tenable

CUSTOMER STORY

CANCOM COUNTS ON TENABLE FOR VULNERABILITY AND EXPOSURE MANAGEMENT

CANCOM

OVERVIEW

As a "Leading Digital Transformation Partner" and hybrid IT service provider in the DACH region, CANCOM has been guiding companies, organizations and the public sector along the path into the digital future for over 30 years. The internationally active company is one of the leading hybrid IT service providers in the DACH region, with more than 5,600 employees at 80 locations in the DACH region as well as in Belgium, Slovakia, Romania and the Czech Republic. CANCOM relies on Tenable's vulnerability and exposure management solutions to protect its own infrastructure and will offer these security solutions to its customers as part of its managed services portfolio in the future.

BUSINESS NEEDS

Industry: IT Service Provider

Location: DACH Region

Solutions:

tenable Security Center

tenable Nessus

The attack surface of all companies is constantly growing, and with it the risk of vulnerabilities.

As an experienced specialist for security solutions, CANCOM designs and implements customized security solutions for its customers and supports them in operating their infrastructure securely. CANCOM relies on Tenable's vulnerability and exposure management solutions to protect its own infrastructure and will offer these security solutions to its customers as part of its managed services portfolio in the future.

“Tenable has established itself as a market leader in the difficult area of exposure management," said Marcel Reifenberger, CISO at CANCOM. "Digital trust is of the utmost importance to us and our customers, and Tenable’s reputation and leadership were key factors in our decision. In addition, we were impressed by Tenable’s streamlined user experience and were immediately sold.”

Attack surface and vulnerability risk on the increase

The services range from analyzing and assessing security and network infrastructure to designing state-of-the-art security solutions and deploying and implementing them. CANCOM helps its customers operate their infrastructure securely with its security support and managed services.

The attack surface of all companies is constantly growing, and with it the risk of vulnerabilities and misconfigurations. As a hybrid IT service provider, CANCOM itself operates a large IT department with its own data centers in Germany and teams across several departments.

CANCOM had been using different vulnerability scanners in individual business units of its IT environment, which has grown over the years. Because of this isolated approach, cybersecurity assessments proved increasingly complex, and maintenance was time-consuming and expensive. In addition, there were problems due to incompatibility with other security solutions. CANCOM has therefore set itself the goal of deploying a uniform solution for vulnerability and exposure management throughout the company.

“Safety is a marathon, not a sprint. Attackers only need to find a single open door, but we must close all the doors. The aim must be to make life so difficult for the attackers as possible,” says Reifenberger. "It is now clear that not all doors – or vulnerabilities – can be patched immediately. That's why it's important to keep them all in mind and to distinguish between doors that are particularly at risk and doors that are less at risk.”

CANCOM chooses Tenable for its vulnerability management solution

To meet this challenge, CANCOM chose technology from Tenable, which specializes in exposure management solutions. Tenable supports B2B customers around the world who want to identify and reduce cybersecurity risks. As the developer of Tenable Nessus®, Tenable has extended its expertise in exposure management to provide the world's first platform for detecting and securing any digital asset on any computing platform.

User-friendliness is the decisive factor in security solutions. CANCOM conducted a proof-of-concept (PoC) with Tenable that quickly addressed any potential concerns. “Tenable is intuitive, easily customizable, and compatible with operating system environments like Windows and Linux and easily integrates with ITSM platforms such as ServiceNow. This seamless integration means that many processes can be automated,” explains Reifenberger.

Gradual rollout, integration into managed services portfolio is planned

All hardware is located in CANCOM data centers in Germany, much of it virtualized. CANCOM relies on comprehensive vulnerability management of its entire corporate environment as well as penetration tests to ensure that all vulnerabilities and possible entry points are found. In the future, Tenable Security Center (formerly Tenable.sc) will be used for vulnerability management. Tenable Security Center is managed on-premises, based on Tenable Nessus® technology, and provides comprehensive vulnerability coverage with continuous assessment of the network in real time.

The solution provides security teams with a risk-based overview of the state of their IT, security and compliance. Security executives have a comprehensive overall picture of all risks in the environment and know exactly which vulnerabilities and assets they should prioritize.

The introduction of Tenable at CANCOM will be gradual and will replace existing solutions. CANCOM intends to use Tenable's solutions not only in-house, but also to integrate them into its managed security services portfolio.

“Security is an essential trademark of CANCOM, and that's why we always use the most innovative solutions. We only offer our customers solutions if we ourselves are convinced that they meet the respective requirements in the best possible way. In this way we would like to take into account an increasing demand in the future. Nowadays, every company needs a solution for vulnerability and exposure management, otherwise the security of the business cannot be guaranteed,” explains Reifenberger.

New challenges of the wireless trend, cloud and hybrid working

The Internet of Things (IoT) will also lead to ever greater and more diverse security challenges for enterprises, as IoT devices bring new vulnerabilities to the corporate environment. Add to that 5G/6G and WLAN 6, because wireless is the future, and attacks through wireless infrastructure will increase as a result. Another critical security issue is the ongoing shift to cloud computing and hybrid working models, as this increases both the attack surface and the number of potential threats and vulnerabilities. Even before the pandemic began, CANCOM was well prepared for hybrid work, but it continues to bring new security challenges.

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

An ever-growing attack surface can also be attributed to corporate growth. CANCOM is growing rapidly and is constantly acquiring companies that need to be integrated into the security concept. This means that vulnerability scanning has to be a continuous, automated process.

Usability, performance and context are key

"End users need to be able to use a security solution without problems and see tangible benefits. You should have as little work as possible with security, so both usability and performance must be right," explains Reifenberger. "Tenable is very compelling in this regard because it simplifies IT security while increasing the level of security."

Roger Scheer, Tenable's Regional Vice President Central Europe, adds, "It's also important to assess vulnerabilities in the context of an organization's specific cyber risk. The importance of a particular vulnerability may change over time as the threat landscape changes as well. Also, a vulnerability in one type of asset may have a less severe impact than another type of asset. Modern, future-proof vulnerability management must be able to recognize exactly this and provide context for the environment that is to be protected. Only then can a company prioritize a vulnerability in such a way that the risk is reduced as much as possible."

Automation pays off

Security is an increasingly complex issue and a challenge for many companies. The overarching goal is to continuously reduce cyber risk. It is therefore important to focus on the essentials, reduce complexity as much as possible and automate as much as possible. But many companies still do too much manual work when it comes to cybersecurity.

"Automation requires an initial investment, but it definitely pays off in the long run. Thanks to Tenable, we can do our 'homework' in terms of vulnerability management better and better," concludes Reifenberger.

tenable®

COPYRIGHT 2023 TENABLE, INC. ALL RIGHTS RESERVED. TENABLE, TENABLE.IO, NESSUS, ALSID, INDEGY, LUMIN, ASSURE, AND LOG CORRELATION ENGINE ARE REGISTERED TRADEMARKS OF TENABLE, INC. OR ITS AFFILIATES. TENABLE.SC, TENABLE.OT, TENABLE.AD, EXPOSURE.AI, AND THE CYBER EXPOSURE COMPANY ARE TRADEMARKS OF TENABLE, INC. OR ITS AFFILIATES. ALL OTHER PRODUCTS OR SERVICES ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.