation von Mailvelope mit WEB.DE generierten öffentlichen Schlüssel abgelegt. Der Nutzer kann diese Speicherung in den Einstellungen von GMX widerrufen.

Die Dialoge sämtlicher Berechnungen, die lokal durchgeführt werden, sind mit einem besonderen Rahmen gekennzeichnet, dem sogenannten Sicherheitshintergrund. Der Sicherheitshintergrund erscheint beispielsweise beim Schreiben oder Entschlüsseln einer E-Mail. Um zu verhindern, dass er imitiert wird, kann er in den Einstellungen von Mailvelope angepasst werden.

2.2. Senden einer verschlüsselten E-Mail

Wenn der Nutzer nun mit einem anderen Nutzer von GMX oder WEB.DE, der auch die verschlüsselte Kommunikation einge-

4 GMX bezeichnet die E2E-verschlüsselte E-Mail-Kommunikation als verschlüsselte Kommunikation.

5 GMX bezeichnet die Passphrase als Schlüsselpasswort.

6 Dieser Artikel beschränkt sich auf die Betrachtung der E2E-Verschlüsselung. Signieren und Verifizieren von E-Mails wird daher nicht beleuchtet.

richtet hat, verschlüsselt kommunizieren möchte, dann erstellt er eine neue, E2E-verschlüsselte E-Mail und gibt die E-Mail-Adresse des Empfängers ein. Daraufhin öffnet sich bei der ersten E-Mail an diesen Empfänger ein neues Fenster mit der Anfrage, den Kontakt zur verschlüsselten Kommunikation zu bestätigen. Dabei werden dem Nutzer Name und E-Mail-Adresse des Kommunikationspartners als Entscheidungsgrundlage geboten. Durch Klicken eines kleinen „i"-Symbols kann der Nutzer darüber hinaus den Fingerabdruck des öffentlichen Schlüssels des intendierten Kommunikationspartners einsehen. Sobald der Nutzer dies bestätigt, wird der öffentliche Schlüssel des Empfängers aus dem Schlüssel-Verzeichnis geladen. Nach einem Klick auf „Verschlüsselt senden" wird der Absender aufgefordert sein Schlüsselpasswort[7] einzugeben. Daraufhin wird die E-Mail und, sofern vorhanden, der Anhang (bis 10 MB) mit Hilfe des öffentlichen Schlüssels des Empfängers verschlüsselt.

2.3. Entschlüsselung einer verschlüsselten E-Mail

Nach Erhalt einer E2E-verschlüsselten E-Mail wird der Nutzer aufgefordert sein Schlüsselpasswort einzugeben. Anschließend wird die verschlüsselte E-Mail mit Hilfe des privaten Schlüssels des Empfängers entschlüsselt und dadurch lesbar.

3 Benutzbarkeitsanalyse

Mit zunehmender Bedeutung der Benutzbarkeit wurden Methoden entwickelt, um diese zu prüfen und zu steigern. Neben Nutzerstudien, die zwar effektiv, aber auch zeit- und kostenintensiv sind, wurden Methoden konzipiert, die auf der Analyse der Benutzerschnittstellen durch Experten beruhen. Dazu zählt auch der *Cognitive Walkthrough* (CW), der häufig bei der Evaluation von Softwarelösungen und auch im Bereich der IT-Sicherheit zur Anwendung kommt [1, 5, 6].

3.1. Methode *Cognitive Walkthrough*

Beim CW steht die Erlernbarkeit bestimmter Aufgaben innerhalb einer Anwendung im Fokus [7, 8], was im IT-Sicherheits-Bereich von besonderer Bedeutung ist. So scheinen Nutzer zum einen Schwierigkeiten bei der korrekten Nutzung von Verschlüsselungssoftware zu haben [1]. Zum anderen ist Sicherheit neben dem Primärnutzen wie Surfen oder dem Versenden von E-Mails als sekundäres Nutzerziel mit einer verringerten Lernmotivation zu bewerten [1].

Der CW gliedert sich in eine Vorbereitungs- und eine Analysephase. In der Vorbereitungsphase werden Annahmen über den potenziellen Nutzer getroffen, die zu untersuchende Aufgabe festgelegt und die korrekte Handlungsabfolge zur Aufgabenbewältigung definiert. In der Analysephase wird die festgelegte Handlungsabfolge chronologisch durch Experten bearbeitet. Für jeden Schritt wird evaluiert, ob ein potenzieller Nutzer diesen Schritt in der geplanten Weise ausführen würde oder nicht.

Zur Bewertung können bestimmte Kriterien wie beispielsweise bei Wharton et al. [8] herangezogen werden. In beiden Fällen wird dokumentiert, warum der potenzielle Nutzer eine Aktion ausführen würde bzw. was zum Misserfolg geführt haben könnte. Unabhängig von der Bewertung der Handlung werden die festgelegten Handlungsschritte weiter bearbeitet, als ob der vorausgehende Schritt erfolgreich gewesen wäre. Auf diese Weise versuchen Experten in der Analysephase eine plausible Nutzungsgeschichte zu erzählen und den kognitiven Problemlöseprozess des potenziellen Nutzers zu modellieren.

3.2 Durchführung des *Cognitive Walkthrough*

Der CW umfasste die wesentlichen Schritte der E2E-verschlüsselten E-Mail-Kommunikation: (1) Einrichtung der verschlüsselten Kommunikation, (2) Senden einer verschlüsselten E-Mail, sowie (3) Entschlüsselung einer verschlüsselten E-Mail. Für diese wurden korrekte Handlungsabfolgen definiert. Hinsichtlich der Nutzer wurde von Laien ausgegangen, mit Vorkenntnissen im Bereich der E-Mail-Kommunikation mit GMX, aber mit fehlenden Sicherheitskenntnissen.

Durchgeführt wurde der CW von vier Personen mit Expertise in den Bereichen IT-Sicherheit, Benutzbarkeit und Psychologie, da sich gezeigt hat, dass Experten mit verschiedenen Perspektiven Probleme unterschiedlicher Art identifizieren [9]. Jeder Handlungsschritt wurde anhand der vier Kriterien nach Wharton et al. [8] mit dem Fokus auf der Menüführung bewertet. Aufgrund des Fokus dieses Artikels wurden zusätzlich folgende Kriterien berücksichtigt:

- **Information**: Erhält der Nutzer Informationen, die es ihm ermöglichen, ein Verständnis für die zugrundeliegende Technik der E2E-Verschlüsselung zu entwickeln? (Dieses Kriterium ist nicht erfüllt, wenn der Nutzer z. B. mit für ihn unverständlichen Fachbegriffen konfrontiert wird.)
- **Privatsphäre**: Wird die Privatsphäre des Nutzers gewahrt? (Dieses Kriterium ist nicht erfüllt, wenn der Nutzer z. B. unzureichende Informationen zum Umgang mit seinen Daten erhält oder dazu aufgefordert wird, für die Funktion nicht benötigte, persönliche Informationen preiszugeben.)
- **Sicherheit**: Ist die Handlung, die der Nutzer ausführt, sicher? (Dies ist nicht erfüllt, wenn der Nutzer z. B. unbeabsichtigt eine nicht E2E-verschlüsselte E-Mail senden kann.)

Durchgeführt wurde der CW im Webinterface von GMX innerhalb des Browsers Firefox-Version 44.0.2 und mit der Mailvelope-Version 1.3.6.

3.3. Ergebnisse und Diskussion

Im Folgenden werden die Ergebnisse in Bezug auf die Benutzbarkeit der Menüführung, die Information des Nutzers sowie sicherheitsrelevante Aspekte in zusammengefasster Form vorgestellt und diskutiert.

3.3.1 Einrichtung der verschlüsselten Kommunikation

Initiiert der Nutzer erstmalig die intendierte E2E-verschlüsselte E-Mail-Kommunikation, so wird er zunächst zum Einrichtungsprozess geleitet. Der einmalige Schritt der Einrichtung ist unter technischen Gesichtspunkten nachvollziehbar, könnte allerdings für den Laien unerwartet sein. Darüber hinaus könnte der zusätzliche Aufwand zum Erreichen des sekundären Nutzerziels Sicherheit ein Hindernis für potenzielle Nutzer mit dem Primärziel einfacher und schneller Kommunikation darstellen.

In Bezug auf die Menüführung des Einrichtungsprozesses wurde keine wesentliche Verletzung der Kriterien identifiziert. Meh-

7 Das Schlüsselpasswort kann 30 Minuten lang zwischengespeichert werden.

rere Wege führen zum Einrichtungsprozess, die Menüführung selbst ist geradlinig aufgebaut und bietet wenige Optionen und damit auch wenige Fehlerquellen für den Nutzer. Anleitungen, wenn auch nicht immer in ihrer Symbolik oder Begrifflichkeit konsistent gehalten, verdeutlichen den Prozess. Die Mehrheit der identifizierten Probleme lässt sich vor allem den Kriterien Information, Privatsphäre und Sicherheit zuordnen. Diese werden im Folgen erläutert:

- **Information – Begrifflichkeiten**: Für Laien unverständliche bzw. neue Begriffe wie z. B. „PGP-Verschlüsselung", „Browsererweiterung" und „Schlüsselpasswort" werden während des Einrichtungsvorgangs nicht erläutert.
- **Information/Privatsphäre – Mailvelope**: Zum Anbieter, den Zugriffsrechten oder zur Funktionsweise der herunterzuladenden Erweiterung Mailvelope erhalten die Nutzer im Prozess ebenfalls keine näheren Informationen.
- **Information/Sicherheit – unterschiedliche Verfahren**: Für den potenziellen Nutzer ohne Vorkenntnisse wird der Unterschied der E2E-Verschlüsselung zu anderen Sicherheitskonzepten wie De-Mail, „E-Mail made in Germany" oder „vertrauliche Kommunikation"[8] nicht deutlich. Hinweise, bereits mit dem automatisch eingerichteten „E-Mail made in Germany" sicher zu kommunizieren, können vom Nutzer falsch interpretiert werden.
- **Information/Sicherheit – Funktionsweise.** Relevante Informationen zum Verfahren und zur Sicherheit erfolgen erst nach Abschluss des Einrichtungsvorgangs; so z. B. der Hinweis, das Verfahren nur auf Rechnern einzurichten, die nicht von unbekannten Dritten genutzt werden. Weiterhin erfährt der Nutzer erst an dieser Stelle, dass E2E-verschlüsselte Kommunikation nur mit Personen möglich ist, die das Verfahren bereits nutzen.
- **Information – Voraussetzungen**: Weitere mögliche Hindernisse, das Verschlüsselungsverfahren als Laie zu benutzen, bestehen in den Voraussetzungen, auf die der Nutzer erst im Laufe des Einrichtungsprozesses aufmerksam gemacht wird: Die Browsererweiterung Mailvelope ist nur für Chrome und Firefox verfügbar, die Installation gilt nur auf dem jeweiligen Endgerät und ein Drucker zum Ausdrucken eines Wiederherstellungscodes, der bei Problemen mit Schlüsselpasswort, Browser oder Endgerät benötigt wird, sollte zur Verfügung stehen.

3.3.2 Senden einer verschlüsselten E-Mail

Bis nach Abschluss der Einrichtung wird dem Nutzer nicht erläutert, wie das Verschlüsselungsverfahren funktioniert und welche Schritte er unternehmen muss, um nun eine verschlüsselte E-Mail zu versenden bzw. zu entschlüsseln. Wählt der Nutzer auf Vorerfahrung basierend den Button „E-Mail schreiben" aus, so hat er keine Möglichkeit, eine geschriebene E-Mail zu verschlüsseln. Ein entsprechender Hinweis erfolgt jedoch nicht.

Darüber hinaus kann die Option, innerhalb einer nicht E2E-verschlüsselten E-Mail vertraulich zu kommunizieren, vom Nutzer falsch interpretiert werden. Nur durch Recherche in den Versandoptionen erfährt der Nutzer, dass eine „vertrauliche" Mail rein informativen Charakter aufweist. Eine mögliche Folge könnte der Versand sensibler Daten in einer nicht E2E-verschlüsselten E-Mail sein.

Eine E2E-verschlüsselte E-Mail kann nur durch Klick auf das verhältnismäßig kleine Schloss-Symbol verfasst werden (siehe Abbildung 1). Aufgrund der Zwischenspeicherung begonnener, unverschlüsselter Nachrichten bei GMX ist diese Trennung technisch sinnvoll, aber für den Laien nicht unbedingt ersichtlich. Darüber hinaus stellen begonnene, unbeabsichtigt nicht E2E-verschlüsselte E-Mails ein Sicherheitsrisiko dar.

Abbildung 1 | Darstellung der Menüleiste bei GMX.

Wählt der Nutzer jedoch das kleine Schloss-Symbol, findet er sich in einer Umgebung, die der gewohnten E-Mail-Umgebung stark ähnelt, was eine einfache Nutzung auch durch Laien ermöglichen sollte. Der Nutzer erhält durch den Sicherheitshintergrund und eine geänderte Beschriftung von Buttons wie z. B. „verschlüsselt senden" das Feedback, sicher zu kommunizieren.

Wählt der Nutzer einen Kontakt aus, der das gleiche Verschlüsselungsverfahren verwendet, so muss er einmalig entscheiden, ob er diesen Kontakt zur Schlüsselverwaltung hinzufügen möchte. Nach der Bestätigung ist E2E-verschlüsselte Kommunikation mit dem Kontakt möglich. Wozu der Zusatzschritt dient, ist dem Nutzer jedoch möglichweise nicht ersichtlich.

Wählt der Nutzer einen Kontakt aus, der das Verschlüsselungsverfahren nicht nutzt, wird dem Nutzer ein Problem durch ein kleines rotes, statt im Regelfall graues, Schloss-Symbol an der E-Mail-Adresse signalisiert. Erst beim Absenden der E-Mail wird der Nutzer jedoch explizit darauf hingewiesen, dass eine Kommunikation mit diesem Kontakt nur nach Einladung zur Nutzung des Verfahrens möglich ist. Als Alternative bleibt dem Nutzer nur die nicht E2E-verschlüsselte Kommunikation mit diesem Kontakt. Die Abhängigkeit der Verschlüsselung von der Nutzung des Verfahrens durch andere Kontakte könnte ein Hindernis für die Nutzung durch Laien darstellen.

Nach Verfassen der E-Mail genügen ein Klick auf „verschlüsselt senden" und die Eingabe des Schlüsselpassworts. Verbesserungswürdig erscheint hier, dass sich das Feedback nach Absenden einer E-Mail nicht von dem einer nicht E2E-verschlüsselten E-Mail unterscheidet.

3.3.3 Entschlüsselung einer verschlüsselten E-Mail

Eine E2E-verschlüsselte E-Mail, gekennzeichnet durch ein Schloss-Symbol, wird ebenso wie eine herkömmliche E-Mail im Postfach des Nutzers angezeigt und auf gleiche Weise geöffnet. Der einzige Unterschied besteht darin, dass der Nutzer vor dem Lesen der Nachricht zur Eingabe seines Schlüsselpassworts aufgefordert wird. Nach Eingabe und Bestätigung des Passworts erscheint die entschlüsselte E-Mail vor einem Sicherheitshintergrund aus Schloss-Symbolen, was dem Nutzer Sicherheit suggeriert. Dieser Vorgang scheint auch für Laien leicht umsetzbar, da er dem Umgang mit nicht E2E-verschlüsselten E-Mails gleicht.

4 Sicherheitsbewertung

Die Erweiterung Mailvelope und auch OpenPGP.js wurden in den vergangenen Jahren durch die Sicherheitsunternehmen Cure53 und iSECpartners auf Schwachstellen geprüft.[9] Die auf der

8 https://hilfe.gmx.net/email/mailversand.html#optionen (abgerufen am 29.03.2016)

9 https://github.com/mailvelope/mailvelope/wiki/Security (abgerufen am 29.03.2016)

Webseite genannten Schwachstellen wurden in der neusten Version von Mailvelope behoben.

Vor der Generierung der Schlüssel muss ein Schlüsselpasswort festgelegt werden. Die einzige Anforderung an dieses Passwort ist eine Mindestlänge von vier beliebigen Zeichen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) [10] empfiehlt im IT-Grundschutz eine Mindestlänge von acht Zeichen. Außerdem sollten mindestens zwei der folgenden Arten von Zeichen enthalten sein: Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen. Eine Mindestlänge von nur vier Zeichen kann damit ein Sicherheitsrisiko darstellen. Falls der private Schlüssel in die Hände eines Angreifers fällt, ist das Passwort der einzige Schutz um eine unbefugte Nutzung zu verhindern.

Nach Eingabe des Passwortes werden ein privater und ein öffentlicher RSA-Schlüssel der Länge 4096 Bit erzeugt. Diese Schlüssellänge erfüllt die aktuellen Sicherheitsanforderungen. So empfiehlt beispielsweise das BSI ab dem Jahr 2017 eine Mindestlänge von 3072 Bit [11].

Die Erzeugung der Schlüssel wird lokal auf dem Computer des Nutzers durchgeführt. In diesem Schritt verlässt keiner der beiden Schlüssel dessen Computer. Somit ist die Sicherheit der Schlüssel ohne Vertrauen in zentrale Server gewährleistet.[10]

Im Falle der Sicherung werden die Schlüssel und das Schlüsselpasswort des Nutzers in einem Datenpaket zusammengefasst und mit dem 26-stelligen Wiederherstellungscode mittels AES-256 verschlüsselt. Laut IT-Grundschutz ist AES-256 ein sicherer Algorithmus für die symmetrische Verschlüsselung und stellt daher kein Sicherheitsrisiko dar [10]. Darüber hinaus wird das Datenpaket ausschließlich auf dem Computer des Nutzers verschlüsselt.

E2E-verschlüsselte E-Mail-Kommunikation beruht auf der Authentizität des zur Verschlüsselung verwendeten Schlüssels. Zur Erleichterung dieser Authentizitätsprüfung ist der Abgleich sogenannter Fingerabdrücke vorgesehen. Aufgrund der Tatsache, dass dem Nutzer eine Beschreibung zum Abgleich der Fingerabdrücke sowie Informationen über die Notwendigkeit dieser Handlung fehlen, muss die Umsetzung dieses Sicherheitsmerkmals als unzureichend angesehen werden.

Ein weiteres Sicherheitsrisiko stellt die Einstellung „Nutzungsstatistiken und Absturzberichte automatisch an Google senden" im Browser Google Chrome dar. Dadurch könnten beim Absturz Speicherinhalte mit dem privaten Schlüssel an Google gesendet werden. Auf dieses Sicherheitsrisiko wird der Nutzer nur in den FAQs von Mailvelope hingewiesen. Aus Sicherheitsgründen wäre es sinnvoll den Nutzer vor der Einrichtung darauf hinzuweisen.

5 Fazit

Die Benutzbarkeitsanalyse ergab, dass die Menüführung der E2E-verschlüsselten E-Mail-Kommunikation weitestgehend auch für Laien nachvollziehbar sein sollte, da sie im Aufbau der gewohnten E-Mail-Kommunikation ähnelt. Allerdings sollte das Symbol zum Schreiben verschlüsselter E-Mails, das im Verhältnis zum regulären „E-Mail schreiben" sehr klein und unauffällig ist, präsenter gestaltet werden. Ein Hinweis auf das Symbol sollte bereits am Ende des Einrichtungsprozesses erfolgen. Weiterhin erhält der Nutzer kaum Informationen zum Mehrwert und zur Funktionsweise der E2E-Verschlüsselung, in Abgrenzung zu „E-Mail made in Germany" und De-Mail. Integrierte Informationen, die ein konzeptuelles Verständnis für das Verfahren ermöglichen, können außerdem die Benutzbarkeit steigern und Nutzungswahrscheinlichkeit erhöhen [3, 13].

Insbesondere aus Sicht der IT-Sicherheit ist die Umsetzung des Verfahrens verbesserungswürdig. So besteht aufgrund fehlender Hinweise, dem unauffälligen Schlosssymbol und für den Nutzer irritierender Formulierungen wie „vertrauliche" Kommunikation die Gefahr, ungewollt nicht E2E-verschlüsselt zu kommunizieren. Daher sollte beim Schreiben einer unverschlüsselten Nachricht ein entsprechender Hinweis erfolgen.

Die Anforderungen an Schlüsselpasswörter können aus Sicht der IT-Sicherheit als kritisch angesehen werden. Diese sollten daher zukünftig an etablierte Empfehlungen angepasst werden. Letztlich beruht die Sicherheit des Verfahrens darauf, dass verwendete öffentliche Schlüssel tatsächlich von den intendierten Kommunikationspartnern erzeugt wurden. Insbesondere die fehlenden Informationen zum Abgleich der Fingerabdrücke stellen daher ein Sicherheitsrisiko für die Kommunikation dar. Daher sollten zukünftig eine für Laien nachvollziehbarere Möglichkeit zur Authentizitätsprüfung öffentlicher Schlüssel erarbeitet werden.

10 Sicherheitsbewusste Nutzer haben die Möglichkeit den Quellcode von Mailvelope selbst zu überprüfen und zu kompilieren.

Danksagung

Diese Arbeit ist über CRISP durch das Bundesministerium für Bildung und Forschung (BMBF) und über CASED durch die Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz (LOEWE) finanziert.

Literatur

[1] Whitten, A. and J.D. Tygar. *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.* in *Usenix Security*. 1999.

[2] Sheng, S., et al. *Why johnny still can't encrypt: evaluating the usability of email encryption software.* in *Symposium On Usable Privacy and Security*. 2006.

[3] Ruoti, S., et al., *Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client*. 2015.

[4] Ruoti, S., et al., *"We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users*, in *34th Annual ACM Conference on Human Facors and Computing Systems (CHI 2016)*. 2016: San Jose, CA, USA.

[5] Hollingsed, T. and D.G. Novick. *Usability inspection methods after 15 years of research and practice.* in *Proceedings of the 25th annual ACM international conference on Design of communication*. 2007. ACM.

[6] Good, N.S. and A. Krekelberg. *Usability and privacy: a study of Kazaa P2P file-sharing.* in *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2003. ACM.

[7] Lewis, C. and C. Wharton, *Cognitive walkthroughs.* Handbook of human-computer interaction, 1997. 2: p. 717-732.

[8] Wharton, C., et al. *The cognitive walkthrough method: A practitioner's guide*. in *Usability inspection methods*. 1994. John Wiley & Sons, Inc.

[9] Karat, C.-M., R. Campbell, and T. Fiegel. *Comparison of empirical testing and walkthrough methods in user interface evaluation.* in *Proceedings of the SIGCHI conference on Human factors in computing systems*. 1992. ACM.

[10] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Kataloge.* 2014.

[11] Bundesamt für Sicherheit in der Informationstechnik, *Kryptographische Verfahren: Empfehlungen und Schlüssellängen.* 2016.

[13] Renaud, K., M. Volkamer, and A. Renkema-Padmos. *Why doesn't Jane protect her privacy?* in *Privacy Enhancing Technologies*. 2014. Springer.