HZ216998 · ISSN 1868-5757 · www.itsicherheit-online.com August/September 4/2024

IT-SICHERHEIT

Management und Technik

RAGs für die Informationssicherheit

Effizienteres ISMS durch KI

Kubernetes sicher betreiben

Mögliche Angriffsziele, mitigierende Maßnahmen und sinnvolle Prüfziele

Intrusion-Detection-Systeme im Praxistest

Angriffserkennung in Energieanlagen

Der Weg zur kollektiven Cyberresilienz

Zusammenarbeit und Vertrauen im Kampf gegen Cyberkriminalität

DATAKONTEXT

Online-Schulungen IT-Sicherheit 2024

Themen	Referenten	Termine
KI im Kontext der Cybersecurity	Alexander Jaber	03.09.2024 07.11.2024
KI-Abwehrmechanismen in ein Unternehmens-ISMS integrieren – Eine praxisorientierte Blaupause	Jürgen Kreuz	04.09.2024 03.12.2024
Einführung Notfallmanagement nach BSI-Standard 200-4	Tobias Baader	10.09.2024 19.11.2024
CISO und Consulting Exzellenz für Informationssicherheit	Alexander Jaber	11.09.2024
Praxisfall: Herausforderungen und Bewältigung eines Cyberangriffes – vom Angriff bis zur Abwicklung	Tobias Baader	12.09.2024 14.11.2024
Das NIS2 Umsetzungsgesetz (NIS2UmsuCG): Was Unternehmen jetzt beachten müssen	Tobias Baader Dirk Seeburg	17.09.2024 12.11.2024
Quickwins für IT-Sicherheit: Mental-Tool-Box für Sofortmaßnahmen zur Risikoreduzierung	Alexander Jaber	19.09.2024 21.11.2024
Informationssicherheit beim Einsatz von KI für IT, OT und im produzierenden Umfeld	Alexander Jaber	24.09.2024
IT-Sicherheit von M365 – Sicheres Design und sichere Konfiguration	Eric Soldierer	25.09.2024 04.11.2024
KI-Blaupause – Standardszenarien für Angriff und Verteidigung	Jürgen Kreuz	01.10.2024 05.12.2024
Physische Sicherheit für IT-Profis: Vom Konzept zur Umsetzung	Alexander Jaber	02.10.2024 11.11.2024
Betriebssystem Windows härten und absichern – Eine Schritt-für-Schritt-Anleitung	Tobias Elsner	13.11.2024
Incident-Response-Maßnahmen – Auf Sicherheitsvorfälle optimal reagieren	Tobias Elsner Thomas Wallutis	16.12.2024

Jeweils von 10:00 Uhr bis 14:30 Uhr | online

Änderungen bei Terminen bleiben vorbehalten.

10 % Rabatt für <kes>+ Abonnenten

Jetzt anmelden für nur 349,– € zzgl. MwSt.:
www.datakontext.com/it-sicherheit-seminare

Liebe Leserinnen, liebe Leser,

Klartext statt Fachchinesisch: In der digitalen Welt von heute brauchen wir starke Schilde für unsere sensiblen Daten. Da sind sich alle einig. Doch die meisten Informationssicherheits-Managementsysteme (ISMS) sind so kompliziert wie ein Behördendeutsch-Wörterbuch. Kein Wunder, dass viele Mitarbeiter damit nicht zurechtkommen. Hier setzt die innovative Technologie der **Retrieval-Augmented Generation (RAGs)** an. Sie vereint die Vorteile von Sprachmodellen und Wissensdatenbanken, um **ISMS auf ein neues Level zu heben.** Diese Systeme verstehen komplexe Richtlinien und erklären sie uns in einfachen Worten. So weiß jeder, was zu tun ist – ohne Rätselraten und Frust. RAGs sind nicht nur wortgewandt, sondern auch blitzschnell: Sie durchsuchen riesige Datenmengen im Nu und finden genau die Informationen, die die Mitarbeiter im Moment brauchen. **So sparen sie Zeit und Nerven – und arbeiten gleichzeitig sicherer.** Im Vergleich zu herkömmlichen Methoden wie Fine-Tuning bieten RAGs entscheidende Vorteile: Sie sind ressourcenschonend, flexibel und transparent. Zudem ermöglichen sie eine rollenbasierte Zugriffskontrolle, um den Schutz sensibler Daten zu gewährleisten. In unserem Artikel „Effizientes ISMS durch KI“ ab Seite 22 erfahren Sie, wie Unternehmen RAGs konkret im ISMS einsetzen können, welche Vorteile sie bieten und wie sie die Zukunft der IT-Sicherheit prägen werden.

Digitalisierung? Großartig! Vernetzung? Super! Aber Vorsicht, liebe Unternehmen: In der schönen neuen Onlinewelt lauern bekanntlich Gefahren! Das mussten kürzlich (wieder einmal) viele Firmen schmerzlich erfahren, als ein fehlerhaftes Update der Cybersicherheitssoftware Falcon des Unternehmens **Crowdstrike** weltweit zu massiven IT-Ausfällen führte. Flughafen-chaos, lahmgelegte Krankenhäuser, schließende Supermärkte: **Die Folgen des Ausfalls waren immens.** Einmal mehr zeigte sich, wie fragil unsere vernetzte Welt ist und wie schnell ein kleiner Fehler zu einem Dominoeffekt mit katastrophalen Auswirkungen führen kann. Was also tun? **Ein individueller Ansatz zur Cybersicherheit reicht nicht mehr aus.** Komplexe Lieferketten und die zunehmende Vernetzung machen Unternehmen von anderen Akteuren abhängig. Angriffe auf einen Partner können das gesamte Ökosystem gefährden. Der Schlüssel zur erfolgreichen Abwehr von Cyberangriffen liegt daher in der **Zusammenarbeit.** Unternehmen müssen sich zu einem vernetzten Sicherheitsbündnis zusammenschließen, um Informationen auszutauschen, Bedrohungen zu erkennen und gemeinsam Lösungen zu entwickeln. **Digitales Vertrauen ist dabei die Basis für eine erfolgreiche Kooperation.** Der Text „Der Weg zur kollektiven Cyberresilienz“ zeigt auf, wie Unternehmen ein cyberresilientes Ökosystem aufbauen können und beschreibt eine langfristige Strategie (Seite 38).

Darüber hinaus beleuchten wir in unserem **Schwerpunkt Malware** in dieser Ausgabe die immer größer werdende Gefahr durch Ransomware-Angriffe (Seite 10) und stellen **Zero-Trust-Segmentierung** als wirksame **Gegenmaßnahme** vor (Seite 12), denn herkömmliche Sicherheitslösungen stoßen beim Schutz vor der Ransomwareplage an ihre Grenzen. Sie sind oft reaktiv und können Angriffe nicht zuverlässig erkennen oder verhindern. Die Zero-Trust-Segmentierung minimiert die Angriffsfläche, indem kritische IT-Bereiche isoliert werden. So wird die Ausbreitung von Ransomware im Netzwerk eingedämmt und eine schnelle Reaktion auf Bedrohungen ermöglicht.

Viel Spaß bei der Lektüre wünscht Ihnen

Sebastian Frank

www.itsicherheit-online.com/newsletter

INHALT

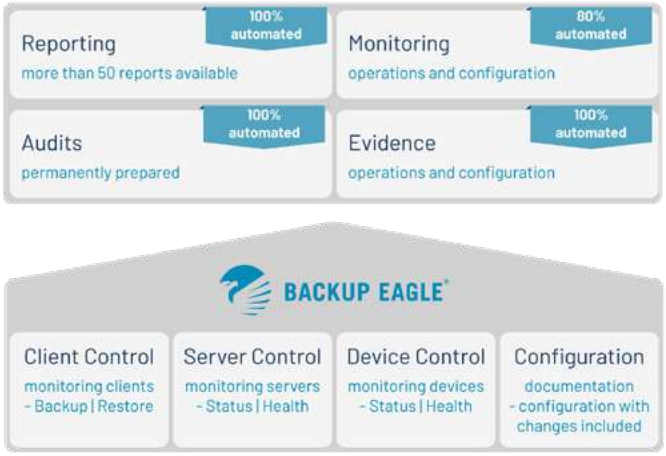
22 RAGS FÜR DIE INFORMATIONSSICHERHEIT
EFFIZIENTERES ISMS DURCH KI (1)

SEP UND **BACKUP EAGLE** SCHLIESSEN PARTNERSCHAFT

Die SEP AG, ein Anbieter von plattformunabhängigen Backup- und Disaster-Recovery-Lösungen, und BACKUP EAGLE geben ihre neue Partnerschaft bekannt. Ziel der Zusammenarbeit ist es, Unternehmen in Deutschland bei der Bewältigung der wachsenden Herausforderungen in den Bereichen Datensicherheit und Compliance zu unterstützen.

Die Kombination aus SEP sesam Apollon und den Überwachungs- und Audit-Funktionen von BACKUP EAGLE ermöglicht es Unternehmen, ihre Datensicherungsstrategie auf das nächste Level zu heben. BACKUP EAGLE bietet tägliche revisionssichere Kontrolle von Backups, Wiederherstellungen und Monitoring für alle Backup-Umgebungen. Alle erforderlichen Nachweise werden automatisch erstellt, potenzielle Probleme werden erkannt und die zentrale Administration macht die Verwaltung sehr einfach.

„Unsere Partnerschaft mit BACKUP EAGLE stärkt die Datensicherheit und die Compliance unserer Kunden erheblich. Gemeinsam bieten wir eine umfassende Lösung, die den Schutz vor Cyberbedrohungen maximiert und die strengen Anforderungen der NIS-2-Richtlinie erfüllt", sagt Susanne Moosreiner, CEO der SEP AG. ■



Lösungsübersicht BACKUP EAGLE (Bild: SEP AG)

KOOPERATION VON **VERTIV** UND **ZINCFIVE**

Vertiv, ein Spezialist von Lösungen für kritische digitale Infrastrukturen und Kontinuität, erweitert sein Portfolio an Batteriesystemen für die Notstromversorgung von Rechenzentren. Ab sofort bietet das Unternehmen die unterbrechungsfreie Stromversorgung (USV) der ZincFive BC-Serie von ZincFive an, einem Anbieter von Lösungen auf Basis von Nickel-Zink-Batterien (NiZn). Die sicheren und wiederverwertbaren Nickel-Zink-Batterien sind mit ausgewählten großen und mittleren Vertiv USV-Systemen, einschließlich der kürzlich eingeführten Vertiv Trinergy, als Quelle für Backup-Energiespeicher kompatibel.

Die USV-Batterieschränke der BC-Serie von ZincFive sind die erste Nickel-Zink-Batterie-Energiespeicherlösung mit Abwärts- und Aufwärtskompatibilität mit USV der Megawattklasse. Die BC-Serie bietet im Vergleich zu VRLA- und Lithium-Ionen-Batterien branchenweit die kleinste Stellfläche und ist äußerst wartungsarm. Die NiZn-Chemie sorgt für einen zuverlässigen Betrieb, wobei die Batteriestränge selbst bei schwachen oder verbrauchten Zellen leitfähig bleiben. Darüber hinaus haben die NiZn-Batterien von ZincFive laut einer von Boundless Impact durchgeführten und von ZincFive in Auftrag gegebenen Studie deutlich geringere Auswirkungen auf die Umwelt als Blei-Säure- und Lithium-Batterien. Dies wurde auch durch die Analyse eines unabhängigen Experten bestätigt. ■

HID UND **INNER RANGE:** WALLET-FÄHIGE LESEGERÄTE FÜR ZUTRITTSKONTROLLE

HID baut seine Partnerschaft mit Inner Range, einem globalen Anbieter von integrierten Zutrittskontrollsystemen, aus. Die erweiterte Kooperation bietet Unternehmen weltweit sicherere und zukunftsfähige Lösungen, die auf den Signo-Lesegeräten von HID basieren und SIFER Credential von Inner Range unterstützen.

Durch die Wallet-fähigen Lesegeräte von HID erweitert Inner Range sein Produktportfolio und bietet Unternehmen eine zusätzliche Möglichkeit, mobile Credentials von HID zu integrieren. Mitarbeiter, Mieter und Besucher erhalten einen einfachen und gleichzeitig sicheren Zugang zu Büros, Besprechungsräumen, Druckern, Schließfächern und anderen Bereichen, indem sie ihr Smartphone oder ihre Smartwatch in die Nähe eines SIFER-fähigen Lesegeräts halten. Die auf HID Mobile Access basierende In-Wallet-Lösung verwendet fortschrittliche Verschlüsselungs- und Sicherheitsprotokolle.

„Der mobile Zugang entwickelt sich weltweit zu einer starken Triebkraft für die Neugestaltung der physischen Zutrittskontrolle", betont Steve Katanas, Regional Head for HID Physical Access Control Solutions, ANZ. „Die Kunden von Inner Range werden von allen Vorteilen profitieren, die sich aus dem Hinzufügen mobiler Zugangsdaten in die Apple oder Google Wallet – und in naher Zukunft auch andere OEM-Wallets – ergeben." ■

LANCOM SYSTEMS ERHÄLT ISO/IEC-27001-ZERTIFIZIERUNG

Der deutsche Netzwerkinfrastruktur- und Security-Ausrüster LANCOM Systems hat sein Informationssicherheits-Managementsystem (ISMS) nach der international anerkannten ISO/IEC-27001-Norm zertifizieren lassen. Die unabhängige Zertifizierung durch den TÜV Rheinland belege den hohen Stellenwert, den LANCOM dem Schutz sensibler Daten und der IT-Sicherheit seiner Kunden und Partner beimisst.

Die ISO/IEC 27001 ist eine weltweit anerkannte Norm für Informationssicherheits-Managementsysteme. Sie bietet Unternehmen klare Leitlinien für die Planung, Umsetzung, Überwachung und Verbesserung ihrer Informationssicherheit. LANCOM hat seine internen Abläufe einem offiziellen Audit unterzogen. Das Informationssicherheits-Management in den Bereichen LANCOM Management Cloud sowie Service- und Support-Prozesse wurde gemäß dem ISO/IEC-27001-Standard durch den TÜV Rheinland geprüft und zertifiziert.

LANCOM Kunden und Partner erhalten damit den objektiven Nachweis, dass ihre Daten gemäß höchster Sicherheits- und Datenschutzstandards verarbeitet, Risiken für die Integrität und Verfügbarkeit von IT-Systemen minimiert und potenzielle Sicherheitsvorfälle schnell und effektiv gehandhabt werden. LANCOM-Gründer und -Geschäftsführer Ralf Koenzen: „In einer zunehmend vernetzten und digitalisierten Welt wird Informationssicherheit zum alles entscheidenden Faktor. Für LANCOM Systems hat der Schutz unseres Unternehmens und damit auch unserer Kunden und Partner und ihrer Daten höchste Priorität. Diese Verantwortung nehmen wir sehr ernst. Deshalb haben wir unsere Prozesse auf den Prüfstand gestellt und freuen uns sehr über das erfolgreiche Audit und die ISO/IEC-27001-Zertifizierung." ■

OUTPOST24 ERNENNT IDO ERLICHMAN ZUM NEUEN CEO

Mit Ido Erlichman an der Spitze stellt sich Outpost24, ein Anbieter von Cyberrisikomanagement- und Threat-Intelligence-Lösungen, für die Zukunft auf. Der neue Chief Executive Officer (CEO) bringt mehr als **20 Jahre Erfahrung** in den Bereichen Cybersicherheit, Technologie und Finanzen mit und kann auf eine beeindruckende Erfolgsbilanz in Führungspositionen und Innovationen verweisen. Zuletzt war Erlichman CEO des IT-Sicherheitsunternehmens Kape Technologies, das er zu einem globalen Marktführer im Bereich Datenschutz und Cybersicherheit führte.

„Wir freuen uns, Ido Erlichman als unseren neuen CEO begrüßen zu dürfen", sagte Niklas Savander, Vorstandsvorsitzender von Outpost24. „Seine Erfahrung und Führungsqualitäten werden von unschätzbarem Wert sein, und ich habe volles Vertrauen, dass er unsere strategischen Ziele vorantreiben und das Unternehmen weltweit auf die nächste Entwicklungsstufe bringen wird."

Ido Erlichman (Bild: Outpost24)

„Ich bin stolz darauf, die Rolle des CEO bei Outpost24 zu übernehmen", erklärt Erlichman. „Ich freue mich darauf, auf dem starken Fundament des Unternehmens aufzubauen, indem wir neue Möglichkeiten zur Erweiterung und Kombination unseres Produktportfolios ausloten …" ■

INFINIGATE GROUP INVESTIERT IN WAVELINK

Die Infinigate Group übernimmt die Mehrheit des australischen IT-Distributors Wavelink. Mit dieser strategischen Investition erweitert Infinigate seine Präsenz im Pazifikraum und erschließt sich gleichzeitig neue Geschäftsfelder in den Bereichen Cybersecurity und Mobility. Wavelink, mit Sitz in Melbourne, gilt als schnell wachsender Distributor mit einem ausgezeichneten Ruf in der Region. Das Unternehmen ist spezialisiert auf die Distribution von IT-Sicherheitslösungen und Mobility-Produkten.

Klaus Schlichtherle, CEO der Infinigate Group, zeigt sich erfreut: „Im Zuge unseres globalen Expansionsplans öffnet dieses strategische Investment in Wavelink für unser Unternehmen eine Tür in einen neuen, wichtigen Markt außerhalb von EMEA. Die Philosophien und Geschäftsmodelle unserer Unternehmen passen hervorragend zusammen. Vereint können wir unser gemeinsames Wachstum weiter steigern, auch dank einer breiteren und stärkeren Mitarbeiterschaft. Unser Portfolio an Lösungen und auch unser Können und Wissen ergänzen sich bestens."

Wavelink wird weiterhin unter seinem eigenen Namen und mit dem bestehenden Managementteam operieren. Die Geschäfte in der Region Australien und Neuseeland (ANZ) werden nach wie vor von Ilan Rubin geführt. Innerhalb der Organisationsstruktur der Infinigate Group berichtet Rubin direkt an Mahmoud Nimer, den Präsidenten MEA (Middle East and Africa) und APAC (Asia Pacific) bei der Infinigate Group und Co-Gründer von Starlink. ■

Klaus Schlichtherle, CEO der Infinigate Group (Bild: Infinigate Group)

ZUSAMMENARBEIT ZWISCHEN **BITDEFENDER** UND **ARROW ELECTRONICS**

Bitdefender und Arrow Electronics erweitern ihre Kooperation: Gemeinsam werden die beiden Unternehmen den Managed Service Providern (MSPs) sowie deren Kunden eine breitere Palette an leistungsstarken Lösungen zur Prävention, Erkennung und Reaktion auf Gefahren auf Subskriptionsbasis anbieten. Dafür wird Arrow zu einem Abonnement-basierten Modell wechseln. Kunden in Deutschland, Großbritannien, Frankreich und Benelux erhalten das gesamte MSP-Produktportfolio von Bitdefender als Pay-as-you-go-Modell.

„Unternehmen müssen jeden möglichen Vorteil nutzen, um mit der neuesten Malware und den Techniken Schritt zu halten, die Cyberkriminelle für die Infiltration von Systemen und das Eindringen in IT-Umgebungen einsetzen", sagt Richard Tallman, Senior Director, Worldwide MSP and Cloud bei der Bitdefender Business Solutions Group. „Unsere erweiterte Zusammenarbeit mit Arrow bietet den Kunden einen optimalen Weg, um Cyberangriffe durch leistungsstarke Prävention, Erkennung und Reaktion zu unterbinden. Dafür steht eine sofort einsetzbare Gesamtlösung mit den von Kunden bevorzugten flexiblen Diensten bereit." ■

SECUVERA ALS PRÜFSTELLE IM PROGRAMM NESAS CCS-GI ANERKANNT

Die secuvera GmbH ist seit dem 1. Juni 2024 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als neue Prüfstelle im Zertifizierungsprogramm NESAS CCS-GI anerkannt. Damit stehen interessierten Herstellern nun drei anerkannte Prüfstellen für die Evaluierung von Netzwerkprodukten zur Verfügung.

Prüfstellen in NESAS CCS-GI evaluieren Netzwerkprodukte, die Bestandteile von Mobilfunknetzen sind, anhand der spezifizierten Testfälle des Generation Partnership Project (3GPP). Diese Testfälle prüfen Netzwerkprodukte auf bekannte Schwachstellen oder Fehler, die sich aus der Umsetzung der Spezifikationen der 3GPP ergeben. So wird eine grundlegende Sicherheit von Netzwerkprodukten in Mobilfunknetzen gewährleistet. ■

AKTUALISIERTER LEITFADEN ZUR „CYBERSICHERHEIT UND IT-COMPLIANCE IM UNTERNEHMEN“

Trend Micro hat seinen juristischen Leitfaden „Cybersicherheit und IT-Compliance im Unternehmen“ neu aufgelegt. Der umfassende Ratgeber bietet Unternehmen einen praxisnahen Überblick über wichtige rechtliche Themengebiete im Zusammenhang mit dem Einsatz von IT und Internet. Mit der Neuauflage wurden insbesondere die neuen Regularien NIS-2 und DORA berücksichtigt. Diese EU-Richtlinien definieren verbindliche Mindestanforderungen an die Cybersicherheit von Unternehmen in kritischen Sektoren. Der Leitfaden erläutert detailliert die Verantwortlichkeiten und Pflichten, die mit damit verbunden sind. Darüber hinaus beleuchtet der Ratgeber aktuelle Fragen zur DSGVO-Compliance beim Einsatz von Cybersicherheitslösungen sowie die Sicherheitsanforderungen an Cloud-Dienste gemäß C5-Kriterienkatalog.

Seit dem Inkrafttreten von NIS-2 und DORA am 16. Januar 2023 sehen sich viele Unternehmen mit neuen Herausforderungen im Bereich der Cybersicherheit und der IT-Compliance konfrontiert. Der aktualisierte Leitfaden unterstütze Unternehmen dabei, diese komplexen Regularien zu verstehen und die notwendigen Maßnahmen für eine rechtskonforme und sichere IT-Infrastruktur zu ergreifen, so Trend Micro. ■

Der Leitfaden „Cybersicherheit und IT-Compliance im Unternehmen“ von Trend Micro ist kostenlos zum Download verfügbar (Registrierung erforderlich):

KOMPLETTPAKET FÜR SICHERES ULTRAMOBILES ARBEITEN AUF IOS-BASIS

Mit dem neuen Sicherheitskonzept „indigo“ können Behörden und öffentliche Verwaltungen iPhones und iPads für die Bearbeitung von geheimen Informationen bis hin zur Einstufung „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD) nutzen. Materna Virtual Solution bietet ab sofort umfassende und maßgeschneiderte Lösungen rund um indigo an – von der ersten Idee bis zum laufenden Betrieb.

„iOS Native Devices in Government Operation“ (indigo) ermöglicht die sichere Nutzung von iPhones und iPads für grundlegende Kommunikations- und Kollaborationsfunktionen wie E-Mail, Kalender und Kontakte im VS-NfD-Bereich. Materna Virtual Solution erweitert diese Basisfunktionen um ein breites Spektrum an zusätzlichen zertifizierten Apps und Services, die im eigenen indigo-Kompetenz-Zentrum entwickelt wurden. Das indigo-Produktportfolio umfasst unter anderem:

- **TrustDok:** eine App für das sichere Bearbeiten von Dokumenten, die alle gängigen Funktionen wie Lesen, Erstellen, Bearbeiten, Löschen, Freigeben und lokales Speichern vereint
- **TrustOwl:** ein sicherer Intranet-Browser, der den mobilen Zugriff auf interne Ressourcen und Fachanwendungen ermöglicht
- **TrustCam:** eine Kamera-App für die sichere Aufnahme und Übertragung von Fotos (in Entwicklung)

Darüber hinaus bietet Materna Virtual Solution in Partnerschaft mit Rhode & Schwarz sowie agilimo Consulting die Lösung „indigo-in-a-box. Diese Komplettlösung beinhaltet Hardware, Software und Server-Infrastruktur und ermöglicht eine schnelle, einfache und sichere Aktivierung der mobilen Endgeräte. Als Apple Managed Service Provider liefere das Unternehmen aber nicht nur die für das ultramobile Arbeiten notwendigen Anwendungen und Geräte, sondern auch einen umfassenden Service entlang der gesamten Wertschöpfungskette. Das Portfolio des indigo Kompetenz-Center umfasst neben der Entwicklung behördenspezifischer Anwendungen eine Lernplattform für den richtigen Umgang mit indigo, einen indigo Readiness Check für das Prüfen der infrastrukturellen Gegebenheiten, Experten „on demand“ sowie Unterstützung und Beratung bei Konzeption, Rollout und Betrieb von indigo-Umgebungen. ■

VIDEOKONFERENZLÖSUNG MIT IT-SICHERHEITSKENNZEICHEN DES BSI

Mit der feierlichen Übergabe am 4. Juli durch Joshu Wiebe, Referatsleiter im Bundesamt für Sicherheit in der Informationstechnik (BSI), hat OpenTalk einen Meilenstein erreicht: Als erste Videokonferenzlösung überhaupt darf sich OpenTalk mit dem IT-Sicherheitskennzeichen des BSI schmücken. Diese Auszeichnung unterstreiche das konsequente Engagement des Unternehmens für höchste Sicherheitsstandards und Datenschutz.

Die neue DIN SPEC 27008 bildet die Grundlage für das IT-Sicherheitskennzeichen und definiert Mindestanforderungen an IT-Produkte. Dazu gehören der Schutz der Benutzerdaten, ein angemessenes Update- und Schwachstellenmanagement, zeitgemäße Anmeldeverfahren, ein sicherer Rechenzentrumsbetrieb, aktuelle Verschlüsselungstechnologien sowie Transparenz und Kontrolle während der Videokonferenz. Das BSI prüft im Rahmen der Marktaufsicht über die gesamte Laufzeit des Kennzeichens anlassbezogen (stichprobenartig) und anlasslos (zum Beispiel bei Bekanntwerden von Schwachstellen), ob die Anforderungen erfüllt werden.

Die OpenTalk-Lösung zeichne sich durch viele Funktionen aus, die eine sichere und bequeme digitale Zusammenarbeit ermöglichen. Dazu zählen revisionssichere Abstimmungen, Multi-Moderatoren-Meetings, praktische Breakout-Räume sowie ein umfassendes Dashboard zur Konferenzplanung. Die Lösung basiere auf einer Open-Source-Architektur und vereine die 30-jährige Expertise der Heinlein Gruppe im Bereich freier und sicherer elektronischer Kommunikation. ■

TOOL ZUR ERKENNUNG VON SCHWACHSTELLEN AUS DER SICHT EINES HACKERS

KnowBe4 stellt BreachSim vor. Das kostenlose Tool ermöglicht Unternehmen die Identifizierung und Behebung von Netzwerk-Schwachstellen – und zwar aus der Sichtweise von Hackern. Mit BreachSim können Unternehmen Schwachstellen aufdecken, die für konventionelle Sicherheitsscans oft unsichtbar bleiben. Das Tool simuliert Angriffe und zeigt auf, wie Daten exfiltriert und welche Schwachstellen im Netzwerk dazu

ausgenutzt werden. Die gewonnenen Erkenntnisse erlauben es Unternehmen, ihre Cybersicherheitsdefizite gezielt zu stärken und ihre Mitarbeiter zu schulen, um als „menschliche Firewall" zu fungieren.

BreachSim arbeitet effizient und liefert in wenigen Minuten detaillierte Ergebnisse. Kompatibel mit Windows 10 oder höher sowie Windows Server 2016 oder höher, ermöglicht es eine umfassende Analyse potenzieller Datenexfiltrationen. So können Unternehmen schnell reagieren und ihre Systeme wirkungsvoll schützen. „Mit BreachSim geben wir Organisationen die Möglichkeit, ihre Netzwerke mit den Augen eines potenziellen Cyberangreifers zu sehen", sagt Stu Sjouwerman, CEO von KnowBe4. „Indem wir dies kostenlos anbieten, stellen wir sicher, dass Organisationen jeder Größe von diesen proaktiven Sicherheitsmaßnahmen profitieren können." ■

IT-SAFE: MICRO-RECHENZENTRUM MIT TÜVIT-ZERTIFIZIERUNG

Prior1 bietet mit dem IT-Safe eine hochsichere und zugleich flexible Lösung, die Unternehmen dabei unterstützt, ihre Daten zu schützen. Dieses TÜV-zertifizierte Micro-Rechenzentrum zeichnet sich durch seinen modularen Aufbau aus und lässt sich somit individuell an die spezifischen Bedürfnisse jedes Unternehmens anpassen.

Ob Feuer, Einbruch oder Umwelteinflüsse: Der IT-Safe bietet laut Hersteller zuverlässigen Schutz vor einer Vielzahl von physischen Bedrohungen. Die robuste Konstruktion und die Sicherheitstechnik sorgen dafür, dass die unternehmenskritische IT-Infrastruktur stets sicher verwahrt ist. Die unabhängige Zertifizierung nach EN 50600 durch den TÜVIT bestätigt den hohen Qualitätsstandard des IT-Safe und belegt die Einhaltung strenger Sicherheits- und Verfügbarkeitsanforderungen.

Der IT-Safe ist in verschiedenen Konfigurationen erhältlich. Vier Varianten mit unterschiedlichen Optionen für Kälte- und Stromversorgung bieten Unternehmen die Möglichkeit, die ideale Lösung für ihre Bedürfnisse zu wählen. Ob Einzelinstallation, 2er-Verkettung oder 3er-Verkettung: Der IT-Safe passt sich flexibel an die jeweilige Betriebsumgebung und die gewünschten Sicherheitsstandards an. Die skalierbare Lösung lässt sich jederzeit erweitern, um neuen Anforderungen gerecht zu werden. ■

DOKUMENTATION IM IT-GRUNDSCHUTZ: NEUE FAQS UND HILFSMITTEL

Die Dokumentation spielt eine zentrale Rolle für die Informationssicherheit. Mit ihr lassen sich Prozesse standardisieren, Informationen weitergeben und Beweise sichern. Um Unternehmen und Organisationen bei der Erstellung einer effektiven Dokumentation zu unterstützen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) FAQs und Hilfsmittel veröffentlicht.

Das Thema Dokumentation wird im IT-Grundschutz an verschiedensten Stellen sowie für unterschiedliche Zielgruppen behandelt. Bisher war jedoch oftmals nicht immer eindeutig beschrieben, wann etwas wie und für wen zu dokumentieren ist und welchen Zweck die jeweilige Dokumentation überhaupt erfüllen soll. Im Rahmen der Weiterentwicklung des IT-Grundschutzes stelle man nun FAQs zur Dokumentation zur Verfügung, die eine zentrale Einführung zum Thema im IT-Grundschutz bieten und auf die wesentlichsten Fragen eingehen. Die FAQs werden durch eine tabellarische Übersicht ergänzt, die eine Möglichkeit aufzeigt, welche Dokumente für welche Anforderungen aus den BSI-Standards und Bausteinen des IT-Grundschutz-Kompendiums erstellt werden sollten. Sie hat empfehlenden Charakter und ist nicht als verbindlich anzusehen, da es im Einzelfall sinnvoll sein kann, die Struktur und die Form an die eigene Situation anzupassen. ■

Bevor die Hilfsmittel in die BSI-Publikationen integriert werden, möchte das Amt Unternehmen und Organisationen um ihre Meinung bitten. Sie werden daher im Community-Draft-Format zur Verfügung gestellt und können kommentiert werden:

ENDE-ZU-ENDE-LÖSUNG FÜR SICHERE MOBILE KOMMUNIKATION

Mit dem VNCphone präsentiert der Schweizer Softwareentwickler VNC AG eine Lösung für die sichere mobile Kommunikation und Kollaboration. Das VNCphone vereint ein Mobiltelefon mit einem gehärteten Betriebssystem und vorinstallierten Anwendungen zu einem Komplettpaket. Der Markt für mobile Geräte und Lösungen sei aktuell von Anbietern dominiert, die in puncto Sicherheit fragwürdig sind, so das Schweizer Unternehmen. Sensible Daten werden demnach bei der Nutzung oft ungefragt und intransparent an unbekannte Empfänger weitergegeben. Das VNCphone setze dem ein Ende und bietet eine sichere Alternative.

VNC hat ein eigenes integriertes System entwickelt, das von der Hardware des Geräts bis hin zu den Anwendungen auf Applikationsebene reicht. Die Hardwarebasis bildet das in Deutschland produzierte Volla Phone, welches unter anderem Dual-Boot-fähig ist und somit den Nutzer zwischen VNClagoon OS, Ubuntu Touch und Google Android wählen lässt. Auf dem VNCphone ist der modulare Software-Stack VNClagoon bereits vorinstalliert. Apps wie VNCtalk, VNCmail, VNCproject und VNCtask können über die VNC-Website per Subskription freigeschaltet und sofort für die mobile Zusammenarbeit genutzt werden.

„Mit dem VNCphone steht endlich ein rundum sicheres Paket für die professionelle mobile Kommunikation und Kollaboration zur Verfügung", betont Andrea Wörrlein, Geschäftsführerin von VNC in Berlin und Verwaltungsrätin der VNC AG in Zug. „Es eignet sich ideal für den Einsatz in sicherheitsrelevanten Umgebungen wie etwa öffentlichen und staatlichen Einrichtungen, kritischen Infrastrukturen oder sicherheitssensiblen Unternehmen." ■

Der Software-Stack VNClagoon mit Apps wie VNCtalk ist auf dem VNCphone bereits vorinstalliert. (Quelle: VNC)

Ransomware-Analyse

HARDBIT 4.0 SCHLÜPFT MIT TARNKAPPE DURCH ANALYSEPROGRAMME

Ein perfider Verwandlungskünstler unter den Erpressungsschädlingen greift jetzt in IT-Systemen um sich. Was diesen HardBit-Ransomware-Ableger so brandgefährlich macht, ist seine Tarnkappe. Mit einem ausgeklügelten Verschleierungsmechanismus für Passwörter schlüpft er unbemerkt durch die Maschen der Analyseprogramme und erschwert die Identifizierung der Schadsoftware enorm.

Die HardBit-Ransomware hat sich in ihrer neuesten Version 4.0 ein dickes Fell zugelegt, wie Sicherheitsexperten von Cybereason jetzt herausfanden. Um die Analyse durch Malware-Jäger zu erschweren, schützt sich die Schadsoftware jetzt mit einem zusätzlichen Passwortschutz. „Die Passphrase muss während der Laufzeit eingegeben werden, damit die Ransomware ordnungsgemäß ausgeführt werden kann", so die Experten. „Zusätzliche Verschleierungsmechanismen erschweren darüber hinaus die Analyse."

HARTE BROCKEN: DIE HARDBIT-BANDE UND IHRE DOPPELTE ERPRESSUNG

Seit Oktober 2022 mischt die HardBit-Bande im Geschäft mit der Erpressungssoftware mit. Wie andere Gangster dieser Art setzen sie auf doppelte Erpressung, um ihre illegalen Gewinne zu maximieren.

Was die HardBit-Gruppe von anderen unterscheidet, ist ihre Vorgehensweise. Anders als die meisten Erpressergruppen, die ihre Opfer mit der Veröffentlichung gestohlener Daten auf einer „Datenleck-Seite" unter Druck setzen, betreiben die HardBit-Akteure keine solche Seite. Stattdessen verschärfen sie die Situation für ihre Opfer, indem sie mit weiteren Angriffen in naher Zukunft drohen. Die Kommunikation mit den Opfern läuft dabei über den Instant-Messaging-Dienst Tox ab.

WIE DIE HARDBIT-BANDE IHRE OPFER INS VISIER NIMMT

Wie genau die HardBit-Bande ihre Angriffe startet, ist noch unklar. Vermutet wird allerdings, dass sie Schwachstellen in RDP- und SMB-Diensten ausnutzen, um sich Zugang zu ihren Opfern zu verschaffen. Mit Werkzeugen wie Mimikatz und NLBrute stehlen sie dann Anmeldeinformationen und nutzen fortschrittliche Portscanner, um sich im Netzwerk zu bewegen. So erlangen sie Zugriff auf weitere Systeme.

„Sobald ein Opfer-Host kompromittiert wurde, wird die HardBit-Ransomware ausgeführt. Diese führt eine Reihe von Schritten aus, welche die Sicherheitslage des Hosts destabilisieren, bevor die Daten des Opfers verschlüsselt werden", so Varonis in einem technischen Bericht über HardBit 2.0 im vergangenen Jahr.

Für die Verschlüsselung selbst setzen die Angreifer auf bewährte Technik. Die HardBit-Ransomware enthält den bekannten Dateiinfektionsvirus Neshta, der in der Vergangenheit auch für die Verbreitung der Big-Head-Ransomware verwendet wurde.

HINTERLISTIGER EINDRINGLING

HardBit ist raffiniert darauf ausgelegt, sich tief ins System einzuschleichen und maximale Kontrolle zu erlangen. Zunächst schaltet es den Microsoft Defender Antivirus aus, schwächt so die Abwehr des Systems und blockiert gleichzeitig die Systemwiederherstellung – ein cleverer Schachzug, um jegliche Gegenmaßnahmen zu unterbinden. Anschließend geht HardBit zur Tat über: Dateien werden verschlüsselt, wichtige Symbole und das Hintergrundbild auf dem Desktop werden verändert sowie die Daten-

trägerbezeichnung in den unheilvollen Namen „Locked by HardBit" umgewandelt. So hinterlässt die Schadsoftware ihre digitale Visitenkarte und macht den Ernst der Lage deutlich.

Die Ransomware gibt es als Befehlszeilen- oder GUI-Version. Für die Ausführung ist eine Autorisierungs-ID erforderlich. Die GUI-Variante unterstützt auch einen Wiper-Modus, der Dateien unwiderruflich löscht. „Nach Eingabe der entschlüsselten Autorisierungs-ID fordert HardBit zur Eingabe eines Verschlüsselungsschlüssels auf und beginnt mit dem Verschlüsseln der Dateien auf dem Zielcomputer", erklärt Cybereason. „Der Wiper-Modus muss von der HardBit-Gruppe aktiviert werden und ist wahrscheinlich eine zusätzliche Funktion, welche die Betreiber erwerben müssen. Wenn die Betreiber den Wiper-Modus benötigen, müssen sie die Datei hard.txt bereitstellen, eine optionale Konfigurationsdatei der HardBit-Binärdatei, die eine Autorisierungs-ID zur Aktivierung des Wiper-Modus enthält."

Tactics	HardBit 2.0	HardBit 3.0	HardBit 4.0
Disable Windows Defender	✓	✓	✓
Inhibit System Recovery	✓	✓	✓
Packed by Neshta			✓
Password protected			✓
Stop services	✓	✓	✓
Support HardBit GUI version		✓	✓
Support wiper mode		✓	✓
Use configuration file hard.txt		✓	✓
Use "Ryan-_-Borland_Protector Cracked v10"-packer	✓	✓	✓

Tabelle 1: Die Entwicklung der HardBit-Versionen

RANSOMWARE-WELLE ROLLT UNGEBREMST WEITER

Die Bedrohung durch Ransomware-Angriffe bleibt auch im Jahr 2024 hoch. Im ersten Quartal dieses Jahres verzeichneten Experten 962 Angriffe – ein besorgniserregender Anstieg im Vergleich zu den 886 Angriffen im Vorjahr. Unter den am häufigsten verwendeten Ransomware-Familien im ersten Quartal 2024 finden sich laut Symantec LockBit, Akira und BlackSuit.

Der Bericht „2024 Unit 42 Incident Response" von Palo Alto Networks offenbart zudem, dass sich die Zeitspanne zwischen der Kompromittierung eines Systems und der Exfiltration von Daten dramatisch verkürzt. Während im Jahr 2021 noch durchschnittlich neun Tage vergingen, schrumpfte diese Zeitspanne im letzten Jahr auf nur zwei Tage. In fast der Hälfte (45 Prozent) der Fälle im Jahr 2024 dauerte der Datenraub sogar nur knapp 24 Stunden.

„Die verfügbaren Daten deuten darauf hin, dass die Ausnutzung bekannter Schwachstellen in öffentlich zugänglichen Anwendungen weiterhin der Hauptvektor für Ransomware-Angriffe ist", so das zu Broadcom gehörende Unternehmen Symantec. „Bring Your Own Vulnerable Driver (BYOVD) bleibt eine beliebte Taktik von Ransomware-Gruppen, insbesondere um Sicherheitslösungen zu deaktivieren." BYOVD ist eine Angriffsmethode, bei der Angreifer bewusst eine bekannte, anfällige Treibersoftware (Driver) verwenden, um Sicherheitsmechanismen auf einem Zielsystem zu umgehen. Diese Technik funktioniert, indem der Angreifer einen Treiber, der legitime Funktionen hat, aber bekannte Schwachstellen enthält, in das Zielsystem einbringt und ausnutzt. ■ *THN/SF*

Defense in Depth

RANSOMWARE-ANGRIFFE MIT ZERO-TRUST-SEGMENTIERUNG EINDÄMMEN

Ransomware-Angriffe sind eine große Gefahr. Die gute Nachricht ist: Sie brauchen Zeit. Die Angreifer müssen sich erst in der IT-Umgebung eines Unternehmens ausbreiten, sensible Daten finden und Zugriffsrechte sichern, bevor sie umfassend Daten verschlüsseln können. Mit Zero-Trust-Segmentierung etablieren Unternehmen „Defense in Depth" und verhindern so laterale Bewegungen von Cyberangreifern sowie eine ungehinderte Ausbreitung von Ransomware.

Laut dem Verizon Data Breach Investigations Report (DBIR) 2024 ist Ransomware nach wie vor eine zentrale Herausforderung für die IT-Sicherheit. Bei rund einem Drittel aller Sicherheitsverletzungen weltweit kommt Ransomware zum Einsatz. In Deutschland waren laut einer Cybereason Ransomware-Studie 63 Prozent der befragten Unternehmen in den letzten 24 Monaten von mehr als einem Ransomware-Angriff betroffen. Dazu verdeutlicht der Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI), dass von Ransomware derzeit die größte Bedrohung ausgeht.

Ransomware-Angriffe verursachen nicht nur enorme wirtschaftliche Schäden, sondern können ganze Wertschöpfungsketten nachhaltig beeinträchtigen. Wenn große Teile der IT-Infrastruktur verschlüsselt werden, sind Unternehmen oft gezwungen, ihren gesamten Betrieb einzustellen oder ihre IT-Systeme komplett vom Netz zu nehmen. Die Folgen reichen von Produktionsausfällen über Reputationsschäden bis hin zu langfristigen finanziellen Einbußen.

DER ABLAUF EINES RANSOMWARE-ANGRIFFS

Um Ransomware effektiv zu bekämpfen, ist es wichtig, den Ablauf eines Angriffs zu verstehen. Entgegen der landläufigen Meinung erfolgt ein Ransomware-Angriff nicht in wenigen Minuten, sondern erstreckt sich oft über Tage, Wochen oder sogar Monate. Der Prozess lässt sich in mehrere Phasen unterteilen:

1. **Initiale Kompromittierung:** Ransomware infiltriert zunächst ein unzureichend geschütztes Asset. Dies kann ein Endpunkt, eine Anwendung oder ein Workload mit einer offenen Verbindung zum Internet sein. Diese Assets sind oft weniger abgesichert, da sie nicht als wichtig wahrgenommen werden oder ihre Anfälligkeit dem Unternehmen nicht bewusst ist.

2. **Laterale Bewegung:** Nach der ersten Infiltrierung erkunden Angreifer das Netzwerk und bewegen sich dabei seitlich durch dieses. Sie nutzen verschiedene Techniken, um unentdeckt zu bleiben und sich Zugang zu wichtigen Systemen und Netzwerken zu verschaffen.

3. **Datenexfiltration:** In dieser Phase sammeln die Cyberangreifer sensible Daten, die später als zusätzliches Druckmittel verwendet werden können.

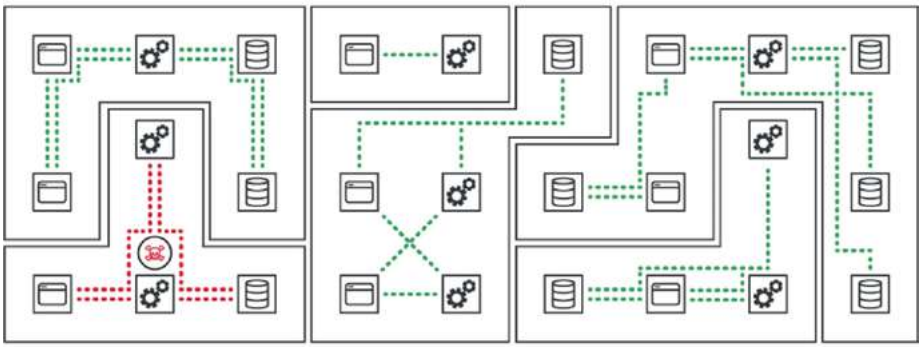
4. **Eskalation von Privilegien:** Die Angreifer versuchen, Administratorrechte oder andere privilegierte Zugänge zu erlangen, um weitreichenden Zugriff auf Systeme zu erhalten.

5. **Verschlüsselung:** Sobald die Angreifer genügend Kontrolle über die Systeme haben, beginnen sie mit der Verschlüsselung wichtiger Daten und Systeme.

6. **Erpressung:** Abschließend fordern die Cyberkriminellen ein Lösegeld für die Entschlüsselung der Daten und drohen oft mit der Veröffentlichung sensibler Informationen.

GRENZEN KONVENTIONELLER SICHERHEITSLÖSUNGEN

Viele Unternehmen verlassen sich beim Schutz ihrer Assets auf etablierte Sicherheitslösungen wie Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR) sowie Netzwerk-Monitoring- und Observability-Tools, um Angriffe zu erkennen und abzuwehren. Diese Lösungen sind wichtige Bestandteile einer umfassenden Sicherheitsstrategie und decken die Funktionen „Erkennen (Detect)" und „Reagieren (Respond)" des NIST Cybersecurity Frameworks ab. Das Framework ist ein ganzheitlicher Ansatz aus Anleitungen, Richtlinien und Best Practices für Organisationen zur Verbesserung des Risikomanagements für Informationssicherheit, der von der US-amerikanischen Bundesbehörde National Institute of Standards



Durch Zero-Trust-Segmentierung, auch als Mikrosegmentierung bekannt, wird die Angriffsfläche minimiert. (Bild: Illumio)

and Technology veröffentlicht wurde. Konventionelle Sicherheitslösungen erkennen verdächtige Aktivitäten oder direkte Angriffe auf Endpunkte, Server, Cloud-Workloads und Netzwerkverkehr und reagieren, indem sie Warnungen ausgeben, Antiviren-Tools aktivieren, Dateien löschen oder in Quarantäne stellen.

Allerdings bieten sie keinen hundertprozentigen Schutz. Angriffe können übersehen werden oder aufgrund von Software-Schwachstellen, Zero-Day-Exploits oder neu entwickelten Angriffsmethoden oft lange Zeit unentdeckt bleiben. Außerdem bieten sie keinen umfassenden Schutz vor der initialen Kompromittierung und der anschließenden lateralen Bewegung von Angreifern im Netzwerk. Stattdessen sind diese Ansätze oft reaktiv und greifen erst ein, wenn ein Angriff bereits im Gange ist. Ein einziger unentdeckter Angriffsversuch kann daher schwerwiegende Folgen haben.

EFFEKTIVER SCHUTZ DURCH SEGMENTIERUNG

Um die Auswirkungen von Ransomware-Angriffen zu minimieren, müssen Unternehmen einen umfassenden Überblick über ihre IT-Umgebung gewinnen, ihre Widerstandsfähigkeit stärken und kritische Assets segmentieren. Eine Lösung, die diese Anforderungen erfüllt und zudem den Richtlinien des NIST-Frameworks entspricht, ist die Zero-Trust-Segmentierung (ZTS), eine grundlegende Komponente einer Zero-Trust-Strategie.

Der Zero-Trust-Ansatz basiert auf der Annahme, dass keinem Benutzer oder Gerät, unabhängig davon, ob es sich innerhalb oder außerhalb des Netzwerks befindet, automatisch vertraut wird. Somit wird unbefugter Zugriff auf sensible Daten verhindert. ZTS minimiert die Angriffsfläche, indem sie Netzwerke in isolierte Bereiche unterteilt. Diese Segmente lassen nur den notwendigen Datenverkehr zu, der für geschäftskritische Prozesse erforderlich ist. Jeglicher andere Verkehr wird standardmäßig blockiert. Die Vorteile von Zero-Trust-Segmentierung im Kampf gegen Ransomware sind:

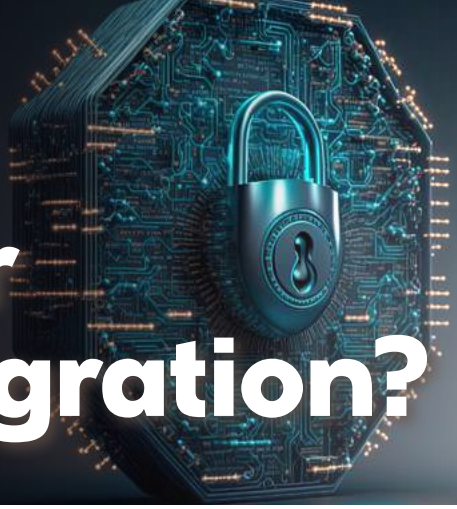
- **Minimierung der Angriffsfläche:** ZTS reduziert die Anzahl der potenziellen Angriffspunkte, indem es den Zugriff auf sensible Ressourcen strikt kontrolliert und nur autorisierten Entitäten gewährt.
- **Einschränkung lateraler Bewegungen:** Durch die Segmentierung des Netzwerks wird die Bewegungsfreiheit von Angreifern erheblich eingeschränkt. Selbst wenn ein System kompromittiert wird, kann sich die Bedrohung nicht ungehindert im gesamten Netzwerk ausbreiten.
- **Verbessertes Monitoring:** Durch die Segmentierung wird der Netzwerkverkehr übersichtlicher, was die Erkennung verdächtiger Aktivitäten erleichtert.
- **Granulare Kontrolle:** Sicherheitsteams können präzise Richtlinien erstellen und maßgeschneiderte Sicherheitsvorkehrungen durchsetzen.
- **Aufbau von Cyberresilienz:** Cyberresilienz ermöglicht es Unternehmen, ihre Kernfunktionen aufrechtzuerhalten, auch wenn Teile der IT-Infrastruktur bereits kompromittiert sind. Im Fall eines erfolgreichen Angriffs ermöglicht Segmentierung eine gezielte Isolierung betroffener Systeme und eine schnelle Wiederherstellung.
- **Unterstützung bei der Einhaltung von Compliance-Vorschriften:** Segmentierung hilft Unternehmen dabei, die regulatorischen Anforderungen von geltenden Vorschriften wie NIS-2, DORA und DSGVO zu erfüllen.

AUFBAU VON CYBER-RESILIENZ DURCH ZERO TRUST

Perimeter- und rein reaktive Sicherheitslösungen allein reichen nicht aus, um Unternehmen effektiv vor Ransomware zu schützen. Moderne Strategien wie Zero Trust, die das implizite Vertrauen in die IT-Umgebung reduzieren, sind entscheidend für die Stärkung der Cyberresilienz, und Ansätze wie ZTS sind unverzichtbar, um einen umfassenden, kontinuierlichen und proaktiven Schutz der Unternehmens-IT zu gewährleisten. Ransomware-Simulationen von Bishop Fox, einem Anbieter von Penetrationstests, zeigen, dass ZTS Ransomware in weniger als zehn Minuten neutralisieren kann und damit vier Mal schneller ist als Abwehrversuche, die allein auf EDR basieren.

Ransomware bleibt eine anhaltende Bedrohung, daher müssen die Eindämmung von Sicherheitsverletzungen und die Begrenzung des Aktionsradius von Angriffen höchste Priorität haben. Durch die Implementierung von Segmentierung als Teil einer ganzheitlichen Zero-Trust-Strategie können Unternehmen ihre Widerstandsfähigkeit gegen Ransomware und andere Cyberbedrohungen sofort stärken. ■

PAUL BAUER
ist Regional Sales Director bei Illumio.



PCert® – Bereit für Post-Quantum Migration?

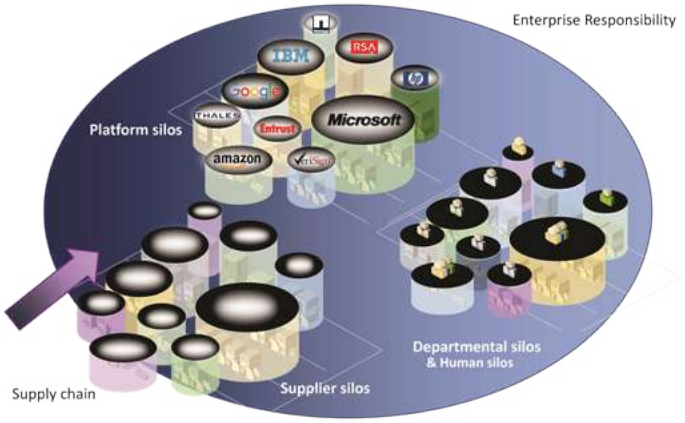
Ein durch Zertifikate verursachter Ausfall kostet Unternehmen circa drei bis fünf Millionen US-Dollar, sie treten drei bis fünf Mal pro Jahr auf.

Stellen Sie sich vor, Sie könnten einen davon verhindern! Oder alle? **Verstößt Ihr Unternehmen gegen Compliance-Anforderungen?** Möchten Sie dies überprüfen? **2035 ist Ihre heutige Kryptografie obsolet.** Wie bereiten Sie sich darauf vor?

Die Enterprise Plattform PCert® von Data-Warehouse ist die Lösung:

Die Anforderungen durch NIS-2 (DORA, SOX, FedRAMP), existierende, bisher unbekannte Abhängigkeiten in digitalen Kernsystemen aufzudecken und zu managen, ist die umfassende Herausforderung und Verantwortung der C-Suites von heute. Ohne automatisierte Methoden wie PCert® mit mehr als zehn Jahren Produkterfahrung ist dies nicht möglich. Wir unterstützen Ihr Unternehmen, Ihre Zulieferer und Kunden beim Aufbau eines kryptografischen Inventars, das es Ihnen ermöglicht, mit einer transparenten und minimal-invasiven Integration die nächste Sicherheitsstufe zu erreichen und Ihre bestehende Produkt- und Netzwerkstruktur mit Automatisierung und neuen Funktionen zu erweitern: Auffinden der Assets, Migration zu Post-Quantum, Krypto-Agilität, Auditierung Ihrer Unternehmenssicherheit, Identifizierung von Risiken in Produkten und Lieferketten, CBOM und SBOM, Sicherstellung der Produktkonformität und Automatisierung Ihrer Verwaltungsprozesse – zum Beispiel Handhabung von Zertifikaten oder Sicherung Ihrer Betriebs- und Geschäftskontinuität – sowie Reduzierung der Arbeitsbelastung Ihrer Verwaltungsteams, unabhängig von Ihrem Geschäftszweck, dem Alter Ihrer Infrastruktur und deren Betriebskonzept.

Zweifel? Das NCCOE Lab von NIST und MITRE setzen PCert® bereits ein und nutzen die Erkenntnisse, um die neuen Standards für Post-Quantum Migration und Att&ck® zu definieren.



Ihre Verantwortung und Herausforderung: Beseitigen Sie Ihre kryptografischen Silos, erstellen Sie Ihr kryptografisches Inventar und untersuchen Sie Ihre Software-Lieferketten.

Der ganzheitliche Ansatz von PCert® ermöglicht die Untersuchung, Entdeckung, Bewertung, Automatisierung der Verwaltung eines sehr breiten Spektrums von IT-Vertrauensbeziehungen, unabhängig davon, ob es sich um Webdienste, Produkte oder Geräte handelt. Der Ansatz von PCert® besteht darin, jedes Zertifikat, jeden Schlüssel und jeden Schlüsselspeicher in jedem Gerät zu identifizieren, um Schwachstellen und menschliche oder systematische Fehler zu erkennen, Infrastruktur-, Programm- und Produktprobleme zu vermeiden und den Übergang zu neuen Technologien (beispielsweise Post-Quantum-Technologien) vorzubereiten oder durchzuführen. Die Vorteile von PCert® sind nicht nur die vollständige Transparenz Ihrer technischen Umgebung und Ihrer Public Key Infrastructure (PKI), sondern auch die Verbesserung Ihrer Cybersicherheit sowie die Einbeziehung Ihrer Lieferkette und der Nachweis der Einhaltung verschiedener Standards mit reduziertem Aufwand.

Ihre Verantwortung und Herausforderung: Integrieren Sie die neuen Compliance-Anforderungen in Ihre Unternehmensführung

PCert® ermöglicht mit seinen flexiblen APIs und Agenten eine nahtlose Integration und einen optimalen Informationsaustausch in der Infrastruktur des Kunden, unabhängig vom Schnittstellentyp wie XML, JSON, REST, CSV mit maximalem Nutzen innerhalb Ihrer Prozesse und unterstützt SIEM, SOC, ITIL-Prozesse – unabhängig davon, ob On Premises, Cloud oder Hybrid. ■

Sprechen Sie mit uns, um Ihre Strategie zu optimieren.

PCert®-Testmöglichkeit für US-Unternehmen/Behörden
im Post-Quantum Migration Lab bei NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Data-Warehouse GmbH
Beethovenstraße 33-35
85521 Ottobrunn
E-Mail: info@dwh.gmbh
www.dwh.info

Mehr dazu hier

Data-Warehouse GmbH

Bild: 2rogan - stock.adobe.com

OT-Sicherheit:

WIE DIE ANGREIFER-SICHT BEIM SCHUTZ DES UNTERNEHMENS HILFT

Unternehmen investieren viel Zeit und Aufwand in den Aufbau einer Sicherheitsarchitektur für ihre industrielle IT. Trotzdem kommt es immer wieder zu erfolgreichen Angriffen. Wie kann das sein? Dieser Frage und einem möglichen Lösungsansatz geht der Autor im folgenden Beitrag nach.

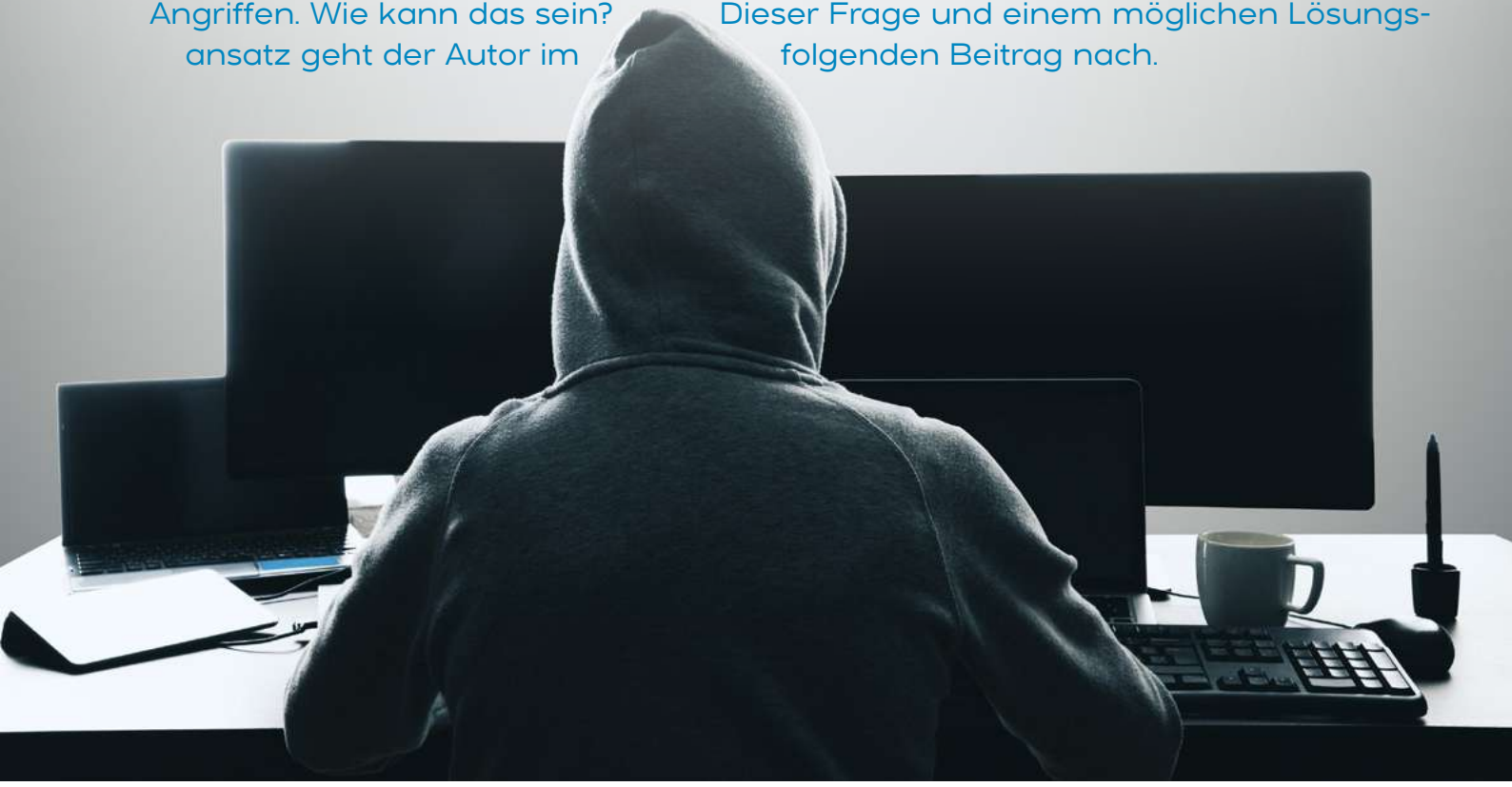


Bild: Who is Danny - stock.adobe.com

Nutzt Ihr Unternehmen Automatisierungstechnik? Sie sind Teil von Industrie 4.0 oder wollen es werden? Predictive Maintenance oder Remote Access gehören zu Ihrem Tagesgeschäft? Dann haben Sie hoffentlich nicht nur von Operational-Technology-(OT)-Security gehört, sondern sind bereits aktiv an der Analyse und Umsetzung von Maßnahmen beteiligt. Dafür gibt es eine Vielzahl von Frameworks und Best Practices, die Firmen bei der Auswahl von Maßnahmen helfen.

Darüber hinaus macht es jedoch zusätzlich Sinn, sich das eigene Unternehmen aus der Sicht eines Angreifers anzusehen. Um dieses Vorgehen zu verdeutlichen, stellen wir einige Beispiele aus der Praxis vor:

Beispiel 1: „Wir haben Policies, Procedures und diverse Guidelines im Unternehmen, wir sind sicher!"

Zuerst einmal ist dies ein guter Schritt in die richtige Richtung, denn diese Dokumentation hilft am Ende bei einem strukturierten und effizienten Vorgehen. Wichtig ist aber zu wissen,

dass die Dokumente selbst einen Angreifer nicht abwehren. Nur weil man auf mehreren hundert Seiten beschreibt, wie der Soll-Zustand aussehen müsste, ist man noch kein bisschen sicherer geworden. Entscheidend ist hier, dass Policies, Procedures und Guidelines nicht nur erstellt, sondern auch im Unternehmen kommuniziert, implementiert und gegebenenfalls trainiert werden.

Beispiel 2: „Tool xyz sieht super aus und wird dafür sorgen, dass wir sicher sind!"

Das ist leider ein Klassiker, dem man immer wieder über den Weg läuft. Seien es vollmundige Werbeprospekte voller Buzzwords bestenfalls noch in Kombination mit KI oder die Versprechungen, dass man unbedingt ein Tool benötigt, um automatisiert compliant und sicher zu werden. Klingt erstmal verlockend, aber ist wirklich klar, welche Herausforderung das Tool lösen soll oder müssen die passenden Herausforderungen für das Tool erst noch entdeckt werden?

Beispielsweise macht es wenig Sinn, aufwendig Network-Intrusion-Detection-Systeme auszurollen, wenn die Schalt- und Serverräume sowie die zugehörigen Gebäude nicht grundlegend abgeschlossen/abgesichert sind und auch die Racks selbst keine Schließung aufweisen, da hier leicht eine physische Manipulation vorgenommen werden kann, die ein solches System dann nicht erkennt.

Es ist wichtig, nicht direkt mit der Auswahl von Tools zu beginnen, sondern sich zunächst Gedanken über die zu lösenden Herausforderungen zu machen. Darauf aufbauend können kompakte Anforderungen an eine Lösung erarbeitet werden und erst dann sollte damit begonnen werden, mögliche Tools neutral gegen diese Anforderungen zu evaluieren. Klassisches Requirements Engineering also. Andernfalls läuft man Gefahr, eine Lösung für ein nicht vorhandenes/nicht relevantes Problem zu beschaffen oder nur einen Teil der eigentlichen Herausforderungen abzudecken.

Beispiel 3: „Wir haben eine high-end technische Absicherung, wir sind sicher!"

Das ist schon einmal sehr gut! Wichtig ist hierbei, nicht zu vergessen, dass Sicherheit drei Dimensionen hat: Menschen, Prozesse und Technologie. Diese müssen nicht alle auf dem gleichen Niveau sein, aber es sollte zumindest sichergestellt sein, dass keine der Dimensionen übersehen wird. Sonst kann es passieren, dass beispielsweise ein Mitarbeiter im Rahmen von Social Engineering Informationen verrät, die zur Kompromittierung von Systemen führen.

Beispiel 4: „Wir haben unser aktuelles Security-Programm abgeschlossen, wir sind jetzt sicher!"

Zumindest zum Zeitpunkt des Abschlusses ist man sicher, aber sobald Unternehmen meinen, man könne sich nun entspannt zurücklehnen, ist der sichere Zustand sehr schnell wieder dahin, da unter anderem Schwachstellen regelmäßig bearbeitet werden müssen. Treffend ist hier auch die Aussage von Bruce Schneier: „Security is a process, not a product".

Beispiel 5: „Wir brauchen kein führendes Tool, unser System/Netz ist so einfach, das Tool bauen wir uns selbst und dann sind wir sicher!"

Es mag verlockend klingen, wenn ein findiger Mitarbeiter auf die Idee kommt, dass man eine Log-Analyse mit Python auch selbst entwickeln kann und sich in diesem Fall die Ressourcen für eine Security-Information-and-Event-Management-(SIEM)-Software sparen kann. Letztendlich steckt der Teufel aber wieder im Detail und nicht umsonst beschäftigen Unternehmen wie SPLUNK ein entsprechend großes Entwicklerteam. Aus Angreifersicht hat die eigenentwickelte Lösung jedenfalls einen Vorteil: Sie durchläuft vermutlich keine entsprechend strengen Tests wie kommerzielle Software und kann daher eventuell sogar als Ausgangspunkt für den einen oder anderen Angriff nützlich sein.

Beispiel 6: „Unsere Systeme sind komplett isoliert! Wir können nicht angegriffen werden und sind sicher!"

Kann man ein System vollständig isolieren, um Sicherheit zu gewährleisten? In der Theorie mag das möglich sein, wenn man die Kabelverbindungen anschließend einbetoniert und jegliche Ports des Systems mit Heißkleber unbrauchbar macht und noch dazu sicherstellt, dass Peripheriegeräte nicht gewechselt werden können. Ansonsten ist das System zwar in einem isolierten Netzwerk, aber es gibt diverse Schnittstellen, über die sich ein Angreifer Zugriff verschaffen könnte. Sei es über einen infizierten USB-Datenträger oder auch über das Erstellen eines zusätzlichen Ports auf einem Netzwerkkabel.

Sobald ein unbefugter Zugriff auf das System oder Teile des Systems nicht ausgeschlossen werden kann oder sobald ein Datentransfer mit externen Systemen erfolgt, kann man nicht mehr von einer Sicherheit durch Isolation ausgehen. Darüber hinaus gibt es noch verschiedene Untersuchungen zu Side-Channel-Attacks, die nach einer initialen Kompromittierung des Systems auch zur Kommunikation mit Systemen außerhalb des isolierten Netzes genutzt werden können.

OFFENSIVE SECURITY ZUR VERBESSERUNG DER ABSICHERUNG?

Typischerweise verfügen Unternehmen über Teams, die auf der Basis von Frameworks die Absicherung des Betriebs vornehmen. Durch die reine Fokussierung auf den defensiven Aspekt kann jedoch schnell eine Lücke zur Realität entstehen, da man die „dunkle" Seite nicht kennt beziehungsweise individuelle Schwachstellen übersieht. Einige Beispiele wurden bereits vorgestellt.

Um das zu verbessern, bietet es sich an, mindestens einen Experten für Offensive Security / Red Teaming im Sicherheitsteam zu haben. Speziell im OT-Umfeld kann es zusätzlich hilfreich sein, wenn diese Person einen Hang zum Thema physische Sicherheit hat. Alternativ kann man auch unterstützend einen Experten aus dem Bereich Objektschutz hinzuziehen. So kann das Team bestehend aus offensiven und defensiven Experten das Unternehmen oder einzelne Standorte mit dem Blick eines Angreifers betrachten. Die Offensivexperten entwerfen Pläne, wie man die existierenden Maßnahmen überwinden kann, auf deren Grundlage können anschließend die Schutzmaßnahmen optimiert werden.

In der praktischen Umsetzung empfiehlt es sich, die Standorte regelmäßigen Bewertungen durch das (erweiterte) Sicherheitsteam zu unterziehen, um zu analysieren, wie gut die definierten Maßnahmen umgesetzt werden und welche Schwachstellen gegebenenfalls vorhanden sind und behoben werden müssen. Auch können durch die regelmäßigen Prüfungen etwaige

Fehlkonfigurationen, die bei Wartungen oder Umbauten auftreten, erkannt und anschließend behoben werden.

ERSTE HILFE

Der Aufbau eines entsprechenden (erweiterten) Sicherheitsteams ist sicherlich nicht von heute auf morgen möglich. Im Rahmen von Audits zeigen sich jedoch immer wieder Punkte, die in vielen Betrieben vernachlässigt werden. Diese gilt es zu schließen:

1. **Serverracks/Schaltschränke sind nicht verschlossen beziehungsweise haben kein Schloss.**
   Sofern der zugehörige Raum entsprechend gesichert ist und sich nicht unterschiedliche Gewerke (z. B. IT, Leittechnik, TK) im gleichen Raum befinden und von verschiedenen Firmen betreut werden, kann dies akzeptabel sein. Ansonsten empfiehlt es sich, eine Schließung pro Gewerk einzuführen, um „unabsichtliche" Änderungen weitgehend auszuschließen.

2. **Schaltschränke verwenden die Hersteller-Standardschließung mit Vierkant-Schlüssel oder ähnlichem.**
   Siehe Punkt 1. Anderenfalls sollte über eine Nachrüstung/Umrüstung nachgedacht werden. Die gängigen Schrankhersteller (unter anderem Rittal) haben mittlerweile selbst für ältere Modelle Umrüstkits im Angebot, die sogar den Einbau von elektronischen Schließsystem unterstützen.

3. **Schlüssel stecken in den Schlössern der Schränke beziehungsweise hängen frei zugänglich im Schaltraum.**
   Hier kann ein einfacher Schlüsselkasten Abhilfe schaffen – am besten in Kombination mit dem gleichen Schließsystem, das auch für die Türen im Gebäude verwendet wird. So ist die Usability gewährleistet. Ansonsten ist natürlich die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter entscheidend, damit sie verstehen, wie wichtig sie für die Cybersicherheit des Unternehmens sind.

4. **Passwörter stehen auf Zetteln/Post-its am Gerät (immer noch).**
   Auch hier kann die Nutzung einer abschließbaren Box mit Passwörtern helfen. Am besten ist es natürlich, überhaupt keine schriftlichen Passwortlisten zu haben. Ansonsten kann auch hier eine Sensibilisierung der Mitarbeitenden hilfreich sein.

5. **USB-Lizenz Dongles hängen außen am Gerät.**
   Um den Verlust oder Diebstahl oder auch die anderweitige Nutzung des Ports zu verhindern, sollten interne USB-Ports genutzt werden und die äußeren Ports durch Port-Blocker verschlossen werden.

6. **Netzwerkports in Lagerhallen werden nicht genutzt, sind aber aktiv geschaltet.**
   Die Ports sollten regelmäßig überprüft und bei Nichtbenutzung deaktiviert werden. Dies kann zum Beispiel in Zusammenarbeit mit dem Netzwerkteam geschehen, das regelmäßig überprüft, welche Ports ungenutzt sind und diese dann am Switch deaktiviert. Alternativ hilft auch hier die Sensibilisierung, damit die Beschäftigten verdächtige Aktivitäten in der Lagerhalle melden und nicht ignorieren.

7. **Nach Umbaumaßnahmen (z. B. Verlegung eines Control Rooms) sind die alten Netzwerkports noch immer auf das Anlagennetz geschaltet.**
   Man sollte sich nicht darauf verlassen, dass dies bereits „jemand" getan hat. Stattdessen sollten die Änderungen nach den entsprechenden Änderungen verifiziert und validiert werden. Abhängig von der Kritikalität des Systems sollte diese Überprüfung durch einen unabhängigen Dritten erfolgen.

8. **IT-Geräte werden beim Betreten des Geländes erfasst, aber beim Verlassen wird nicht kontrolliert, ob man die gleichen oder nur diese Geräte mitführt.**
   Auf diese Weise können Geräte/Daten beliebig extrahiert werden, daher sollte das betroffene Personal sensibilisiert werden, die Geräte detailliert zu erfassen, die Seriennummer zu dokumentieren und gegebenenfalls auch Ports an den Geräten für die Nutzung zu sperren.

9. **Fehlende Sicherheitspatches (das kann selbst bei neuen Anlagen vorkommen, sofern kein Passus in den Vertrag aufgenommen wurde)**
   Hier bietet es sich an, ein kurzes Dokument mit ergänzenden Vertragsbedingungen zu erstellen, das die wichtigsten Punkte zur IT-/OT-Sicherheit zusammenfasst. Dieses Dokument wird mit dem Einkauf abgestimmt und dann anschließend bei jeder Beschaffung in die Vertragsdokumente ergänzt.

10. **Geringe Security Awareness des Personals**
    Je nach Sensibilisierung des Personals kann es vorkommen, dass „falsche" Techniker in Gebäude gelassen werden oder dass es niemanden interessiert, wenn Unbekannte in Lagerhallen herumlaufen und Laptops an Geräte anschließen. Hier sollte man auf eine möglichst permanente Sensibilisierung der Mitarbeitenden achten.

FAZIT

Unternehmen sollten neben technischen und prozessualen Maßnahmen auch die Perspektive eines Angreifers einnehmen, um ihre OT-Sicherheit zu verbessern. Denn die Angreifersicht ist ein wertvolles Werkzeug, um Schwachstellen zu identifizieren und durch geeignete Schritte zu schließen. Darüber hinaus sind es aber auch oft die einfachen Dinge, die die Sicherheit bereits erheblich verbessern können. ■

CHRISTIAN SCHLEHUBER (CISSP, GICSP, C|EH)
ist Geschäftsführer/Managing Director bei Cybershield.

Schlüssel zur Erfüllung neuer IT-Sicherheitsanforderungen

WARUM UNTERNEHMEN EIN ISMS BRAUCHEN

Die Implementierung eines Informationssicherheits-Managementsystems (ISMS) ist für viele Unternehmen heute unerlässlich, um die zahlreichen neuen Gesetze im Bereich der Cybersicherheit zu erfüllen. Unser Autor gibt einen kurzen Überblick über die gesetzlichen Anforderungen und beschreibt die wichtigsten Vorteile eines ISMS.

In den letzten Jahren haben zahlreiche neue gesetzliche Regelungen zur IT-Sicherheit Organisationen vor erhebliche Herausforderungen gestellt. Diese Gesetze fordern umfassende Maßnahmen zur Sicherung ihrer IT-Infrastruktur und Daten. Angesichts der wachsenden Anforderungen bietet sich die Einführung eines Informationssicherheits-Managementsystems (ISMS) an. Ein ISMS hilft nicht nur dabei, die gesetzlichen Vorgaben zu erfüllen, sondern trägt auch zur Verbesserung der allgemeinen Sicherheitslage eines Unternehmens bei. Im Folgenden werden einige der wichtigsten Gesetze zur IT-Sicherheit vorgestellt:

NEUE GESETZLICHE REGELUNGEN ZUR IT-SICHERHEIT

- **Network Information Security Directive (NIS-2):** Die NIS-2-Richtlinie muss bis zum 17. Oktober 2024 von den nationalen Gesetzgebern der EU-Mitgliedstaaten umgesetzt werden. Sie erweitert den Anwendungsbereich der ursprünglichen NIS-Richtlinie von 2016 und legt strengere Sicherheitsanforderungen für Betreiber wesentlicher und Anbieter digitaler Dienste fest. Betroffene Unternehmen müssen angemessene technische und organisatorische Maßnahmen ergreifen, um ihre Netzwerke und Informationssicherheitssysteme zu schützen. Die NIS-2-Richtlinie umfasst zudem auch erweiterte Meldepflichten bei Sicherheitsvorfällen sowie strengere Sanktionen bei Verstößen.

- **Digital Operational Resilience Act (DORA):** Der Digital Operational Resilience Act konzentriert sich auf die Stärkung der operationellen Resilienz im Finanzsektor. Finanzunternehmen werden verpflichtet, robuste Systeme und Prozesse zu implementieren, um sicherzustellen, dass sie gegenüber Cyberangriffen und anderen IT-bezogenen Störungen widerstandsfähiger sind. Dies umfasst regelmäßige Tests und Bewertungen der IT-Sicherheitsmaßnahmen sowie die Erstellung von Notfallplänen und Krisenübungen. Die in der Verordnung niedergelegten Pflichten treffen die betroffenen Stellen ab dem 17. Januar 2025.

- **Critical Entities Resilience Directive (CER-Richtlinie):** Die CER-Richtlinie, die parallel zur NIS-2-Richtlinie im Januar 2023 in Kraft trat und durch die Bundesregierung bis Oktober 2024 umgesetzt werden muss, richtet sich an die Betreiber kritischer Infrastrukturen. Sie verlangt von diesen Unternehmen, umfassende Risikoanalysen durchzuführen und geeignete Sicherheitsmaßnahmen zu implementieren, um ihre Widerstandsfähigkeit

gegen eine Reihe von Bedrohungen wie Naturkatastrophen, Terroranschläge, Insiderbedrohungen oder auch Sabotage zu stärken. Abgrenzend zur NIS-2-Richtlinie betrifft die CER-Richtlinie Vorgaben zur Cyberresilienz, nicht zur Cybersicherheit.

- **Cyber Resilience Act (CRA):** Der Cyber Resilience Act, der in der zweiten Hälfte des Jahres 2024 in Kraft treten und ab 2027 gelten soll, zielt darauf ab, Verbraucher und Unternehmen zu schützen, die Produkte oder Software mit einer digitalen Komponente kaufen oder verwenden. Hersteller und Einzelhändler sollen verbindliche Cybersicherheitsanforderungen einhalten müssen, wobei sich der entsprechende Schutz über den gesamten Produktlebenszyklus erstrecken soll. Die Pflichten umfassen die Implementierung von Mechanismen zur schnellen Behebung von Sicherheitslücken sowie auch die Bereitstellung regelmäßiger Sicherheitsupdates.

- **Verordnung über Künstliche Intelligenz (KI-VO):** Die Verordnung über Künstliche Intelligenz (KI-VO) wurde im Juli 2024 im Amtsblatt der EU veröffentlicht, 20 Tage später ist sie in Kraft getreten. Die einzelnen Vorschriften und resultierende Verpflichtungen werden gestaffelt Geltung erlangen. Die Verordnung zielt darauf ab, die Nutzung von KI-Systemen sicherer und transparenter zu gestalten. Die Verordnung legt Anforderungen an die Entwicklung, Bereitstellung und Nutzung von KI-Systemen fest, insbesondere in Bezug auf Risikobewertungen, Transparenz und die Einhaltung ethischer Standards.

Neben den oben genannten Gesetzen gibt es eine Vielzahl weiterer Regelungen, die die IT-Sicherheit betreffen. Dazu gehören das IT-Sicherheitsgesetz 2.0 in Deutschland, das spezifische Anforderungen an die Sicherheitsmaßnahmen von Betreibern kritischer Infrastrukturen stellt, sowie die Datenschutz-Grundverordnung (DSGVO), die umfassende Vorgaben zum Schutz personenbezogener Daten macht. Diese Regelungen ergänzen und verstärken die Anforderungen an die IT-Sicherheit in Unternehmen.

ISMS: EIN ÜBERBLICK

Ein Informationssicherheits-Managementsystem (ISMS) ist ein systematischer Ansatz zur Verwaltung sensibler Unternehmensinformationen, um deren Sicherheit zu gewährleisten. Es bindet Menschen, Prozesse und IT-Systeme ein, auf deren Zusammenwirken eine umfassende Informationssicherheitsstrategie aufgebaut wird. Ein ISMS basiert oft auf international anerkannten Standards wie ISO/IEC 27001 oder SOC 2 und bietet einen strukturierten Rahmen zur Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken.

Ein solches System hat zahlreiche Vorteile, die es Unternehmen ermöglichen, den Anforderungen der neuen IT-Sicherheitsgesetze gerecht zu werden und darüber hinaus die allgemeine Sicherheitslage zu verbessern. So bietet der ganzheitliche Ansatz des ISMS die Möglichkeit, alle Aspekte der Informationssicherheit, von technischen Maßnahmen bis hin zu organisatorischen Prozessen, zu integrieren und somit eine umfassende Abdeckung aller potenziellen Sicherheitslücken zu gewährleisten. Darüber hinaus unterstützt ein ISMS Unternehmen bei der Erfüllung der gesetzlichen Anforderungen aus NIS-2, DORA, CER-Richtlinie, CRA sowie KI-VO und reduziert damit das Risiko von Sanktionen und anderen rechtlichen Konsequenzen.

Es bietet zudem einen strukturierten Ansatz, der es Unternehmen erleichtert, fundierte Entscheidungen zu treffen und gezielte Sicherheitsmaßnahmen zu ergreifen.

Durch klar definierte Prozesse und Verantwortlichkeiten können die Verantwortlichen schneller und effizienter auf Vorfälle reagieren und so den möglichen Schaden minimieren. Ein ISMS stellt sicher, dass alle Beteiligten wissen, welche Schritte im Fall eines Sicherheitsvorfalls zu unternehmen sind und dass notwendige Maßnahmen sofort eingeleitet werden können, um die Auswirkungen auf das Unternehmen so gering wie möglich zu halten.

Dies kann gegenüber Kunden, Geschäftspartnern und Aufsichtsbehörden dokumentiert werden: Eine Zertifizierung nach ISO/IEC 27001 oder SOC 2 schafft Vertrauen, weil Unternehmen damit nachweisen, dass sie hohe Sicherheitsstandards einhalten und der Informationssicherheit Priorität einräumen. Besonders im öffentlichen Sektor sind ISMS-Zertifizierungen oft eine Voraussetzung für die Teilnahme an Ausschreibungen. Unternehmen, die eine solche Zertifizierung vorweisen können, haben somit bessere Chancen, neue Aufträge zu gewinnen und sich von der Konkurrenz abzuheben.

Nicht zuletzt erhöht ein ISMS das Sicherheitsbewusstsein innerhalb der Organisation, indem es eine Kultur fördert, die dazu beiträgt, die Wahrscheinlichkeit menschlicher Fehler, die häufig die Ursache von Sicherheitsvorfällen sind, zu verringern. Wenn alle Mitarbeiterinnen und Mitarbeiter ein tiefes Verständnis für Sicherheitspraktiken entwickeln und diese konsequent anwenden, sinkt das Risiko von Sicherheitslücken erheblich.

Schließlich erleichtert ein zertifiziertes ISMS die Durchführung interner und externer Audits, da die Prozesse und Dokumentationen klar definiert sind und die Unternehmen so Zeit und Ressourcen besser nutzen können.

WESENTLICHE SCHRITTE ZUR EINFÜHRUNG EINES ISMS

Bei der Einführung eines ISMS ist ein strukturiertes und systematisches Vorgehen unerlässlich. Die einzelnen Schritte dabei sind:

- **Initiierung und Planung:** Festlegung der Ziele und des Umfangs des ISMS, Ernennung eines ISMS-Teams und Entwicklung einer ISMS-Politik
- **Risikobewertung und -behandlung:** Durchführung einer umfassenden Risikobewertung zur Identifikation potenzieller Bedrohungen und Schwachstellen; Entwicklung und Implementierung von Maßnahmen zur Risikobehandlung
- **Implementierung der Kontrollen:** Umsetzung der identifizierten Sicherheitsmaßnahmen und Schulung der Mitarbeiter. Unternehmen sollten sicherstellen, dass sie geeignete technische und organisatorische Maßnahmen implementieren, um ihre Informationssicherheit zu verbessern.
- **Überwachung und Bewertung:** kontinuierliche Überwachung der Wirksamkeit des ISMS und Durchführung regelmäßiger interner Audits
- **Zertifizierung:** Vorbereitung auf das externe Audit und Durchführung durch eine anerkannte Zertifizierungsstelle
- **Pflege und kontinuierliche Verbesserung** des ISMS unter Anwendung des sogenannten Plan-Do-Check-Act-(PDCA)-Ansatzes

FAZIT

Die Implementierung eines ISMS und dessen Zertifizierung nach international anerkannten Standards ist für Unternehmen in der heutigen digitalen Welt nahezu unverzichtbar. Ein ISMS bietet einen systematischen Ansatz, um Informationssicherheitsrisiken zu managen und gesetzliche Anforderungen zu erfüllen. Es schafft Vertrauen bei Kunden und Geschäftspartnern, erleichtert Audits und verbessert die Erfolgsaussichten bei Ausschreibungen. Die Einführung eines zertifizierten ISMS bietet die Chance, die Informationssicherheitsstrategie eines Unternehmens auf ein solides Fundament zu stellen, besonders vor dem Hintergrund der zunehmenden Bedeutung von Cybersecurity und neuer gesetzlicher Anforderungen. Um die so erreichte Cybersicherheit der Systeme auch langfristig zu gewährleisten, ist eine kontinuierliche Verbesserung und Anpassung des ISMS an neue Bedrohungen und technologische Entwicklungen entscheidend. ■

DR. JAN SCHARFENBERG, LL.M. (Stellenbosch)
ist als Rechtsanwalt bei der Kanzlei Schürmann Rosenthal Dreyer im Bereich Datenschutz- und Informationssicherheitsrecht tätig. Daneben arbeitet er als Director für den Bereich Informationssicherheit bei der ISiCO Datenschutz GmbH. Dr. Jan Scharfenberg verfügt über mehr als 15 Jahre Erfahrung im Bereich Regulatory und Corporate Compliance, mit Stationen in einer renommierten internationalen Großkanzlei und als Rechts- und Compliance-abteilungsleiter in einem Gesundheits-Start-ups eines internationalen Versicherungskonzerns.

www.srd-rechtsanwaelte.de

17. – 20. September 2024

SECURE YOUR BUSINESS

Digital Networking Security

JETZT TICKET SICHERN!

50 years

security essen

Die Leitmesse für Sicherheit

www.security-essen.de

MESSE ESSEN

RAGs für die Informationssicherheit

EFFIZIENTERES ISMS DURCH KI (1)

Bild: tippapatt - stock.adobe.com

Informationssicherheits-Managementsysteme (ISMS) sind zentral für den Schutz sensibler Daten und gewinnen durch EU-Vorschriften wie den AI Act und NIS-2 an Bedeutung. Moderne Sprachmodelle, ergänzt durch lokale Wissensdatenbanken beziehungsweise durch Retrieval-Augmented Generations (RAGs), können die Anwendung von ISMS erleichtern und die Akzeptanz bei den Mitarbeitern erhöhen, indem sie die Verständlichkeit von Richtlinien und Vorschriften verbessern und auf die Bedürfnisse der Anwender anpassen. Sie sind zudem quellen- und branchenunabhängig einsetzbar und werden in Zukunft noch leistungsfähiger und vielseitiger sein.

Informationssicherheits-Managementsysteme spielen in der heutigen digitalen Welt eine zentrale Rolle. Sie sind entscheidend für den Schutz sensibler Daten in Unternehmen und die Gewährleistung der IT-Sicherheit. Darüber hinaus gewinnen ISMS aufgrund neuer EU-Vorschriften wie dem AI Act und NIS-2 zunehmend an Bedeutung. Diese Regelungen stellen zusätzliche Anforderungen an die IT-Sicherheit und machen ein robustes ISMS unabdingbar.

Doch trotz ihrer Bedeutung sind viele Systeme nicht intuitiv nutzbar. Es bedarf gezielter Maßnahmen, um die Mitarbeiter zur aktiven Nutzung zu motivieren und die Anwendung eines ISMS zu fördern. Ein wesentlicher Aspekt ist dabei, die Komplexität von IT-Sicherheitsrichtlinien zu reduzieren. Diese müssen so formuliert sein, dass sie für jeden Mitarbeiter verständlich sind, unabhängig von seiner Rolle oder seinem technischen Hintergrund. Darüber hinaus müssen die Richtlinien verfügbar sein, da die Suche nach ihnen die Arbeitsprozesse stark verlangsamt. Nur so kann sichergestellt werden, dass jeder in der Lage ist, die Richtlinien effektiv umzusetzen.

In diesem Zusammenhang bieten moderne Technologien wie Sprachmodelle und Retrieval-Augmented Generation erhebliche Vorteile. Sie können dazu beitragen, die Bedienung und Umsetzung von ISMS zu vereinfachen und deren Akzeptanz zu erhöhen. Beispielsweise werden Richtlinien in der Sprache des Sprachmodell-Nutzers ausgegeben, was die Verständlichkeit verbessert. Mitarbeiter haben zudem nur Zugriff auf die für sie freigegebenen Informationen, was die Sicherheit erhöht. RAGs sind nicht nur flexibel einsetzbar, wenn ein effizienter Wissenszugriff erforderlich ist, sondern zudem auch universell und branchenunabhängig. Abbildung 1 zeigt einen Prototypen eines RAG-Chatbots, der automatisiert Unternehmensrichtlinien überprüft. Ein Video dazu ist in voller Länge unter *www.advisori.de/news-projekte/advisori-chatbot* verfügbar.

RAG-CHATBOTS: FUSION VON GENERATIVEN UND RETRIAVAL-BASIERTEN MODELLEN

RAGs nutzen große Sprachmodelle wie ChatGPT, um mithilfe von Wissensdatenbanken nach relevanten Informationen zu suchen und präzise Antworten zu liefern. Sie bestehen im Wesentlichen aus den folgenden zwei Komponenten:

- **Retrieval-Modell:** Diese Komponente sorgt dafür, dass relevante Informationen aus einer Wissensdatenbank abgerufen werden.

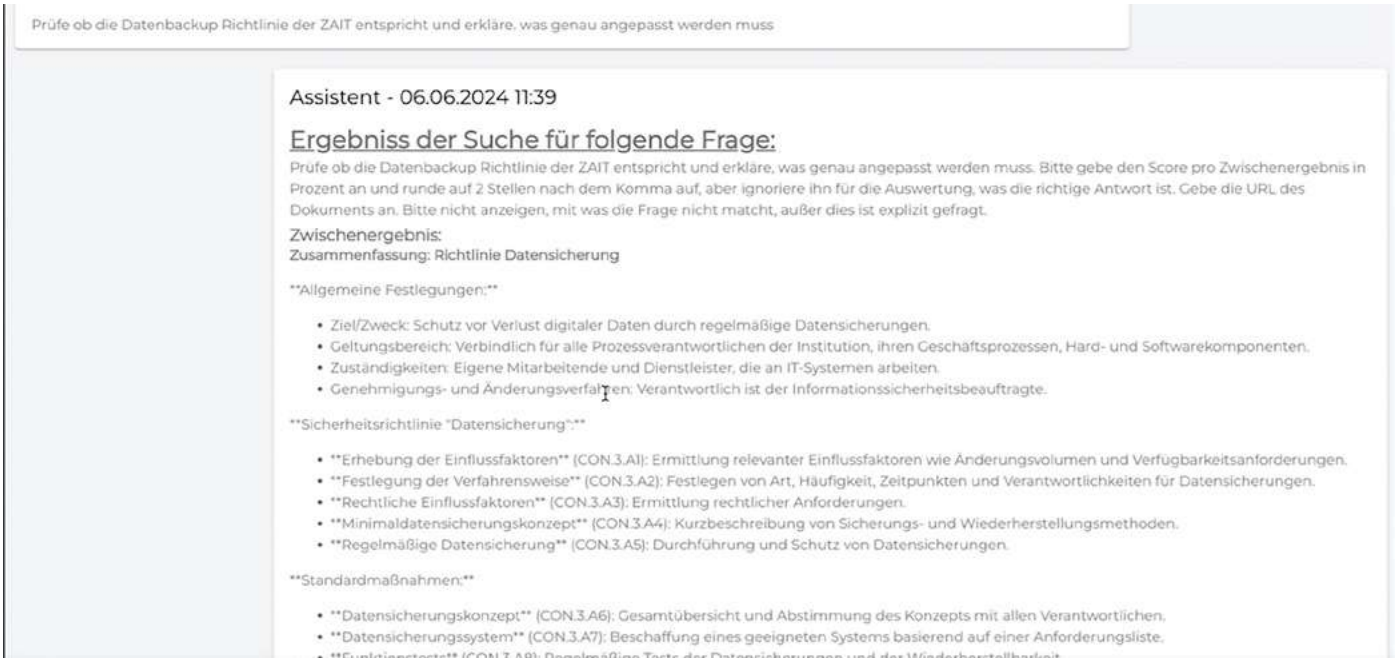


Abbildung 1: Prototyp eines Chatbots für das Überprüfen von Unternehmensrichtlinien. Mehr dazu unter www.advisori.de/news-projekte/advisori-chatbot (Bild: ADVISORI FTC GmbH)

- **Generatives Sprachmodell:** Diese Komponente nutzt die vom Retrieval-Modell abgerufenen Informationen, um mithilfe eines Sprachmodells (zum Beispiel ChatGPT, Gemini oder Llama et cetera) eine benutzerspezifische Antwort zu generieren.

Das generative Sprachmodell nutzt zusätzlich die ursprünglich im Training erworbenen Fähigkeiten und kombiniert diese mit externem domänenspezifischem Wissen aus der Wissensdatenbank. Daten für so eine Wissensdatenbank können vielfältig sein, darunter unternehmensspezifische Quellen wie Wikis, Intranet-Seiten, Datenbanken, das SharePoint sowie Informationen aus Kundensupport-Tickets und deren Lösungen. Für den Benutzer bedeutet dies, dass er seine Suche direkt in das Suchfeld eingeben kann und anschließend interaktiv, ähnlich wie bei ChatGPT, mit den Dokumenten kommuniziert, anstatt relevante Informationen mühsam über Stichwortsuchen oder Keywords herauszufiltern. RAGs können aber auch effektiv zur kontinuierlichen Überprüfung von Informationen eingesetzt werden, indem sie automatisch prüfen, ob beispielsweise Unternehmensrichtlinien den aktuellen Standards entsprechen oder ob Anpassungen erforderlich sind. Die Funktionsweise des RAG-Chatbots im Rahmen des ISMS wird im Folgenden Schritt für Schritt anhand eines Beispiels demonstriert (siehe dazu auch Abbildung 2).

Schritt 1: Anfrage eines Benutzers

Ein User (1) stellt eine Anfrage an das System, die wie folgt lauten kann: „Wie sieht die Richtlinie zum Patchmanagement aus?"

Schritt 2: Umwandlung der Benutzeranfrage in Vektoren

Bevor das Retrieval-Modell nach relevanten Informationen suchen kann, wird die Anfrage des Benutzers tokenisiert (2) und in einen Vektor umgewandelt (3). Beim Tokenisieren werden Textinhalte in ihre Grundbestandteile, sogenannte Tokens, zerlegt. Diese Tokens bestehen aus einzelnen Wörtern, Satzzeichen oder anderen bedeutungstragenden Einheiten. Diese Tokens werden durch ein Embedding-Modell in Vektoren umgewandelt. Dabei erhält jedes Wort eine numerische Repräsentation in einem multidimensionalen Raum. Das Modell ordnet ähnlichen Wörtern ähnliche Vektoren zu, wodurch semantische Beziehungen zwischen den Wörtern abgebildet werden. Diese Vektorrepräsentationen ermöglichen folglich, die Bedeutung von Wörtern basierend auf ihrer Verwendung im Kontext zu erfassen.

Schritt 3 (Retrieval-Modell): Aufbau einer Wissensdatenbank

Für die Wissensdatenbank werden Unternehmensrichtlinien, branchenspezifische Vorschriften und Regularien aus unterschiedlichen Quellen (zum Beispiel Sharepoint, Google Drive et cetera) ebenfalls zunächst tokenisiert (4) und in Vektoren (5) umgewandelt. Die durch das Embedding-Modell generierten Vektoren werden in einer Vektordatenbank (6) gespeichert, wodurch der Inhalt der Dokumente semantisch repräsentiert wird. Diese Speicherung ermöglicht eine effiziente Suche und Analyse, da die Vektoren die Bedeutung der Dokumente erfassen und deren inhaltliche Beziehungen abbilden. So können ähnliche Dokumente und Informationen schnell identifiziert und abgerufen werden, was die Nutzung der Wissensdatenbank optimiert. Es ist wichtig, dass für alle Text-zu-Vektor-Umwandlungsschritte ein einheitliches Embedding-Modell verwendet wird, da sonst die Kontextrepräsentationen der unterschiedlichen Modelle variieren würden. Dies könnte zu Inkonsistenzen bei der semantischen Analyse und bei den Suchergebnissen führen.

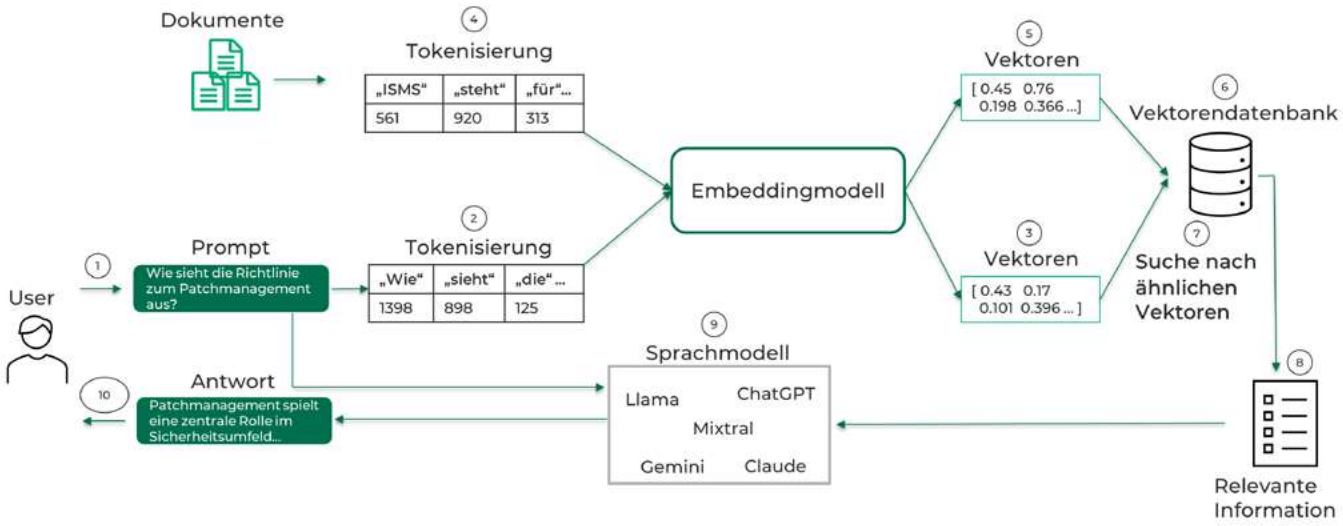


Abbildung 1: Prototyp eines Chatbots für das Überprüfen von Unternehmensrichtlinien. Mehr dazu unter www.advisori.de/news-projekte/advisori-chatbot (Bild: ADVISORI FTC GmbH)

Schritt 4 (Retrieval-Modell): Suche nach ähnlichen Dokumenten in der Wissensdatenbank

Die vektorisierte Suchanfrage des Benutzers (3) wird verwendet, um in der Wissens(vektor)datenbank nach semantisch ähnlichen Vektoren (7) zu suchen. Dabei kommen Techniken zum effizienten Indexieren und Durchsuchen großer Datensätze zum Einsatz, die eine schnelle und präzise Identifikation relevanter Informationen ermöglichen. Die gefundenen Vektoren, in unserem Fall zum Patchmanagement, werden anschließend in ihre ursprüngliche Textform (8) zurückgewandelt und zur weiteren Verarbeitung an ein Sprachmodell (9) übergeben.

Schritt 5: Generierung der Antwort

Das Sprachmodell sieht somit nicht nur die Frage des Nutzers, sondern auch das Hintergrundwissen, das erforderlich ist, um korrekt zu antworten (10). Das eigens erlernte Wissen wird vom Sprachmodell genutzt, um die Anfrage in der vom Benutzer gewünschten Form zu beantworten. Auf diese Weise kann ein Chatbot sämtliche Fragen zu einem Thema beantworten, vorausgesetzt, die Antwort ist Bestandteil der Wissensdatenbank. In unserem Fall wären es Richtlinien zur sicheren Softwareentwicklung und Software-Patches, einschließlich Verlinkungen zu den Originaldokumenten. Diese Informationen ermöglichen es dem Nutzer, auf fundierte Quellen zuzugreifen und aktuelle Sicherheitsstandards direkt einzusehen.

RAGS VS. FINE-TUNING: EIN VERGLEICH

Sowohl RAGs als auch Fine-Tuning sind leistungsstarke Werkzeuge zur Anpassung und Optimierung von Sprachmodellen. Zwar umfassen fertig trainierte Sprachmodelle allgemeines Wissen, das auf eine Vielzahl von Aufgaben angewendet werden kann. Um allerdings den spezifischen Anforderungen der verschiedenen Anwendungen gerecht zu werden, wird das Fine-Tuning eingesetzt, um das Modell zu spezialisieren und seine Leistungsfähigkeit zu steigern. Bei dieser Technik werden bestimmte Parameter und Gewichte eines Sprachmodells während einer Anpassung weiter optimiert, um das Modell gezielt auf spezifische Daten, wie etwa Unternehmensrichtlinien, abzustimmen. Das gelernte Vorwissen geht dabei nicht verloren, sondern wird durch spezifische Anpassungen optimiert, um Nutzeranfragen präziser beantworten zu können.

Dieser Ansatz hat jedoch einige Nachteile. Das Fine-Tuning erfordert spezielle Kenntnisse im Bereich des maschinellen Lernens, einen hohen Rechenaufwand einschließlich leistungsfähiger GPUs oder TPUs und kann sehr zeitaufwendig sein. Darüber hinaus muss der Prozess für jede neue Anwendung oder Änderung der Daten wiederholt werden. Wenn die Themen nicht Teil der Trainingsdaten sind, wie es bei aktualisierten Richtlinien und Standards der Fall ist, können Sprachmodelle ungenaue und irreführende Informationen erzeugen, die man als „Halluzinationen" bezeichnet. Besonders in Domänen, in denen sich die Wissensbasis ständig ändert oder nicht öffentlich verfügbar ist, stellt das Fine-Tuning eine Herausforderung dar.

RAGS: HÖHERER GRAD DER AUTOMATISIERUNG UND VERBESSERTE KOSTENEFFIZIENZ

Zwar bietet das Fine-Tuning eine gezielte und spezialisierte Verbesserung von Modellen an, wenn es allerdings um Anwendungen geht, die auf aktuelle und sich ständig ändernde Informationen angewiesen sind, haben RAGs eine Reihe weiterer entscheidender Vorteile:

- **Ressourcenschonend:** Es muss kein Sprachmodell zeit- und ressourcenaufwendig nachtrainiert oder „fine-tuned" werden.
- **Relevanz und Flexibilität**: RAG-Systeme können leicht angepasst werden, um neue Datenquellen und Informationen zu inte-

grieren. Jede Wissensquelle lässt sich in den Prozess einbinden. Dadurch liefern sie stets aktuelle und präzise Antworten.

- **Transparenz:** Da RAG-Systeme in der Lage sind, die Herkunft der abgerufenen Informationen zu dokumentieren und die verwendeten Quellen zu zitieren, ermöglichen sie eine Überprüfung der generierten Antwort. Die Neigung der Sprachmodelle zur Halluzination wird dadurch verringert.

- **Zugriffssteuerung:** Eine rollenbasierte Zugriffskontrolle kann auf Dokumentenebene implementiert werden, um den Zugriff auf Daten zu steuern und den Zugriff nur autorisierten Personen zu erlauben.

- **Zeitersparnis durch Automatisierung:** Es ist nicht notwendig, Informationen manuell oder durch Stichwort- oder Schlagwortsuche zu suchen. Das System kann die Suche und Integration der relevanten Daten übernehmen, um effizient und schnell relevante Informationen abzurufen.

- **Verbesserte Benutzererfahrung:** RAG-Systeme sind in der Lage, Antworten zu generieren, die auf den spezifischen Kontext und die Bedürfnisse des Benutzers abgestimmt sind, was die Benutzerzufriedenheit erhöht. Dies bedeutet, dass neben dem „Was" auch das „Wie" der bereitgestellten Informationen bestimmt werden kann – auch mehrsprachig.

DIE ROLLE DES PROMPT-ENGINEERINGS

Damit Sprachmodelle präzise und kontextbezogene Antworten generieren, spielt das Prompt-Engineering eine entscheidende Rolle. Dabei wird der Eingabeprompt so gestaltet und klar definiert, dass das Sprachmodell genau auf die Anfrage eines Benutzers antworten kann. Da das Prompting einen wesentlichen Einfluss auf die Qualität der abgerufenen Informationen und der generierten Antworten hat, spielt dieser Prozess insbesondere bei automatisierten RAGs eine entscheidende Rolle. Ein gut durchdachter und präziser Prompt kann den Unterschied zwischen einer allgemeinen und einer sehr spezifischen Antwort ausmachen.

Oftmals ist es notwendig, den Prompt iterativ zu verfeinern, basierend auf den ersten Ergebnissen. Dies bedeutet, dass der Benutzer den Prompt anpassen und umformulieren muss, um bessere und genauere Ergebnisse zu erhalten. Das ist besonders wichtig bei komplexen Abfragen, bei denen verschiedene Aspekte und Details berücksichtigt werden müssen. Beispielsweise kann ein Benutzer statt *„Wie sieht die Richtlinie zum Patchmanagement aus?"* den Prompt wie folgt anpassen, um vom Sprachmodell eine präzisere Antwort zu erhalten: *„Bitte erläutere die aktuellen Richtlinien und Best Practices zum Patchmanagement, insbesondere in Bezug auf die neuesten Updates und Änderungen. Welche Schritte sind in der Implementierung und Überwachung besonders wichtig?"*

WIE WERDEN RAGS DIE ZUKUNFT PRÄGEN?

Im Bereich des Wissensmanagements eröffnen Retrieval-Augmented-Generative-Systeme beeindruckende Möglichkeiten. Im ISMS stellen sie eine dynamische Lösung dar, um Sicherheitsrichtlinien und -standards effektiv zu verwalten. RAGs zeichnen sich durch ihre Fähigkeit aus, aktuelle Informationen effizient abzurufen und zu verarbeiten, wodurch sie die Limitationen rein generativer Chatbots überwinden. Im Vergleich zum Fine-Tuning von Modellen sind sie ressourcenschonender und flexibler, während sie gleichzeitig eine höhere Transparenz bieten. Dies geschieht durch die Dokumentation der Herkunft von Informationen sowie der Angabe der genutzten Quellen.

Durch ihre vielseitige Anwendbarkeit werden RAGs nicht nur die Zukunft der IT-Sicherheit maßgeblich beeinflussen, sondern werden auch universell und branchenunabhängig eingesetzt werden, um einen effizienten Zugriff auf Wissen zu ermöglichen und Mitarbeitern gezielt relevante Informationen bereitzustellen. In unserem nächsten Artikel in Ausgabe 5 der IT-SICHERHEIT werden wir genauer darauf eingehen, wie sich RAGs effektiv im IT-Ticketsystem einsetzen lassen. Beispielsweise können diese automatisiert Ähnlichkeiten und Muster zwischen Tickets identifizieren, wodurch häufige Probleme erkannt und deren Lösungen standardisiert werden können. Das verbessert nicht nur die Effizienz der Problemlösung, sondern ermöglicht auch eine proaktive Wartung, indem wiederkehrende Probleme schneller erkannt und behoben werden.

Die kontinuierliche Weiterentwicklung und Optimierung der RAG-Technik wird dazu führen, dass sie ihre Fähigkeiten zur Wissensverarbeitung und -integration weiter ausbauen werden, beispielsweise durch die Berücksichtigung von nutzerspezifischem Wissen. Darüber hinaus werden Weiterentwicklungen wie autonome KI-Agenten und multimodale Chatbots, die neue Möglichkeiten eröffnen und die Fähigkeiten von Chatbots erweitern werden. KI-Techniken wie das „verstärkende Lernen" (Reinforcement Learning) werden RAGs unterstützen, wodurch vielseitige und kontextbezogene Systeme entstehen, die komplexere Aufgaben lösen können, um den Nutzen dieser Systeme zu erhöhen. ■

ASAN STEFANSKI
ist Director des Bereiches Digital Transformation bei der ADVISORI FTC GmbH. Er verfügt außerdem über langjährige Erfahrung als Teamleiter im Bereich Software Engineering.

INNA VOGEL
ist Senior Consultant im Bereich Digital Transformation bei der ADVISORI FTC GmbH. Vorher hat sie mehrere Jahre an einem renommierten Institut im Bereich maschinelles Lernen und Sprachtechnologie geforscht.

So schaufeln Unternehmen Ressourcen frei und stärken die Sicherheit ihrer IT

MIT MANAGED SERVICES GEGEN DEN FACHKRÄFTEMANGEL

Bild: klyaksun - stock.adobe.com

Durch die Auslagerung von IT-Aufgaben an externe Dienstleister können Unternehmen Kosten sparen, die Effizienz steigern und die Sicherheit erhöhen. Managed Services versprechen Skalierbarkeit, Flexibilität und Konzentration auf das Kerngeschäft. Doch was leisten Managed Services und wo liegen die Unterschiede zum klassischen Outsourcing?

Das Schreckgespenst Fachkräftemangel geht um. Die Generation der Babyboomer, die einen Großteil der heute in Deutschland Beschäftigten ausmacht, wird bald das Rentenalter erreichen. Dazu kommen noch etliche Herausforderungen durch Hybrid-Work, künstliche Intelligenz (KI), Cloud-Migrationen, ein halbes Dutzend neuer Compliance-Richtlinien und neue Bedrohungen, die dafür sorgen, dass Firmen verschiedenster Branchen die Fachkräfte ausgehen. Laut Branchenverband Bitkom sind derzeit rund 149.000 Stellen für IT-Experten unbesetzt. „Zu wenige Fachkräfte und zu viel Regulierung bremsen das digitale Deutschland", mahnt in diesem Zusammenhang Bitkom-Präsident Dr. Ralf Wintergerst. Unternehmen, denen Mitarbeiter fehlen, müssen deshalb dringend handeln. Eine Option, mangelndes Wissen und fehlende Manpower in den eigenen Reihen abzufedern, sind Managed Services.

DAS KÖNNEN MANAGED SERVICES

Doch was sind Managed Services genau? Unter Managed Services versteht man die Auslagerung bestimmter IT-Funktionen, wiederkehrender IT-Dienstleistungen und -Prozesse, an einen externen Dienstleister. Dieser nennt sich Managed Services Provider, kurz MSP. Derartige Services werden in der Regel aus der Ferne erbracht und verwaltet, sodass Unternehmen die Verantwortung für bestimmte Aspekte ihres IT-Betriebs an externe Experten abgeben können. Es gibt aber auch die Option, firmeneigene Räume zur Verfügung zu stellen.

Managed Services können eine breite Palette von IT-Funktionen abdecken. Beispiele sind Infrastrukturmanagement, Netzwerküberwachung, Sicherheitsmaßnahmen, Datensicherung und -wiederherstellung, Anwendungs-Hosting und technischer Support. Unternehmen nutzen so kostengünstig und effizient externes Fachwissen, verbessern die eigenen IT-Fähigkeiten und optimieren ihre Performance. Das ist aber noch nicht alles, denn Managed Services helfen auch, die Belastung zu verringern, die durch die interne Verwaltung komplexer IT-Umgebungen aufkommen kann.

Zusammengefasst haben Managed Services folgende Vorteile:

- **Planbare Kosten:** Managed Services werden zumeist als Abonnement angeboten, sodass Unternehmen IT-Ausgaben besser vorhersagen und budgetieren können. Statt hoher Vorlaufkosten für IT und Personal zahlen sie eine wiederkehrende Gebühr – sie bezahlen zudem nur für die Leistungen, die wirklich benötigt werden.

- **Verbesserte Sicherheit und Compliance:** MSP sind von Haus aus auf „Compliance" getrimmt und schützen sensible Daten und Systeme vor Cyberbedrohungen und Compliance-Brüchen.

- **Konzentration aufs Kerngeschäft:** Durch die Auslagerung von IT-Routineaufgaben und -Verantwortlichkeiten an einen MSP können Unternehmen ihre IT-Teams einfach mal durchatmen lassen und sich auf ihr Kerngeschäft konzentrieren, Innovationen angehen und schlicht produktiver arbeiten.

- **Proaktive Überwachung und Wartung:** MSP überwachen die Leistung und den Zustand von IT-Systemen und -Infrastrukturen kontinuierlich – je nach Modell entweder zu bestimmten Zeiten (9 to 5) oder 24/7. Sie entdecken Schwachstellen proaktiv und minimieren Ausfälle im Betrieb.

- **Experten-Know-how:** MSP beschäftigen Teams qualifizierter Experten, die über Fachwissen in verschiedenen IT-Bereichen verfügen, darunter Netzwerke, Cybersicherheit, Cloud Computing und Anwendungsentwicklung – Wissen, dass sich intern nur teuer durch Trainings und Recruiting von Experten erkaufen lässt.

- **Flexibilität:** Managed Services sind so konzipiert, dass sie ganz einfach mit dem Betrieb skalieren. Egal, ob der Betrieb ausgeweitet wird, neue Nutzer hinzukommen oder neue Technologien eingeführt werden: Unternehmen können ihre Managed Services jederzeit problemlos erweitern.

MANAGED SERVICES VS. OUTSOURCING

Die Auslagerung von IT-Aufgaben ist beliebt: Der Umsatz im IT-Outsourcing-Markt soll 2024 bei rund 147,6 Milliarden Euro liegen. Doch wie unterscheiden sich Managed Services vom klassischen Outsourcing? Eins vorweg: Auch Managed Services werden ausgelagert – hier gibt es also begriffliche Überschneidungen: Bei Managed Services übernimmt der Dienstleister die Verantwortung für bestimmte Aufgaben und Dienstleistungen, oft mit einem höheren Maß an Autonomie. Der Kunde konzentriert sich auf sein Kerngeschäft, während der Dienstleister die Verwaltung und Wartung der Dienstleistungen übernimmt.

Beim klassischen Outsourcing werden hingegen bestimmte Geschäftsprozesse oder Funktionen

an einen externen Dienstleister ausgelagert. Der Dienstleister führt diese Aufgaben im Namen des Kunden durch, doch der Kunde behält zumeist eine gewisse Kontrolle und Verantwortung. Da nur bestimmte Unterabteilungen und IT-Services an den Dienstleister gehen, verbleibt die IT im Haus des Kunden. Dieser hat also auch weiterhin das Sagen hinsichtlich seiner Infrastruktur, IT-Struktur und Abläufe. Die zu erbringenden IT-Dienstleistungen sind schon im Voraus genau definiert und müssen regelmäßig auf Grundlage von Service Level Agreements (SLA) bereitgestellt werden.

Managed Services können sehr spezifisch auf den individuellen Bedarf abgestimmt werden, da sie oft kleinteiliger sind. Sie sind meistens auch kosteneffektiver, da nur das eingekauft wird, was auch benötigt wird.

MANAGED SERVICES PROVIDER VS. KLASSISCHER IT-DIENSTLEISTER

Der Hauptunterschied zwischen einem Managed Service Provider und einem klassischen IT-Dienstleister liegt in seinem Dienstleistungsmodell, den Verantwortlichkeiten und dem Umfang der bereitgestellten Dienstleistungen sowie in der Art der Beziehung gegenüber dem Kunden (siehe Tabelle 1).

Managed Service Provider	Klassischer IT-Dienstleister
Dienstleistungen auf Basis eines abonnement-basierten Modells: Kunden zahlen zumeist eine regelmäßige Gebühr für die bereitgestellten Services, die auf einer Service-Level-Vereinbarung (SLA) basieren. MSP übernehmen die Verantwortung für die Verwaltung und Wartung bestimmter IT-Funktionen und -Systeme ihrer Kunden.	Dienstleistungen auf Anfrage: Berechnung in der Regel auf Stundenbasis oder projektorientiert. Kunden beauftragen den Dienstleister für spezifische Projekte, Problemlösungen oder Beratungsleistungen, und die Abrechnung erfolgt je nach erbrachter Leistung.
Langfristige Partnerschaft: MSP bietet kontinuierliche Unterstützung sowie Beratung über einen längeren Zeitraum hinweg. Zudem arbeitet der Service Provider eng mit seinen Kunden zusammen, um IT-Infrastruktur und -Dienste kontinuierlich zu verbessern.	Engagement für spezifische Projekte oder Aufgaben: Dienstleistungen können zeitlich begrenzt sein. Sobald das Projekt abgeschlossen ist, endet die Zusammenarbeit in der Regel, es sei denn, es gibt weitere Anforderungen oder Projekte.
Verwaltung und Betrieb spezifischer IT-Dienste: Beispiele sind Netzwerküberwachung, Sicherheitsmanagement, Daten-Backup, Cloud-Hosting usw. Der MSP agiert als verlängerter Arm des Unternehmens und übernimmt die täglichen Betriebsaufgaben.	Vollumfängliche Dienstleistungen: Lösungen für konkrete technische Probleme oder Projekte. Dies kann die Entwicklung einer maßgeschneiderten Software-Anwendung, die Bereitstellung von Hardware und Software oder die Durchführung einer IT-Infrastrukturüberprüfung umfassen.

Tabelle 1: Gegenüberstellung MSP und klassischer IT-Dienstleister

Es stellt sich die Frage: Was passt zu welchem Unternehmen oder zu welcher Anforderung? Sollte lieber ein MSP oder der klassische IT-Dienstleister gewählt werden? Entscheidend sind hier Definition und Anforderungen. Im Allgemeinen lässt sich sagen: Liegen sehr spezielle Anforderungen, beispielsweise an Produkte oder Aufgaben vor, sind Managed Services die angemessene Wahl. Sollte die Unterstützung vollumfänglich stattfinden oder betrifft sie Inhalte, die durch ganze Abteilungen abgebildet werden, rückt das klassische Outsourcing mittels IT-Dienstleister in den Vordergrund.

MANAGED SERVICES UND FACHKRÄFTEMANGEL

Managed Services bieten somit viele Vorteile und sind aufgrund ihrer Vielseitigkeit ein gutes Mittel gegen Fachkräftemangel. Das liegt zum einen daran, dass eine Auslagerung von IT-Aufgaben helfen kann, vorhandene Talente besser auszulasten, da nicht jeder alle Fachkräfte inhouse haben muss. Außerdem lassen sich mit Managed Services zeitkritische Themen schneller angehen, zeitintensive Aufgaben wie Log-Analyse oder Dokumentation auslagern, um Inhouse-Personal zu entlasten und die Abhängigkeit von Fachwissen im Sinne des „Brain Drain" minimieren, da die Fachkompetenz ausgelagert ist.

FAZIT

So manches Unternehmen hat aufgrund begrenzter Ressourcen und Fachkenntnisse Schwierigkeiten, die Einhaltung von Branchenvorschriften und Sicherheitsstandards zu gewährleisten. Managed Services können im Bereich Compliance wertvolle Unterstützung leisten – besonders in Zeiten des fortschreitenden Fachkräftemangels. Hierdurch lassen sich teure Bußgelder und Strafen im Zusammenhang mit der Nichteinhaltung von Vorschriften vermeiden. Außerdem umfassen Managed Security Services häufig fortschrittliche Funktionen zur Aufdeckung von und zur Reaktion auf Bedrohungen, etwa Security Information and Event Management (SIEM), Intrusion Detection and Prevention Systems (IDPS) sowie Threat Intelligence Analysis. Mit derartigen Technologien werden aufkommende Bedrohungen effektiver erkannt und abgewehrt als beim alleinigen Einsatz interner Ressourcen. Wenn es an Mitarbeitenden mangelt, sind das Fachwissen und die Erfahrung von MSP Gold wert, um die Sicherheit zu verbessern und komplexe technische Herausforderungen zu bewältigen. ■

OLAF PURSCHE
ist Head of Communications der SITS Group AG.
olaf.pursche@sit-group.ch
Weitere Informationen unter www.sits.com

Die Pflicht zur Prüfung von Dienstleistern

WARUM ZERTIFIZIERUNGEN ALLEIN NICHT AUSREICHEN

Die Cyberangriffe der letzten Monate haben gezeigt, dass auch Schwachstellen in Prozessen und Anwendungen von Dienstleistern ein Risiko für die Sicherheit von Organisationen darstellen. Insofern erscheint es nur logisch, dass bereits vor der Auslagerung von (Teil-)Prozessen betreffende Dienstleister überprüft werden müssen. Zur Wahrheit gehört aber auch, dass derartige Prüfungen in der Praxis oft nur unzureichend stattfinden. Organisationen sind jedoch gut beraten, ein gutes Auslagerungsmanagement zu etablieren.

Die zunehmende Komplexität von Prozessen, Systemen und Anwendungen sowie die unter anderem hieraus resultierende Spezialisierung von Unternehmen machen immer öfter eine Einbeziehung Dritter in die eigenen Geschäftsprozesse erforderlich. Gleichzeitig sorgen steigende regulatorische Anforderungen für eine wachsende Verrechtlichung der Informationssicherheit. Probleme ergeben sich daraus, dass der Bereich des IT-Outsourcing – und hier insbesondere die Nutzung von Cloud-Diensten – zunehmend ein Massengeschäft darstellt, wobei die Umsetzung individueller vertraglicher Regelungen nicht oder nur selten möglich ist.

Auftraggeber sind so regelmäßig aufgrund beschränkter Möglichkeiten zur Einflussnahme auf eine ausreichende technische und organisatorische Gewährleistung von Informationssicherheit durch den jeweiligen Dienstleister angewiesen. Die vertragliche Vereinbarung von Kontroll- und Steuerungsrechten ist daher für Auftraggeber zur Überwachung des Auftragnehmers essenziell. Vor diesem Hintergrund wird es in aller Regel nicht ausreichend sein, lediglich vorliegende Testate und Zertifizierungen einzusehen. Zwar können auch durch Prüfungen des Auftragnehmers nicht alle Risiken ausgeschlossen, jedoch auf ein für die Organisation beherrschbares Maß reduziert werden. Nachstehend betrachten wir mögliche Prüfpflichten und Vorgehensweisen für die Umsetzung in der Praxis näher.

MÖGLICHE PRÜFPFLICHTEN IM DETAIL

Ein Blick auf die aktuelle Normenlandschaft macht deutlich, dass umfassende Prüfpflichten bestehen und die Geschäftsleitung die Wirksamkeit der Prüfprozesse gewährleisten muss.

Normen des Gesellschaftsrechts

Bereits aus den gesellschaftsrechtlichen Normen lässt sich eine Überwachungspflicht der Leitungsebene herleiten. Allen voran ist hierbei insbesondere die Regelung des § 93 Aktiengesetz (AktG) zu nennen. Die Norm legt unter Berücksichtigung verschiedener Kriterien, zum Beispiel die Art und Größe des Unternehmens, das wirtschaftliche Umfeld sowie die Art der Geschäftsführungsmaßnahmen, einen Sorgfaltsmaßstab zugrunde. Zwar steht der Geschäftsleitung auch ein erheblicher Ermessensspielraum in Form der sogenannten Business Judgement Rule zu, jedoch sind unternehmerische Entscheidungen stets auf Grundlage angemessener Informationen zu treffen. Insoweit kann man argumentieren, dass die Auslagerung von (Teil-)Prozessen an Dienstleister eine vorherige und fortlaufende Prüfung voraussetzt. Nur so kann die Zuverlässigkeit des Dienstleisters beziehungsweise das Bestehen etwaiger Risiken sowie die Notwendigkeit risikominimierender Maßnahmen unter Berücksichtigung der jeweiligen Risikostrategie (Risikomanagement) wirksam festgestellt werden.

Die Norm bezieht sich zwar zunächst ausschließlich auf Aktiengesellschaften, jedoch lässt sich über § 43 Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) eine solche Verpflichtung ebenfalls für die Geschäftsführungen von Gesellschaften mit beschränkter Haftung sowie nach § 347 Handelsgesetzbuch (HGB) für Leitungspersonen von Handelsgesellschaften herleiten. Flankierend ist weiterhin § 91 Abs. 2 AktG zu nennen, wonach beispielsweise Aufsichtsmaßnahmen ergriffen werden müssen. Insbesondere gilt es existenzgefährdende Risiken rechtzeitig zu erkennen und diese abzuwenden beziehungsweise vorzubeugen. Hierbei sind selbstverständlich auch die wachsenden Risiken durch die stetig steigende Anzahl von (erfolgreichen) Cyberangriffen und der regelmäßig damit verbundene Verlust vertrauenswürdiger Informationen sowie die damit einhergehenden finanziellen Verluste zu berücksichtigen.

Anforderungen aus dem Informationssicherheitsrecht

Ergänzend ergeben sich weitere zahlreiche Verpflichtungen aus den Vorgaben des Rechtes der Informationssicherheit. So lassen sich speziell aus dem Datenschutzrecht unter Heranziehung von Art. 5 Abs. 2 und Art. 24 Datenschutz-Grundverordnung (DS-GVO) entsprechende Nachweispflichten zur ordnungsgemäßen Datenverarbeitung herleiten. Im Rahmen der Auftragsverarbeitung kann sich eine Prüfpflicht bereits aus Art. 28 Abs. 1 DS-GVO (Geeignetheit des Auftragsverarbeiters) und einem bestehenden Haftungsrisiko des für die Datenverarbeitung Verantwortlichen für die Handlungen des Auftragsverarbeiters ergeben. Ebenso kann Art. 32 DS-GVO mit seiner Verpflichtung des Verantwortlichen und des Auftragsverarbeiters für eine angemessene Sicherheit der Verarbeitung zu sorgen, angeführt werden.

Für den Bereich der kritischen Infrastrukturen gilt zudem das BSI-Gesetz (BSIG) und insbesondere § 8a BSIG mit der Verpflichtung angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Vergleichbare Anforderungen gelten nach § 8c BSIG für die Anbieter digitaler Dienste.

Indes kann in Anbetracht der zahlreichen Normen zum Recht der Informationssicherheit die Auflistung auch an dieser Stelle beliebig fortgeschrieben werden. Auch wenn aus den meisten der vorbenannten Normen keine Prüfpflicht aus dem direkten Wortlaut hervorgeht, ist eine Prüfung von Dienstleistern zur vollumfänglichen Erfüllung der rechtlichen Anforderungen wohl unumgänglich.

Ableitung aus dem Informationssicherheitsmanagementsystem

Ergänzend ist anzuführen, dass sich bereits aus der regelmäßigen Funktionsweise eines Managementsystems zwangsläufig das Bestehen regelmäßiger Prüfpflichten ergibt. Dies lässt sich insbesondere bereits aus dem PDCA-Zyklus ableiten, welcher einem jedem Informationssicherheits-Managementsystem (ISMS) zugrunde liegt. Die Organisation hat demnach nicht nur ein bestimmtes Vorgehen zu planen und vorgabenkonform danach zu handeln, sondern die hieraus resultierenden Ergebnisse stets zu prüfen und die betreffenden Abläufe gegebenenfalls anzupassen. Grundsätzlich sind dabei die spezifischen Anforderungen und die zur Verfügung stehenden Ressourcen einer Organisation angemessen zu berücksichtigen.

MAßNAHMEN NACH BSI IT-GRUNDSCHUTZ

Mit Blick auf die Praxis stellt sich anschließend die Frage der Umsetzung. Die Betrachtung von Sicherheitsaspekten in einem Outsourcing-Vorhaben ist, wie im BSI-Grundschutz-Kompendium im Baustein *OPS.2.3 Nutzung von Outsourcing* explizit vorgeschlagen, typischerweise direkt im Outsourcing-Vertrag zu regeln. Teil-

weise bestehen sogar gesetzliche Verpflichtungen zur vertraglichen Fixierung diverser Aspekte, wie mit Blick auf Art. 28 DS-GVO deutlich wird. Es empfiehlt sich zudem die Aspekte der Informationssicherheit bereits ab der Entscheidung für das jeweilige Outsourcing-Projekt einzubeziehen. Ziel sollte der Aufbau einer möglichst umfassenden Schutzsphäre sein.

Festlegung von Anforderungen an Dienstleister und Verträge

Zunächst bietet sich eine vertragliche Spiegelung der verschiedenen regulatorischen Anforderungen zur Informationssicherheit an. Hierbei erlegt der Auftraggeber den jeweiligen Vertragspartnern die jeweils einschlägigen Vorgaben zur Informationssicherheit auf. Zu beachten ist in diesem Zusammenhang jedoch, dass selbst im Fall derartiger Auslagerung von Aufgaben und Pflichten an Dritte dies nicht gleichbedeutend mit einer Entbindung der Informationssicherheitspflicht, mithin von der generellen Verantwortlichkeit, seitens der auslagernden Stelle ist. Zwar erfolgt die Umsetzung der jeweiligen Vorgaben durch den Vertragspartner, die Verantwortung gegenüber Dritten verbleibt jedoch beim Auftraggeber. Aus diesem Grund erfolgt vielfach die vertragliche Vereinbarung zur ordnungsgemäßen Leistungserbringung sowie zur Überwachung derselben.

Aufgrund zahlreicher gesetzlicher Anforderungen, technische und organisatorische Maßnahmen (TOM) umzusetzen, besteht regelmäßig ein Interesse seitens der gesetzlichen Adressaten auch die Vertragspartner zu konkreten TOM zu verpflichten. An dieser Stelle prallen häufig die Interessen der Auftragnehmer an einer größten möglichen Flexibilität in Bezug auf die Umsetzung der TOM und die Interessen der Auftraggeber an der Vereinbarung weiterreichender Kontroll- und Nachweisrechten aufeinander. In der Vertragsgestaltung werden derartige Konflikte häufig durch die Vereinbarung von flexiblen Änderungsrechten seitens der Auftragnehmer unter Einhaltung bestimmter Mindeststandards, entsprechender Dokumentationspflichten und der Einräumung von Sonderkündigungsrechten seitens der Auftraggeber bei wesentlichen Änderungen gelöst.

Im Rahmen der konkreten Umsetzung erfolgt nicht selten zunächst eine abstrakte Verpflichtung im Hauptvertragswerk der Auftragnehmer zur Umsetzung bestimmter TOM in Übereinstimmung mit dem aktuellen Stand der Technik und hieran anknüpfend eine konkrete Festlegung von Einzelmaßnahmen, meist in Form einer gesonderten Anlage zum Hauptvertrag.

Weiterhin werden die übertragenen Anforderungen durch entsprechende vertragliche Nachweisregelungen abgesichert. Sinn und Zweck liegt darin, dass der Auftraggeber zunächst einmal in die Lage versetzt wird, seinen gesetzlichen Nachweispflichten – wie zum Beispiel aus Art. 5 Abs. 2 DS-GVO – nachkommen zu können. Der Auftraggeber muss bestrebt sein, die einzuhaltenden Informationssicherheitsanforderungen detailliert darzulegen und für den Nachweis Konzepte sowie unabhängige Zertifikate und Prüfberichte seitens des Auftragnehmers einzufordern. Schwierigkeiten bei der Überprüfung ergeben sich allerdings regelmäßig dann, wenn die Wirksamkeit sowie die Aussagekraft hinter derartigen Nachweisen zu hinterfragen ist. Abzugrenzen sind an dieser Stelle zunächst Normen und Standards, die ein ISMS innerhalb einer Organisation beschreiben, wie zum Beispiel die ISO 27000-Reihe oder der BSI-Grundschutz, von Zertifizierungen zur IT-Sicherheit, bei denen beispielsweise ein Produkt oder ein IT-Dienst durch eine zuständige Stelle geprüft und zertifiziert wird. Nur bei der zweiten Gruppe an Zertifizierungen, Normen und Standards, werden tatsächlich technische Anforderungen und mithin der Stand der Technik beschrieben. Dies soll keinesfalls die Bedeutung oder Wertigkeit der Zertifizierungen eines ISMS schmälern. Es ist jedoch hervorzuheben, dass die Unterscheidung in der Praxis nicht immer trennscharf durchgeführt wird und somit beispielsweise eine fehlerhafte Bewertungsgrundlage für die Zuverlässigkeit eines Auftragnehmers geschaffen werden kann.

Bestandteil vertraglicher Regelungen können ferner die Festlegung von Zugangsrechten sowie die Durchführung von Audits und anderen Kontrollmaßnahmen sein. Hinsichtlich des konkreten Umfangs der vertraglich zu vereinbarenden Pflichten können insbesondere Orientierungshilfen und Positionspapiere der deutschen und europäischen Aufsichtsbehörden, Best Practices von Interessenverbänden sowie einschlägige technische Normen, Standards und Regelwerke als Maßstab herangezogen werden. Ferner kann die Implementierung von Berichts- und Informationspflichten vereinbart werden.

Gleichwohl können sich Überprüfungspflichten im Bereich der Haftungsfrage ergeben. Ausgangsfrage ist zunächst, welche Leistung und mithin welche Informationssicherheitspflichten geschuldet sind. Möglicherweise fällt so in diesem Bereich der Nachweis einer Pflichtverletzung leichter, wenn die vertraglich in Bezug genommenen Vorgaben nicht oder nicht vollständig umgesetzt wurden. Jedoch kann sich im Rahmen des Mitverschuldens nach § 254 Bürgerliches Gesetzbuch (BGB) das Vernachlässigen beziehungsweise die Nichteinhaltung der Überprüfungspflichten niederschlagen.

Etablierung eines Auslagerungsmanagements

Der im BSI IT-Grundschutz enthaltene Baustein *OPS.2.3 Nutzung von Outsourcing* enthält unter dem Begriff des Auslagerungsmanagements bereits eine Reihe von Maßnahmen, mit denen die zuvor genannten Problematiken adressiert sowie bestehende Prüfpflichten strukturiert und dokumentiert umgesetzt werden können. Insbesondere werden auf verschiedensten Ebenen zahlreiche Möglichkeiten zur Prüfung in Form eines Soll-Ist-Abgleichs aufgezeigt:

- Die Auslagerung von (Teil-)Prozessen und Geschäftsbereichen bedarf zunächst stets einer kontextbasierten Betrachtung potenzieller Risiken. Zu berücksichtigen sind hierbei insbesondere die Kritikalität und die Abhängigkeit der betroffenen Prozesse sowie die Art und Kategorien, der in diesem Zusammenhang betroffenen Informationen. So muss zunächst geklärt werden, ob überhaupt eine Auslagerung an einen Dienstleister erfolgen kann oder ob die Gefährdungslage eine ausschließlich interne Umsetzung gebietet. Dies stellt grundsätzlich zwar keine Prüfung eines konkreten Auftragnehmers in jedem Fall jedoch eine essenzielle Vorprüfung dar.

- Ist der Einsatz eines Auftragnehmers grundsätzlich möglich, sind weiterhin konkrete Anforderungen an diesen zu definieren. Hierzu muss bereits im Vorfeld festgelegt werden, welche Kompetenzen für die Erbringung der Leistung aus Sicht der Informationssicherheit als erforderlich angesehen werden und welchen Grad an Vertrauenswürdigkeit sowie Zuverlässigkeit der Auftragnehmer leisten muss. Möglicherweise sind derartige Aspekte im öffentlichen Sektor bereits in einem Vergabeverfahren zu berücksichtigen. Ein Dienstleister sollte möglichst schon vor der Aufnahme von Vertragsgesprächen anhand

der definierten Kriterien überprüft werden. In diesem Zusammenhang sollten gegebenenfalls bestehende Interessenkonflikte ausgeschlossen werden.

- Im nächsten Schritt sind konkrete Anforderungen an die vertraglichen Regelungen mit dem jeweiligen Dienstleister unter Berücksichtigung der oben aufgeführten Aspekte festzulegen und zu prüfen. So müssen Verträge zumindest ein Recht auf Überprüfung, einen Zustimmungsvorbehalt zur weiteren Verlagerung der Tätigkeit auf Unterauftragnehmer sowie weitere wesentliche Aspekte der Informationssicherheit, wie beispielsweise eine Verpflichtung auf Vertraulichkeit und die Gewährleistung angemessener Sicherheitsmaßnahmen nach IT-Grundschutz oder vergleichbarer Maßnahmen, umfassen. Auch die Bereitstellung eines auf den jeweiligen Prozess angepassten Sicherheitskonzeptes durch den Dienstleister ist zu vereinbaren. Sinnvoll ist in diesem Zusammenhang auch die Etablierung eines Mustervertrags, der die von der Organisation als essenziell angesehenen Anforderungen dienstleisterunabhängig auch für zukünftige beziehungsweise weitere Vertragsverhältnisse einheitlich darstellt.

Ausgehend von diesen Mindestanforderungen können sich auch weitergehende Maßnahmen als sinnvoll erweisen. Dazu können beispielsweise die Erstellung einer organisationsweiten Strategie sowie die Verabschiedung von Richtlinien zu den Voraussetzungen für die Auslagerungen von Tätigkeiten gehören. Je umfangreicher die Anforderungen einer Organisation zur Inanspruchnahme derartiger Dienstleister gestaltet werden, umso eher empfiehlt sich die Etablierung eines umfassenden Auslagerungsmanagements, einschließlich der Benennung einer zuständigen Person, die beispielsweise auch die zuvor genannten Prüfungen im Rahmen vorvertraglicher Maßnahmen durchführen kann.

Durchführung fortlaufender Prüfungen

Jedoch erschöpft sich die Pflicht zur Prüfung von Dienstleistern nicht in einer einmaligen Vorabprüfung. Schließlich kann eine solche ausschließlich eine Momentaufnahme darstellen, wobei nicht sichergestellt werden kann, dass der Dienstleister fortlaufend ein ISMS oder entsprechende Maßnahmen aufrechterhält und weiterentwickelt. Insofern ist auch die ausschließliche Vorlage einer Zertifizierung regelmäßig als unzureichend zu erachten.

Dementsprechend obliegt der Organisation die Pflicht, die Einhaltung der auferlegten Kriterien fortlaufend zu prüfen. Eine solche Prüfung ist einerseits anlassbezogen, also beispielsweise bei Vorliegen von rechtlichen Änderungen oder bei Eintritt von Sicherheitsvorfällen beziehungsweise -ereignissen, andererseits regelmäßig – anlassunabhängig – durchzuführen. Hinsichtlich des Begriffs der Regelmäßigkeit wird keine allgemeingültige Definition möglich sein. Auch hierbei ist Bezug auf die Kritikalität der jeweiligen Prozesse und der hieraus resultierenden Gefährdungslage zu nehmen. Demnach kann es sinnvoll sein, innerhalb einer Organisation unterschiedliche Prüfungsintervalle zu etablieren. Je nach Komplexität der Anforderungen kann die Erstellung einer entsprechenden Richtlinie oder zumindest die Festlegung entsprechender Kennzahlen Erleichterungen in der praktischen Umsetzung ermöglichen. Gegenstand der fortlaufenden Prüfungen sollten stets die vertraglich festgelegten Sicherheitsanforderungen, ergänzt um zwischenzeitlich gegebenenfalls hinzugetretene gesetzliche Anforderungen sowie Inhalte des vorliegenden prozessspezifischen Sicherheitskonzeptes sein.

Sämtliche der aufgeführten Prüfungen sollten in einer dokumentierten und nachvollziehbaren Form erfolgen. Derartige Prüfberichte ermöglichen unter anderem auch der Leitungsebene die Nachweisbarkeit eingerichteter Prüf- und Überwachungsprozesse zur Abwendung existenzgefährdender Risiken. Auch der zugrunde liegende PDCA-Zyklus kann durch die Prüfergebnisse genährt und die Gewährleistung der Informationssicherheit somit insgesamt (besser) sichergestellt werden.

FAZIT

Für den Aufbau einer ganzheitlichen Informationssicherheit ist es für Organisationen unumgänglich, sich mit der (Über-)Prüfung der eingesetzten Dienstleister auseinanderzusetzen. Der Pflichtenkanon reicht von nationalen Vorschriften des Gesellschaftsrechts über das Datenschutzrecht bis hin zu einer eindeutigen Erforderlichkeit aus dem Funktionieren des Informationssicherheitsmanagementsystems selbst. Die Vernachlässigung dieser Anforderungen kann weitreichende Folgen haben. Organisationen ist deshalb zu raten, ihren Prüfpflichten auch tatsächlich nachzukommen.

Mit Blick auf den Baustein *OPS.2.3 Nutzung von Outsourcing* des BSI IT-Grundschutz sind Organisationen gut beraten, ein entsprechendes Auslagerungsmanagement zu betreiben. Vielfach bildet die vertragliche Gestaltung die Basis für den Start einer Outsourcing-Beziehung. Organisationen sehen sich hierbei nicht selten vorgegebenen Vertragsdokumenten der Auftragnehmer ausgesetzt. Ein schlechter Ratgeber ist das einfache Durchsehen und das „Abnicken" vorgelegter TOM-Auflistungen und/oder bestimmter Zertifizierungen, ohne deren konkrete Bedeutung und Auswirkung für den zu betrachtenden Einzelfall zu würdigen. Das Outsourcing-Management endet jedoch nicht mit der Auftragsvergabe, sondern erfordert eine kontinuierliche Überprüfung der eingesetzten Auftragnehmer. ■

ALEXANDER WEIDENHAMMER, LL.M.
ist Rechtsanwalt, Datenschutzbeauftragter (GDD) und BSI IT-Grundschutz-Praktiker (DGI) beim Dresdner Institut für Datenschutz (DID).

MAX JUST, LL.M.
ist Wirtschaftsjurist, Datenschutzbeauftragter (GDD) und BSI IT-Grundschutz-Praktiker (DGI) beim Dresdner Institut für Datenschutz (DID).

Die KI-Revolution (3)

PROZESSOPTIMIERUNG MIT KI

Die rasante Entwicklung der künstlichen Intelligenz (KI) transformiert Unternehmenslandschaften weltweit. Als Schlüsseltechnologie ermöglicht sie nicht nur die Automatisierung routinemäßiger Abläufe, sondern auch die Neugestaltung komplexer Geschäftsprozesse. In unserer fortlaufenden Artikelserie haben wir bereits die Auswirkungen der KI auf die Unternehmensführung [1] und die fortschreitenden Entwicklungen in der künstlichen Intelligenz [2] beleuchtet. In diesem Artikel fokussieren wir uns darauf, wie KI spezifisch zur Optimierung von Prozessen beiträgt, Effizienz steigert und damit die Produktivität auf ein neues Niveau hebt.

KI-Technologien wie maschinelles Lernen und automatisierte Entscheidungssysteme transformieren Unternehmensabläufe grundlegend, indem sie nicht nur die Effizienz und Marktanpassungsfähigkeit verbessern, sondern auch einen entscheidenden Wettbewerbsvorteil bieten. Diese Technologien ermöglichen eine strategische Neuausrichtung, die über die reine Automatisierung hinausgeht und intelligente, selbstoptimierende Arbeitsabläufe schafft. Unternehmen, die KI frühzeitig in ihre Prozesse integrieren, erleben eine signifikante Steigerung der Produktivität und eine Reduktion von Fehlern [3], was zu niedrigeren Betriebskosten führt. Wie bereits in den vorangegangenen Teilen dieser Serie dargestellt, bedarf es einer tiefgreifenden strategischen Überlegung, die über das reine Technologiemanagement hinausgeht, um die Potenziale der KI voll ausschöpfen zu können.

Die transformative Kraft der KI erstreckt sich über verschiedene Branchen, von der Fertigung, wo Predictive Maintenance die Ausfallzeiten und Kosten minimiert, bis hin zum Finanzwesen, wo algorithmisches Trading neue Möglichkeiten im Asset-Management eröffnet. Auch im Gesundheitswesen ermöglichen KI-basierte Diagnosetools eine schnellere und genauere Patientenversorgung.[4, 5]

Der gezielte Einsatz von KI in der Prozessoptimierung kann zahlreiche Vorteile bringen (siehe Tabelle 1).

Die Einführung von KI in Geschäftsprozesse ist jedoch nicht ohne Herausforderungen. Es ist entscheidend, gerade die menschliche Kompetenz zu nutzen und die Mitarbeiter aktiv in den Veränderungsprozess einzubinden. Die Akzeptanz und das Vertrauen in KI-Lösungen hängen maßgeblich davon ab, wie gut die Belegschaft geschult und informiert ist. Unternehmen müssen sicherstellen, dass die KI-Systeme nicht nur technisch robust, sondern auch ethisch vertretbar und transparent sind. Fragen der Datenqualität, der ethischen Nutzung von Algorithmen und der Integration in bestehende IT-Systeme sind entscheidend für den Erfolg.

Die Vorteile, die sich durch eine gut durchdachte Umsetzung erzielen lassen, wiegen die Heraus-

Effizienzsteigerung	Automatisierte Prozesse sind schneller und präziser, was die Produktivität erheblich steigert.
Kostenreduktion	Durch Automatisierung repetitiver Aufgaben und Optimierung von Ressourcen können Betriebskosten signifikant gesenkt werden.
Fehlerreduktion	KI-Systeme minimieren menschliche Fehler und sorgen für eine konsistente Qualität.
Bessere Entscheidungsfindung	KI kann große Datenmengen analysieren und wertvolle Einblicke liefern, die zu fundierteren Entscheidungen führen.
Skalierbarkeit	Prozesse können leicht skaliert werden, um den wachsenden Anforderungen des Unternehmens gerecht zu werden.
Wettbewerbsvorteil	Unternehmen, die KI frühzeitig und strategisch einsetzen, sichern sich einen entscheidenden Vorteil am Markt.

Tabelle 1: Vorteile von KI in der Prozessoptimierung

forderungen jedoch bei weitem auf. Unternehmen, die bereit sind, in intelligente KI-Lösungen zu investieren und ihre Belegschaft entsprechend einzubinden, setzen sich an die Spitze der digitalen Transformation.

Insgesamt zeigt sich, dass die künstliche Intelligenz nicht nur eine unterstützende Technologie ist, sondern ein fundamentaler Baustein moderner Geschäftsstrategien. Sie verändert, wie Unternehmen denken, operieren und konkurrieren. In den folgenden Abschnitten wird detailliert auf die spezifischen Technologien, die Implementierung und die damit verbundenen rechtlichen sowie ethischen Aspekte eingegangen.

IDENTIFIZIERUNG VON OPTIMIERUNGSPOTENZIALEN

Der Schlüssel zur erfolgreichen Anwendung von künstlicher Intelligenz in der Prozessoptimierung liegt in der präzisen Identifizierung von Verbesserungspotenzialen. Besondere Beachtung finden hierbei unter anderem die systematische Potenzialanalyse (SPA), das Reifegradmodell Digitale Prozesse 2.0 des Bitkom und das OBASHI-Modell.

Wie können KI-Technologien genutzt werden, um tiefgreifende Analysen bestehender Prozesse durchzuführen und Ineffizienzen sowie Automatisierungsmöglichkeiten aufzudecken? Zunächst bedarf es einer gründlichen Untersuchung der aktuellen Prozesse. Ein strukturiertes und methodisches Vorgehen ist dabei unerlässlich, um den größtmöglichen Nutzen zu erzielen.

1. **Prozessaufnahme und -analyse:** Der erste Schritt besteht in der gründlichen Erfassung und Analyse der aktuellen Geschäftsprozesse:
   - Workshops und Interviews: Mit Mitarbeitern und Führungskräften werden Engpässe und Ineffizienzen identifiziert.
   - Dokumentation: Modelle wie OBASHI helfen, Datenflüsse und Abhängigkeiten darzustellen.
   - Datenanalyse: Data-Mining-Techniken und KI-gestützte Tools erkennen Muster und Trends in großen Datenmengen. [6]
2. **Bewertung des KI-Potenzials:** Nach der Analyse folgt die Bewertung des KI-Potenzials:
   - ADE-Prinzip: Untersuchung auf Automatisierungspotenziale (A), Verbesserung des Datenzugriffs (D) und Entscheidungsoptimierung (E)[7]
   - Kosten-Nutzen-Analyse: Bewertung der Auswirkungen auf Kosten, Effizienz und Kundenzufriedenheit, um den ROI abzuschätzen[7]
3. **Priorisierung der Projekte:** Um Ressourcen optimal zu nutzen, werden Projekte priorisiert:
   - ROI-Bewertung: Priorisierung basierend auf ROI, Implementierbarkeit und strategischer Bedeutung
   - Proof of Concept (POC): Testen der Machbarkeit und Effektivität der priorisierten Projekte
4. **Einbindung der Mitarbeiter:** Der Erfolg der KI-Implementierung hängt von der Einbindung der Mitarbeiter ab:
   - Schulungen und Workshops: regelmäßige Trainings, um Akzeptanz und Verständnis zu fördern
   - Transparente Kommunikation: klare Kommunikation über Ziele und Vorteile der KI-Implementierung
5. **Kontinuierliche Verbesserung:** Nach der Implementierung sind die kontinuierliche Überwachung und Verbesserung entscheidend:
   - Monitoring: Fortlaufende Überwachung der KI-Systemleistung [8]
   - Feedback-Mechanismen: Daten sammeln und Systeme basierend auf Feedback anpassen und optimieren [8]

KI-gestützte Analysetools wie Open Source Data Mining und Predictive Analytics ermöglichen es zudem, Muster und Trends in großen Datenmengen zu erkennen, die menschlichen Analysten möglicherweise verborgen bleiben. Solche Werkzeuge können Daten auch in Echtzeit analysieren, wodurch sie nicht nur Probleme erkennen, sondern auch proaktive Maßnahmen ergreifen können, um Ineffizienzen vor ihrer Entstehung zu eliminieren. [9] Wichtig hierbei ist wiederum die Einbindung der Mitarbeiter, um sicherzustellen, dass ihr Wissen und ihre Erfahrungen in die Analyse einfließen und die Akzeptanz der Veränderungen gefördert wird.

Ein weiterer entscheidender Schritt ist die Bewertung der Automatisierbarkeit von Prozessen. Hier setzt KI an, indem sie repetitive und vorhersehbare Aufgaben identifiziert, die für eine Automatisierung geeignet sind. Machine-Learning-Algorithmen sind besonders wertvoll, da sie kontinuierlich aus den durchgeführten Operationen lernen und sich entsprechend anpassen können. Dies führt nicht nur zu einer Reduktion der Fehlerquote, sondern auch zur Freisetzung

Bilder: DALL-E

wertvoller Ressourcen, die dann für strategischere Aufgaben eingesetzt werden können. [10] Zudem sollte darauf geachtet werden, dass die Prozesse flexibel bleiben und weiterentwickelt werden können, um nicht vollständig von externen Ressourcen abhängig zu sein.

Die Akzeptanz der KI im Unternehmen wird zudem maßgeblich dadurch gefördert, dass Optimierungen in den routinemäßigen Geschäftsprozessen der Mehrheit durchgeführt und Wiederholungen automatisiert werden.

Ein praxisnahes Beispiel bietet der Einsatz von KI in der Supply-Chain-Optimierung. Hier ermöglichen KI-Systeme eine genauere Vorhersage der Nachfrage und eine effizientere Lagerhaltung, was zu erheblichen Kosteneinsparungen führt. Unternehmen, die KI in ihre Lieferketten integrieren, berichten von einer Verbesserung der Liefergenauigkeit und einer Reduzierung von Lagerhaltungskosten um bis zu 25 Prozent. [11]

INTEGRATION VON KI-LÖSUNGEN IN BESTEHENDE IT-INFRASTRUKTUREN

Die nahtlose Integration von KI in bestehende IT-Systeme stellt eine der größten Herausforderungen, aber auch eine der vielversprechendsten Chancen für moderne Unternehmen dar. Praktikable Integrationen können durch den Einsatz verschiedener KI-Technologien erreicht werden, wie beispielsweise generative KI (GenAI) und große Sprachmodelle (LLMs). Diese Technologien können entweder On-Premises betrieben oder in der Cloud gehostet werden, je nach den spezifischen Anforderungen und Sicherheitsbedenken des Unternehmens. Eine sorgfältige Auswahl und Implementierung der geeigneten Technologie ist entscheidend, um sowohl die technischen als auch die organisatorischen Aspekte der Integration erfolgreich zu meistern.

Bestandsaufnahme der IT-Landschaft

Zu Beginn ist eine umfassende Bestandsaufnahme der vorhandenen IT-Landschaft unerlässlich. Diese Analyse soll sicherstellen, dass die Systeme, die für die Integration von KI vorgesehen sind, sowohl technisch als auch hinsichtlich ihrer Sicherheitsarchitektur auf dem neuesten Stand sind. Tools wie System-Management-Plattformen können dabei helfen, einen klaren Überblick über die IT-Infrastruktur zu erhalten und potenzielle Kompatibilitätsprobleme frühzeitig zu identifizieren. [12]

Sicherstellung der Datenqualität und -integrität

Ein entscheidender Aspekt bei der Integration von KI ist die Sicherstellung der Datenqualität und -integrität. Daten sind das Fundament jeder KI-Anwendung, und ihre Qualität bestimmt maßgeblich die Effektivität der KI-Lösungen. Unternehmen müssen robuste Datenbereinigungs- und -verarbeitungsverfahren implementieren, um die Genauigkeit und Zuverlässigkeit der von KI-Systemen genutzten Daten zu gewährleisten. [13] Darüber hinaus ist es wichtig, die Mitarbeiter in den Prozess der Datenaufbereitung einzubeziehen, um deren Fachwissen zu nutzen und die Akzeptanz der KI-Lösungen zu erhöhen.

Anpassung der Sicherheitsprotokolle

Die Implementierung von KI erfordert auch eine Anpassung der Sicherheitsprotokolle. Da KI-Systeme häufig auf große Mengen sensibler Daten zugreifen, müssen erweiterte Sicherheitsmaßnahmen wie verschlüsselte Datenübertragungen und fortschrittliche Authentifizierungsmethoden implementiert werden, um Datenschutz und Compliance zu garantieren. [14] Gleichzeitig sollten Mitarbeiterschulungen zur Sensibilisierung für neue Sicherheitsanforderungen durchgeführt werden, um menschliche Fehler zu minimieren.

Schulungs- und Weiterbildungsprogramme

Um die Akzeptanz und den erfolgreichen Betrieb von KI innerhalb der Organisation zu fördern, ist es außerdem notwendig, Schulungs- und Weiterbildungsprogramme für die Mitarbeiter zu entwickeln. Diese Programme sollen nicht nur technische Fähigkeiten vermitteln, sondern auch ein Verständnis für die Möglichkeiten und Grenzen der KI fördern. [15] Dabei ist es entscheidend, dass die Mitarbeiter die Bedeutung ihrer Rolle in einem zunehmend automatisierten Umfeld verstehen und sich aktiv an der Weiterentwicklung der Prozesse beteiligen können.

Fortlaufende Überwachung und Optimierung

Abschließend sind die fortlaufende Überwachung und Optimierung der KI-Systeme entscheidend. Unternehmen sollten Feedback-Mechanismen und kontinuierliche Bewertungsprozesse etablieren, um die Leistung der KI-Anwendungen zu überwachen und bei Bedarf Anpassungen vorzunehmen. Dies sichert nicht nur die langfristige Leistungsfähigkeit der KI-Lösungen, sondern auch ihre Anpassungsfähigkeit an sich ändernde Geschäftsanforderungen. [16] Dabei sollten regelmäßige Audits und Reviews durchgeführt werden, um sicherzustellen, dass die KI-Systeme nicht nur effizient, sondern auch ethisch und rechtlich einwandfrei arbeiten.

FALLSTUDIEN UND ERFOLGSGESCHICHTEN

Das Potenzial von KI wird besonders greifbar, wenn man konkrete Anwendungsbeispiele betrachtet. In diesem Kapitel präsentieren wir einige Fallstudien und Erfolgsgeschichten, die illustrieren, wie KI in verschiedenen Branchen erfolgreich eingesetzt wird.

Automobilindustrie – Autonome Fahrzeugtechnologien

Ein führendes Automobilunternehmen hat mithilfe von KI-Technologien die Sicherheit und die Effizienz seiner Fahrzeuge verbessert. Durch den Einsatz von Deep Learning wurden die Algorithmen für autonomes Fahren optimiert, was zu einer signifikanten Reduzierung von Unfällen und einer Verbesserung der Verkehrseffizienz geführt hat. [17] Diese Innovation wurde in enger Zusammenarbeit mit den Ingenieuren und Fahrzeugsicherheitsexperten entwickelt, um sicherzustellen, dass die KI-Systeme nicht nur technisch fortschrittlich, sondern auch zuverlässig und sicher sind.

Finanzsektor – Betrugserkennung

Eine große Bank implementierte ein KI-gestütztes System zur Betrugserkennung, das auf Machine Learning basiert. Dieses System konnte betrügerische Transaktionen mit einer Genauigkeit von über 90 Prozent identifizieren und verhindern, was zu enormen Einsparungen bei den Betrugsbekämpfungskosten führte. [18] Die Einführung dieses Systems erfolgte schrittweise, wobei die Bankengemeinschaft und die Kunden kontinuierlich informiert und in den Prozess einbezogen wurden, um Vertrauen in die neuen Technologien zu schaffen und mögliche ethische Bedenken frühzeitig zu adressieren.

Gesundheitswesen – Diagnoseunterstützung

In einem Krankenhaus wurde KI eingesetzt, um Diagnoseverfahren zu verbessern. KI-Algorithmen, die auf Bilderkennungstechnologien basieren, unterstützen Ärzte bei der Erkennung von Krankheiten wie Krebs in frühen Stadien, was die Behandlungserfolge deutlich verbessert. [19] Die Implementierung dieser Technologien erfolgte in enger Zusammenarbeit mit medizinischem Fachpersonal, das regelmäßig geschult wurde, um die KI-Ergebnisse korrekt zu interpretieren und in die klinische Praxis zu integrieren. Dies zeigt, wie wichtig die menschliche Beteiligung und das Vertrauen in die Technologie für den Erfolg von KI-Anwendungen im Gesundheitswesen sind.

Einzelhandel – personalisierte Kundenansprache

Ein führendes Einzelhandelsunternehmen nutzt KI, um das Einkaufserlebnis zu personalisieren. Durch die Analyse von Kundendaten kann das Unternehmen personalisierte Angebote erstellen, die zu einer höheren Kundenbindung und gesteigerten Verkaufszahlen führen. [20] Die Integration von KI in das Marketing des Unternehmens wurde durch umfangreiche Schulungen und die Einbindung von Marketingexperten unterstützt, um sicherzustellen, dass die Technologie effektiv genutzt wird und die Kundenansprache ethisch vertretbar bleibt. Zudem wurden Feedback-Mechanismen implementiert, um die personalisierten Angebote kontinuierlich zu optimieren und den Kundenwünschen anzupassen.

Diese Fallstudien illustrieren nicht nur den erfolgreichen Einsatz von KI in verschiedenen Branchen, sondern auch die Bedeutung der menschlichen Beteiligung, kontinuierlichen Schulung und ethischen Überlegungen bei der Implementierung von KI-Systemen. Sie zeigen, dass der Schlüssel zum Erfolg darin liegt, technologische Innovationen mit dem Wissen und der Erfahrung der Mitarbeiter zu kombinieren sowie eine Kultur der verantwortungsvollen Nutzung von KI zu fördern. ■

Literatur

[1] *IT-SICHERHEIT, Chefsache Künstliche Intelligenz, DATAKONTEXT GmbH, Ausgabe 02/2024*

[2] *IT-SICHERHEIT, Einführung in die KI und Technologie, DATAKONTEXT GmbH, Ausgabe 03/2024*

[3] *McKinsey & Company, Artificial Intelligence: The next digital frontier?, McKinsey Global Institute, 2017*

[4] *Smith, John, The Impact of Artificial Intelligence on Business Operations, Journal of Business Technology, 2018*

[5] *Bauer, Helen, AI in Healthcare: A Revolutionary Approach, HealthTech Magazine, 2019*

[6] *Davenport, T. H., & Ronanki, R., Artificial Intelligence for the Real World, Harvard Business Review, 2018*

[7] *Brynjolfsson, E., & McAfee, A., The Business of Artificial Intelligence, Harvard Business Review, 2017*

[8] *Russell, S., & Norvig, P., Artificial Intelligence: A Modern Approach, Pearson, 2020*

[9] *Müller, Anna, Data Mining und Predictive Analytics: Werkzeuge zur Effizienzsteigerung, Journal of Business Analytics, 2020*

[10] *Schmidt, Lucas, Automatisierung durch Machine Learning: Ein Leitfaden für Unternehmen, Tech Innovations Magazine, 2021*

[11] *Jensen, Emily, KI in der Supply Chain: Vorteile und praktische Anwendungen, Logistics Today, 2019*

[12] *Keller, Thomas, Management von IT-Infrastrukturen: Eine Einführung, IT Systems Review, 2022*

[13] *Fischer, Julia, Datenqualität in KI-Anwendungen: Herausforderungen und Lösungen, Data Science Today, 2021*

[14] *Lang, Markus, KI und Datenschutz: Sicherheitsstrategien für Unternehmen, Cybersecurity Insights, 2021*

[15] *Meier, Sophia, Schulung und Weiterbildung in der Ära der KI, Education for Tomorrow, 2020*

[16] *Vogel, David, KI-Systeme erfolgreich managen: Überwachung und Optimierung, Tech Management Journal, 2022*

[17] *Weber, Stefan, KI in der Automobilindustrie: Fortschritte und Herausforderungen, Automotive Innovation, 2022*

[18] *Fischer, Julia, Betrugserkennung durch Machine Learning: Ein Finanzsektor-Fallbeispiel, Financial Technology Today, 2021*

[19] *Schwarz, Lisa, KI in der medizinischen Diagnostik: Vorteile und Grenzen, Medical Tech Review, 2020*

[20] *Bauer, Martin, Personalisierung im Einzelhandel durch KI: Fallstudien und Ergebnisse, Retail Tech Journal, 2021*

Dieser Text ist der dritte Teil einer Artikelserie über künstliche Intelligenz. Der vierte Teil in der nächsten Ausgabe der IT-SICHERHEIT wird sich mit den *rechtlichen Aspekten des Einsatzes von KI* befassen.

Folgende Themen sind Teil unserer KI-Serie:

- *Unternehmensführung in Zeiten von KI*
- *Einführung in KI und Technologie*
- ***Prozess-Optimierung durch KI***
- *Rechtliche Aspekte beim Einsatz von KI*
- *KI-Projekte sicher umsetzen*
- *KI im Feld der praktischen Anwendung*

Bild: DALL·E

MICHAEL THEUMERT,
ist Co-Founder der SECaaS.IT und kombiniert Technik-Expertise mit menschlicher Dynamik. Er gestaltet eine sinnvolle, sichere und freudvolle Zukunft und fokussiert sich auf sichere und nachhaltige Digitalisierung.

JÜRGEN KREUZ
Der Co-Founder der SECaaS.IT, ist Experte in Prozessoptimierung und IT-Governance. Mit langjähriger Erfahrung und zahlreichen Projekten bei kritischen Infrastrukturen leitet er den Consulting-Bereich und unterstützt Kunden bei IT-Sicherheits- und Prozessoptimierungen.

DR. DIETER STEINER
Der Unternehmer und Investor ist seit über 30 Jahren in der IT-Branche mit den Schwerpunkten IT-Security, Datenschutz, digitale Transformation, künstliche Intelligenz und Software-Entwicklung tätig.

Zusammenarbeit und Vertrauen im Kampf gegen Cyberkriminalität

DER WEG ZUR KOLLEKTIVEN CYBERRESILIENZ

Mit der Digitalisierung unserer Wirtschaft und Gesellschaft stehen Unternehmen weltweit vor der Herausforderung, ein komplexes Ökosystem aus Abhängigkeiten wie Internet of Things (IoT), Industrial Internet of Things (IIoT), Cloud Computing, künstliche Intelligenz (KI), Big Data, Blockchain-Technologien und Cybersecurity-Infrastrukturen zu verwalten. Die Verbreitung von IT, OT und IIoT – in Kombination mit einer wachsenden Bedrohungslage, sich entwickelnden regulatorischen Anforderungen und der zunehmenden Abhängigkeit von Lieferantennetzwerken – unterstreicht die Notwendigkeit einer umfassenden Cyberresilienz im gesamten Ökosystem.

Cyberresilienz ist die Fähigkeit eines Unternehmens, Cyberangriffe abzuwehren, angemessen darauf zu reagieren und sich mithilfe von Wiederherstellungsplänen schnell davon zu erholen. Angesichts der wachsenden Bedrohung durch Ransomware, Phishing und andere Malware ist diese Cyberresilienz von entscheidender Bedeutung. Denn Cyberangriffe führen zu verheerenden Betriebsunterbrechungen, Datenverlusten, Reputationsschäden und erheblichen Vertragsstrafen.

Die große Mehrheit der Unternehmen ist stark auf ein perfekt orchestriertes und komplexes Lieferantennetzwerk angewiesen. Besonders der deutsche Mittelstand, der oft als Rückgrat der Wirtschaft bezeichnet wird, ist in hohem Maße von zuverlässigen Zulieferern und Partnern abhängig, um seine Produktionsprozesse aufrechtzuhalten. Bei sogenannten Supply-Chain-Attacken werden die schwächeren Glieder in der Lieferkette angegriffen, um die gesamte Produktionskette zu gefährden. So hackten Cyberkriminelle der Qilin-Gruppe im November 2023 den weltweit agierenden Automobilzulieferer Yanfeng. Das Unternehmen fertigt Innenraumkomponenten für Stellantis (Chrysler, Dodge, Jeep und Ram), VW, BMW und Daimler an. Als Folge des Ransomware-Angriffs musste Stellantis gezwungenermaßen die Produktion in mehreren nordamerikanischen Montagewerken für mehr als eine Woche aussetzen.

Im Kontext der Cyberresilienz scheinen individuelle Ansätze daher unzureichend. Diese umfassen unter anderem regelmäßige Schulungen zur Sensibilisierung der Mitarbeitenden für Cyberbedrohungen sowie die Implementierung technischer Maßnahmen wie Firewalls und Verschlüsselung, um die Sicherheit der Systeme zu gewährleisten. Darüber hinaus ist jedoch ein kollektiver Ansatz unerlässlich, um das gesamte Netzwerk der kooperierenden Unternehmen effektiv gegen Cybergefahren zu schützen.

Was ist der Schlüssel zum Erfolg in einer derartigen dynamischen Umgebung? Es ist das digitale Vertrauen. Durch die Annahme eines „ökosystemischen" Ansatzes, der auf den Prinzipien des digitalen Vertrauens basiert, werden widerstandsfähigere Netzwerke realisiert. Das bedeutet, dass alle Teile des Netzwerks zusammenarbeiten und sich gegenseitig unterstützen, um Angriffe und Ausfälle effektiver abzuwehren. Dadurch wird das gesamte Netzwerk robuster und sicherer.

Ein ökosystemischer Gedankengang kann einen Paradigmenwechsel in der Betrachtung wechselseitiger digitaler Abhängigkeiten bewirken und hat bedeutende Auswirkungen auf die Effektivität der Zusammenarbeit innerhalb des Netzwerkes. Unternehmen, die digitales Vertrauen und Kooperation in ihrem Ökosystem ermöglichen, werden besser in der Lage sein, die vielfältigen und zunehmend komplexen Herausforderungen einer sich ausweitenden Bedrohungslage zu überleben.

FÜR RESILIENZ IST EIN GANZHEITLICHER ANSATZ GEFRAGT

Um in der heutigen Cyberlandschaft wirklich resilient zu sein, müssen Unternehmen ihre digitalen Ökosysteme als Ganzes betrachten. Denn moderne Unternehmen sind keine simplen, isolierten Einheiten mehr, sondern zunehmend Teil vernetzter Ökosysteme, die übergreifend neue Möglichkeiten für Innovation, Effizienz und Wachstum bieten können. In der heutigen hypervernetzten Umgebung spielt digitales Vertrauen eine zentrale Rolle, da zunehmende Verbindungen bedeutende neue Herausforderungen mit sich bringen und eine entsprechende Transformation der Resilienz erfordern.

Unternehmen sind innerhalb ihrer Lieferantennetzwerke in wachsendem Maße abhängig von Dritt-, Viert- und Fünftparteien. Dabei beziehen sich Drittparteien auf direkte Lieferanten oder Dienstleister, mit denen ein Unternehmen einen Vertrag hat. Viertparteien sind die von diesen Drittparteien beauftragten Subunternehmen, während Fünftparteien wiederum von den Viertparteien engagierte Dienstleister sind. Diese Kategorisierung hilft Unternehmen, die Komplexität ihrer Lieferketten zu verstehen und potenzielle Risiken zu identifizieren, die von verschiedenen Ebenen der Dienstleister ausgehen könnten. Diese Form der Zusammenarbeit bietet nicht nur erhebliche Vorteile, sondern birgt auch neue Risiken, die verwaltet werden müssen. Laut dem Bericht „Foresight Cybersecurity Threats For 2030" der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) ist die „Kompromittierung der Lieferkette von Softwareabhängigkeiten" die größte Bedrohung für Unternehmen.

Da Informationssicherheitsbeauftragte zunehmend die wachsenden Risiken in Lieferketten verstehen, nimmt das Misstrauen und die Ausweitung von Managementkontrollen für Gefahren durch Drittparteien entsprechend zu. Gleichzeitig erkennen Regierungsinstitutionen weltweit ihre signifikante Rolle bei der Stärkung der digitalen Resilienz und der Förderung des digitalen Vertrauens. In einigen der neuesten nationalen Cybersicherheitsstrategien beschreiben nationale Sicherheitsbehörden oder ähnliche Institutionen die Notwendigkeit eines resilienten digitalen Ökosystems, zum Beispiel die US National Cybersecurity Strategy 2023, die UK Government Cyber Security Strategy 2022–2030 und die 2023–2026 Australian Cyber Security Strategy. Gleichzeitig erhöht der zunehmende Einfluss staatlicher Stellen auf die Resilienz durch Vorschriften wie die neue Network and Information Security Directive (NIS-2) der EU, die Critical Entities Directive (CED), den Digital Operational Resilience Act (DORA) sowie den Cyber Resilience Act (CRA) – den Druck und die Komplexität für Unternehmen.

Mit der sich entwickelnden Bedrohungs- und IT-Landschaft müssen sich auch die Resilienzstrategien entsprechend weiterentwickeln, um die Überlebensfähigkeit der Unternehmen zu gewährleisten. Letztlich haben Konsumierende digitaler Technologien steigende Erwartungen an die Zuverlässigkeit und Vertrauenswürdigkeit ihrer genutzten digitalen Produkte und Dienstleistungen. Einen transparenten Ansatz für digitales Vertrauen zu verfolgen, um den sich wandelnden Erwartungen der Kunden gerecht zu werden, wird für Unternehmen immer wichtiger. Dadurch können sie sich deutlich von der Konkurrenz abheben und ihre Vertrauenswürdigkeit sowie ihre Zuverlässigkeit stärken.

EINE KOLLEKTIVE UND LANGFRISTIGE STRATEGIE IST UNERLÄSSLICH

Da der Informationsaustausch immer wichtiger wird, können vertrauensbildende Technologien, wie zum Beispiel sichere Verschlüsselungsver-

fahren, eine bessere Zusammenarbeit zwischen Partnern in einem Ökosystem ermöglichen und fördern. Diese Technologien schützen die Privatsphäre und gewährleisten, dass Daten sicher und zuverlässig geteilt werden können, wodurch die Partner effektiver zusammenarbeiten und Vertrauen aufbauen können. Anstelle von rein compliancebasierten Vereinbarungen wie Service Level Agreements (SLAs) und Data Processing Agreements (DPAs) zwischen Unternehmen würden die beteiligten Partner von der Kooperation profitieren.

Eine ökosystemische Perspektive macht bereits für viele Unternehmen einen großen Unterschied. Nicht nur Weltkonzerne wie Microsoft, Apple oder Google erkennen, dass ihre Prozesse, ihre Effizienz und ihre Wettbewerbsfähigkeit von einer Vielzahl von Lieferanten aus unterschiedlichen Branchen abhängen. Auch im deutschen Mittelstand ist hier vieles in Bewegung. Teilweise bieten Unternehmen Plattformen an, auf denen die jeweiligen Partner Ressourcen gemeinsam nutzen können, was dem gesamten Ökosystem einschließlich dem Plattformanbieter zugutekommt. In anderen Fällen geht es darum, das komplette Ökosystem widerstandsfähiger zu machen.

Nicht nur ein globaler Chiphersteller oder ein führendes Technologieunternehmen sollte sich darüber im Klaren sein, dass ein (Hightech-) Produktionsprozess vollständig von einer Vielzahl unterschiedlicher Zulieferer abhängt und ein kostspieliger Cyberangriff auf einen dieser Zulieferer das gesamte Geschäft beeinträchtigen kann. Um die Widerstandsfähigkeit des Systems zu erhöhen, wird in vielen Unternehmen des deutschen Mittelstandes begonnen, Ressourcen, die ursprünglich für die eigene Cybersecurity vorgesehen waren, mit seinen Partnern zu teilen und entsprechend umgekehrt von deren Sicherheitsressourcen zu profitieren.

Viele Unternehmen investieren jedoch nach wie vor in ihre eigene Cybersicherheit, bevor sie sich mit der Sicherheit ihrer Zulieferer befassen. Gründe dafür sind begrenzte finanzielle Mittel, Kompetenzen oder Technologien. Doch Vorsicht: Im Gegensatz zu einem langfristig angelegten Ansatz bringt das nur kurzfristige Vorteile, da sich die Bedrohungen ausweiten und komplexer werden können. Aus diesem Grund sollte der Cybersicherheitsansatz von kurzfristigen Optimierungen zu langfristigen Strategien übergehen – von individueller Sicherheit zu kollektiver Resilienz.

Der Aufbau eines wirklich cyberresilienten Ökosystems erfordert eine langfristige Vision und einen strategischen Schritt-für-Schritt-Ansatz:

1. Unternehmen sollten damit beginnen, ihr gesamtes digitales Ökosystem zu modellieren, um die jeweiligen Abhängigkeiten zu visualisieren, auch solche, die ihnen (noch) nicht bewusst sind.

2. Unternehmen sollten anschließend den inneren Kreis ihres Ökosystems zusammenbringen, gegenseitige Abhängigkeiten und Risiken diskutieren und eine klare Vision, Ziele und Strategien festlegen, zu denen sich jedes Unternehmen verpflichten kann.

3. Unternehmen sollten ihr Ökosystem weiterentwickeln und stärken, indem sie digitales Vertrauen aufbauen. Es sollten klare Grenzen und Richtlinien festgelegt werden, innerhalb derer Ressourcen zur Optimierung der Cybersicherheit geteilt werden können. Die Rolle jedes teilnehmenden Unternehmens muss klar definiert sein, und jeder Partner im Ökosystem sollte eine komplementäre Rolle übernehmen. Diese Rollen können sich im Laufe der Zeit ändern. Der Datenaustausch innerhalb des Ökosystems sowie die Sicherstellung des Vertrauens sind von zentraler Bedeutung. Vertrauensbildende Technologien spielen dabei eine wichtige Rolle.

Das Definieren, Entwickeln und Zusammenbringen der jeweiligen Ökosystempartner bietet keine schnelle Lösung oder kurzfristige Gewinne. Es erfordert Führungspersönlichkeiten mit einer langfristigen Vision und der Fähigkeit, alle Kooperationspartner in einem klaren Plan zu vereinen:

1. **Das Abbilden des Ökosystems und der Strategie:** Unternehmen sollten alle Abhängigkeiten identifizieren, einschließlich derer von Viertanbietern. Zudem müssen sie eine Ökosystemstrategie mit klaren Zielen entwerfen, indem sie die Partner im Ökosystem zusammenbringen und einen mehrjährigen Plan zur Stärkung und Verwaltung der Cyberresilienz aufstellen

2. **Die Auswahl digitaler Ökosystempartner:** Jedes Unternehmen hat in einem effektiven Ökosystem eine ergänzende Rolle zu spielen. Unternehmen sollten entscheiden, welchen Partner sie in ihr Ökosystem einbinden und welchen nicht, um eine effektive Zusammenarbeit und positive Ergebnisse zu erzielen.

3. **Die Entwicklungsunterstützung des digitalen Ökosystems:** Sobald die Unternehmen sich mit ihren Partnern zusammenschließen, können Fachexperten ein sogenanntes Ecosystem-Maturity-Framework erstellen, das die wichtigsten Bausteine für den Erfolg bereitstellt.

4. **Die Optimierung des digitalen Ökosystems:** Um die Prozesse und Sicherheitsmaßnahmen in ihrem digitalen Ökosystem zu verbessern, sollten Unternehmen einen „Ökosystem-Health-Check" durchführen, der Beziehungen zu Dritten und der Prozesse in ihrem digitalen Ökosystem bewertet.

DIGITALES VERTRAUEN IST DIE GRUNDLAGE FÜR EIN WIDERSTANDSFÄHIGES ÖKOSYSTEM

Neben einer soliden Strategie, einer Governance-Struktur und klar definierten finanziellen und rechtlichen Grenzen ist digitales Vertrauen eine der wichtigsten Komponenten eines wirklich cyberresilienten Ökosystems. Expertinnen und Experten haben gemeinsam mit dem Weltwirtschaftsforum (WEF) und anderen Partnern ein globales Rahmenwerk für digitales Vertrauen entwickelt. Das Framework dient als Entscheidungshilfe für Unternehmen und ermöglicht die Entwicklung und den Einsatz vertrauenswürdiger Technologien und damit eine vertrauensvolle Zusammenarbeit im gesamten Ökosystem. Das WEF definiert digitales Vertrauen als die öffentliche Erwartung, dass „digitale Technologien und Dienstleistungen – und die Unternehmen, die sie anbieten – die Interessen aller Beteiligten schützen und gesellschaftliche Erwartungen und Werte aufrechterhalten".

Das Framework bietet einen Fahrplan für die dynamische digitale Landschaft sowie klare Pläne, um die Anpassungsfähigkeit und Cyberresilienz digitaler Ökosysteme zu optimieren. Der Rückgriff auf ein einheitliches Framework, das gemeinsame Standards und Praktiken bietet, fördert die Zusammenarbeit, die Konsistenz und das Vertrauen in sich ständig weiterentwickelnde Technologien und stärkt gleichzeitig die

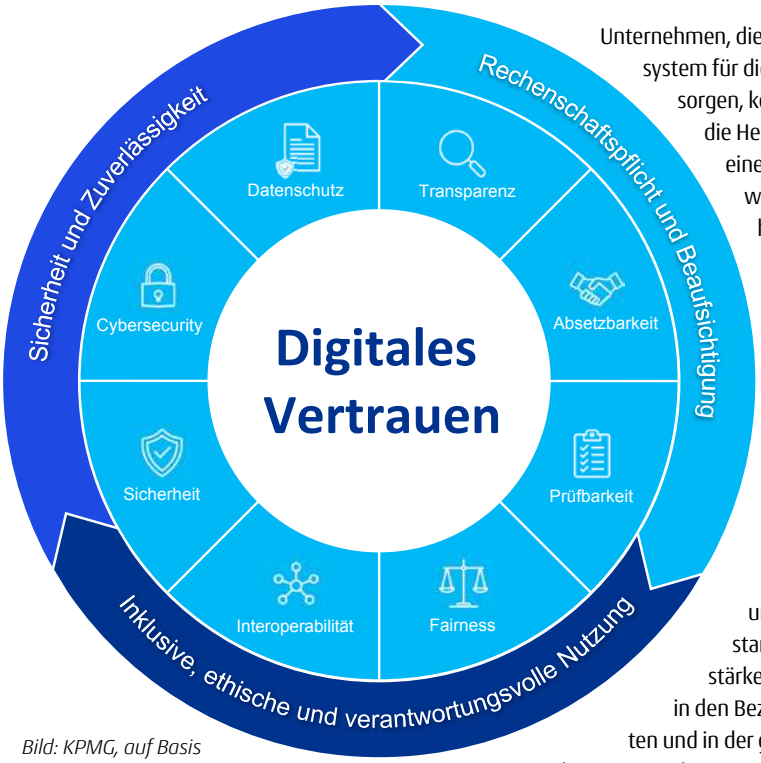


Bild: KPMG, auf Basis von World Economic Forum

Abwehrkräfte des Ökosystems gegen potenzielle Bedrohungen. Der digitale Vertrauensrahmen umfasst drei Ziele:

- Sicherheit und Zuverlässigkeit
- Rechenschaftspflicht und Aufsicht
- inklusive, ethische und verantwortungsvolle Nutzung

Diese Ziele sind in acht Dimensionen unterteilt: Cybersicherheit, Sicherheit, Transparenz, Interoperabilität, Überprüfbarkeit, Wiedergutmachbarkeit, Fairness und Datenschutz. Es ist von größter Bedeutung, alle jene Dimensionen zu berücksichtigen, um die drei Ziele des Vertrauensrahmens zu erreichen.

Vertrauen und Zusammenarbeit zwischen den Partnern im digitalen Ökosystem sind unerlässlich, um ein wirklich cyberresistentes Unternehmen zu werden. Der Ökosystem-Ansatz in Verbindung mit dem Digital Trust Framework ist ein guter Ausgangspunkt. Resilienz ist keine Option mehr, sondern in der heutigen, zunehmend komplexen Umgebung von entscheidender Bedeutung. Wenn Unternehmen die Zusammenarbeit in ihrem digitalen Ökosystem auf der Grundlage eines gemeinsamen Verständnisses von Vertrauen aufbauen und fördern, können sie die Ressourcenzuweisung optimieren und Risiken in der Lieferkette in Chancen umwandeln.

Unternehmen, die in ihrem Ökosystem für digitales Vertrauen sorgen, können nicht nur die Herausforderungen einer immer größer werdenden Bedrohungslandschaft meistern, sondern auch langfristig erfolgreicher werden. Wo also beginnen? Dazu folgende Fragen:

1. Inwiefern nutzt ein Unternehmen digitales Vertrauen, um seine Widerstandsfähigkeit zu stärken und neue Risiken in den Beziehungen zu Dritten und in der gesamten Lieferkette zu mindern?
2. Welche Erwartungen haben Kunden und Stakeholder in Bezug auf digitales Vertrauen und wie können sie diese heute und in Zukunft erfüllen?
3. Wie kann digitales Vertrauen als wichtiges Unterscheidungsmerkmal dienen und den Ruf ihrer Marke in Regionen oder Sektoren verbessern, in denen vertrauenswürdige Lösungen die Norm sind?

Wenn Unternehmen sich diese Fragen stellen und ihre Bemühungen gegenüber Stakeholdern und Kunden offenlegen, können sie ihre Anstrengungen zur Optimierung der digitalen Resilienz innerhalb des Ökosystems demonstrieren.

FAZIT

Mit der Zunahme digitaler Abhängigkeiten, die sowohl die Risiken als auch das Misstrauen exponentiell verstärken, steigen die Ausgaben für die Cybersicherheit. Dies erfordert einen Paradigmenwechsel hin zu einer modernen Perspektive, die über die konventionellen Ansätze zum Schutz unserer zunehmend vernetzten Umgebungen hinausgeht.

Unternehmen sollten sich stärker darauf konzentrieren, durch einen kollektiven Ansatz widerstandsfähiger zu werden, der über die Sicherheit einzelner Unternehmen hinausgeht. Visionäre Führungspersönlichkeiten im Bereich der Cybersicherheit sollten die langfristige Strategie mit ihren Partnern im Ökosystem festlegen und auf persönlicher Ebene Vertrauen aufbauen, indem sie das Potenzial von Vertrauenstechnologien nutzen. Nur dann werden wir in der Lage sein, effizient widerstandsfähige digitale Gesellschaften zu erschaffen. ■

FLORIAN THIESSENHUSEN,
Senior Manager Cyber Security KPMG AG, ist seit über 20 Jahren im Bereich der Cyber Security tätig und hat umfangreiche Erfahrungen in allen Facetten dieses kritischen Feldes gesammelt. Derzeit liegt sein Fokus bei seinem aktuellen Arbeitgeber auf der Wiederherstellung nach Cyber-Angriffen sowie der Prävention solcher Vorfälle.

JIM BOEVINK,
Senior Consultant Cyber Security KPMG Niederlande, kommt aus dem öffentlichen Sektor. Er hat sich auf das Konzept digitaler Ökosysteme spezialisiert und übersetzt dieses Wissen in den Cyber-Bereich.
Er verfügt außerdem über Fachkenntnisse in den Bereichen Business Continuity Management, Risikomanagement und Strategieentwicklung.

Mit freundlicher Unterstützung von
AUGUSTINUS MOHN,
Senior Manager Cyber Security KPMG Niederlande und
ANNEMARIE ZIELSTRA,
Partnerin Cyber Security KPMG Niederlande

NIS-2 und die Operational Technology

(K)EIN TRAUERMÄRCHEN

NIS-2 ist keine reine IT-Sicherheitsübung. Die Gesetzgebung verankert Cybersicherheit auch in industriellen Infrastrukturen. Die Herausforderung besteht darin, die sogenannte OT-Sicherheit schlank, handhabbar und dennoch konsequent und sinnvoll umzusetzen. Gründe dafür gibt es für Unternehmen auch abseits der Paragraphen genug.

Die NIS-2-Richtlinie und das daraus resultierende NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) bedeuten für Tausende deutsche Unternehmen in mehrfacher Hinsicht Neuland. Zum einen werden sie ab Oktober 2024 gesetzlich zu nachweisbarer Cybersicherheit verpflichtet. Zum anderen müssen sie sich erstmals auch gezielt mit der Cybersicherheit ihrer industriellen Infrastrukturen – der Steuerungs- und Prozessleittechnik beziehungsweise der Operational Technology (OT) – auseinandersetzen.

Stand Mai 2024 verpflichtet § 30 (1) des Referentenentwurfs des NIS2UmsuCG Einrichtungen dazu, *„geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Dabei sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen."*

Dieser Absatz des NIS2UmsuCG gibt der OT gleich doppeltes Gewicht:

1. Der Verweis auf die für die Leistungserbringung relevanten Systeme macht die OT automatisch zur essenziellen Infrastruktur, da sie für die Wertschöpfung unabdingbar ist.

2. Der Fokus auf die Risikoexposition gibt der OT einen besonderen Stellenwert, denn OT-Komponenten und -Netze waren in der Vergangenheit von Cybersicherheit komplett ausgenommen.

ES GIBT KEINE SICHERE OT

Dass die OT im Kern unsicher ist, lag (und liegt noch immer) am Fokus der Komponentenhersteller und Betreibenden auf Verfügbarkeit, Prozessstabilität und Einfachheit. Die Cybersicherheit hat erst in den letzten Jahren aufgrund der zunehmenden OT-Störungen durch Cyberangriffe an Relevanz gewonnen (siehe Abbildung 1).

Das bestätigen auch die Schwachstellenanalysen, die wir initial bei der Implementierung eines Angriffserkennungssystems in den OT-Netzen unserer Kunden durchführen: 2023 identifizierten wir durchschnittlich 26 versteckte Schwachstellen in OT-Netzen, welche die Sicherheit und/oder Verfügbarkeit der Anlagen bedrohten (siehe Abbildung 2). Unsichere Authentifizierungsmethoden fanden sich in fast allen Netzen genauso wie veraltete und nicht benötigte Protokolle und Dienste. Meist wurden die Betreiber erst durch die Analysen auf die Schwachstellen aufmerksam. Denn neben fehlender Sicherheit mangelt es in der OT vor allen Dingen einem: Sichtbarkeit.

WAS BRAUCHT DIE OT AN MAßNAHMEN?

Grundsätzlich gelten mit NIS-2 für OT-Netze die gleichen Sicherheitsanforderungen wie für die Unternehmens-IT. Allerdings ergeben sich bei der Umsetzung in der OT einige Schwierigkeiten, die sich aus der spezifischen Zielsetzung

Bild: Kampan - stock.adobe.com

ableiten. Verfügbarkeit, Prozessstabilität und Kontinuität stehen in der OT weit vor den Zielen Sicherheit und Integrität. Darüber hinaus ergeben sich aus den OT-spezifischen Eigenschaften einige Konflikte mit NIS-2, wie in Tabelle 1 auf der nächsten Seite dargestellt.

Die Ziele einer sinnvollen OT-Sicherheitsstrategie müssen deshalb sein:

1. Sichtbarkeit auf die Assets und Sicherheitsvorfälle zu schaffen,
2. die bestehenden Restrisiken und Schwachstellen zu kennen und zu kontrollieren (das heißt, zu überwachen),
3. das Sicherheitsteam zu befähigen, schnell und gezielt auf Störungen zu reagieren,
4. internes OT-Sicherheits-Know-how aufzubauen.

REICHEN FIREWALLS UND SIEM?

Auch in der OT-Sicherheit bleiben Firewalls, Segmentierung und Security-Information-and-Event-Management-(SIEM)-Systeme wichtige Elemente der Angriffsabwehr, haben aber ihre klaren Grenzen.

Klassische Firewalls erkennen weder die vielen Zero-Day-Schwachstellen noch bösartige Netzwerkzugriffe, die authentische Zugangsdaten (stolen credentials) ausnutzen. Zwischen 2018 und 2022 stieg der Anteil der Angriffe ohne Malware von 39 Prozent auf 71 Prozent. Diese beruhen zu einem Großteil auf gestohlenen Zugangsdaten. Sind die Angreifer erst einmal im Netzwerk, hilft keine Firewall mehr – und die OT-Komponenten empfangen neue Nutzer gern mit offenen Armen.

Ein SIEM wiederum benötigt Unmengen an Daten, um Angriffsmuster zu erkennen. Ohne ein dediziertes OT-Monitoring, das diese Daten aus der OT-Kommunikation liefert, bleibt selbst das beste SIEM auf dem OT-Auge blind.

NIS-2-HERAUSFORDERUNGEN BEWÄLTIGEN

Die Sichtbarkeit (siehe Abbildung 3) und die Kontrolle des Restrisikos sind daher zentrale Themen der OT-Sicherheit. Beide Ziele können durch ein

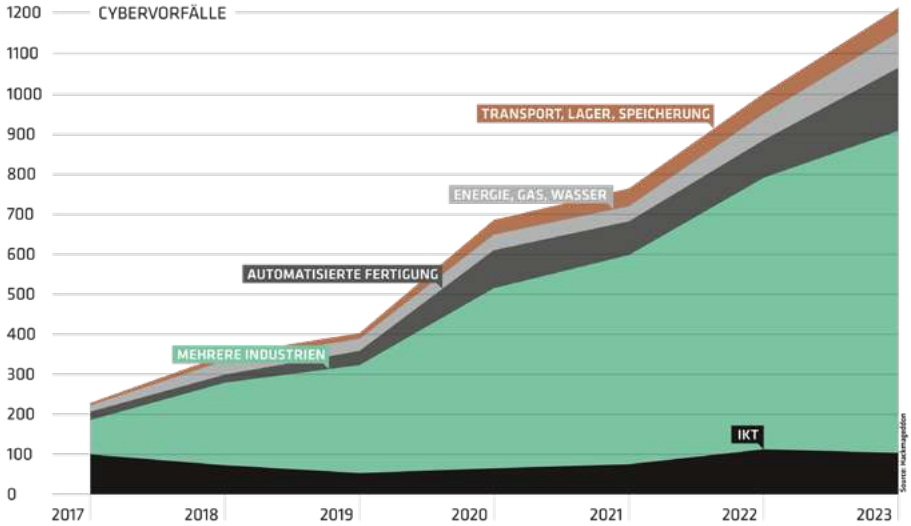


Abbildung 1: Öffentlich bekannt gewordene Cyberangriffe auf industriell geprägte Unternehmen nehmen jährlich zu. (Quelle: Rhebo/Hackmageddon)

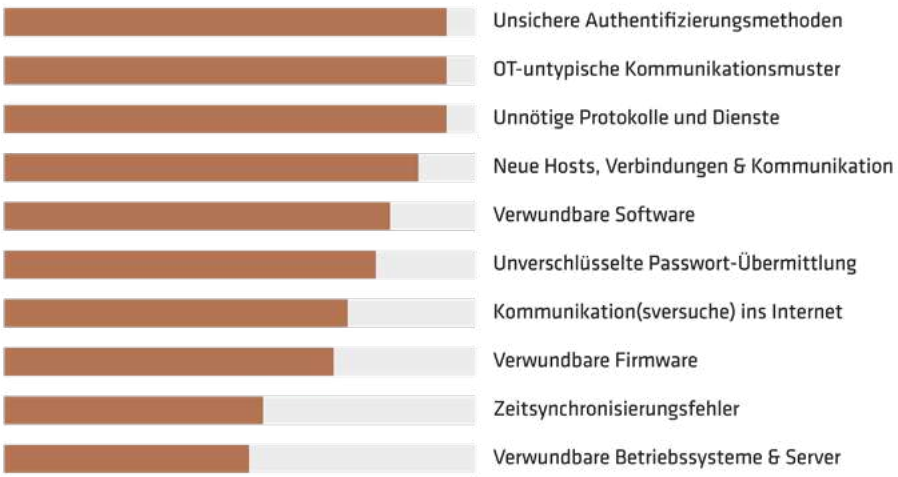


Abbildung 2: OT-Netzwerke stecken voller unbekannter Schwachstellen und Cyberrisiken. (Quelle: Rhebo, Ergebnisse aus Rhebo Industrial Security Assessments in 2023)

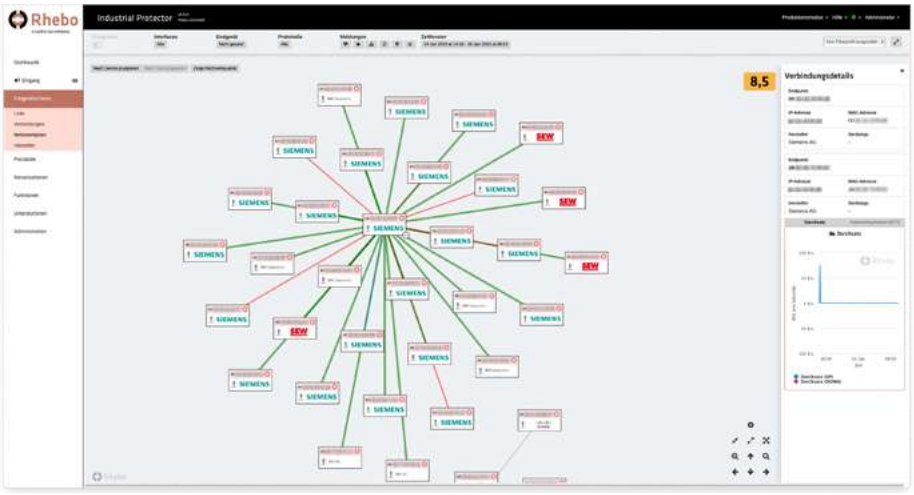


Abbildung 3: OT-Sicherheit basiert auf der Sichtbarkeit aller Assets im Netzwerk mit den dazugehörigen Eigenschaften. (Quelle: Rhebo)

NIS-2-Anforderung	Konflikte in der OT
Multi-Faktor-Authentifizierung (MFA) und Single-Sign-on (SSO)	▪ Bereitstellung der Infrastruktur und Gewährleistung der notwendigen Systemintegration ▪ beschränkte Einflussnahme auf Ausrüstung der Service- und Dienstleistungsunternehmen
Sichere Kommunikationskanäle	▪ ggf. DSGVO-Probleme mit Cloudanbietern ▪ VPN sind leicht zu kapern und auszunutzen
Verschlüsselte Kommunikation	▪ mögliche Konflikte mit Echtzeitprozessen ▪ teilweise fehlende Möglichkeiten bei Industrieprotokollen
Management von Schwachstellen	▪ „Insecure by design"-Komponenten ▪ lange Lebenszyklen ▪ verspätete Aktualisierung durch feste Wartungszyklen ▪ lückenhafte/fehlende Dokumentation der Assets ▪ Fragen der Prozessstabilität bei Aktualisierungen (never change a running system)
Risikoanalyse und Schwachstellenbewertung	▪ fehlende Sichtbarkeit ▪ Lückenhafte/fehlende Dokumentation der Assets
Bewältigung von Sicherheitsvorfällen	▪ fehlende Mechanismen, um sicherheitsrelevante Vorgänge zu erkennen ▪ aktive Abwehrmechanismen nur bedingt/nicht gewollt, um Prozesse und Arbeitsschutz nicht zu gefährden
Bewertung der Cybersicherheitseffektivität	▪ keine Defense-in-Depth-Architektur, die auch erfolgreiche Angriffe innerhalb des Netzwerkes erkennt (gilt häufig auch für die IT)
Business-Continuity-Prozesse	▪ fehlende Sichtbarkeit und Dokumentation sicherheitsrelevanter Vorgänge zur schnellen Lokalisierung und Nachvollziehbarkeit von Störungen
Sichere Supply Chain	▪ beschränkter/kein Einfluss auf Zuliefer- und Dienstleistungsunternehmen und deren Eingriffe in die konkrete OT
Qualifiziertes Personal	▪ Fachkräftemangel und/oder Überforderung

Tabelle 1: Die NIS-2-Anforderungen bergen in der OT einiges an Konfliktpotenzial.

netzwerkbasiertes Intrusion-Detection-System (Network-Intrusion-Detection-System, NIDS) erreicht werden. Es nutzt dabei die Eigenschaft der deterministischen, repetitiven Kommunikation in OT-Netzen, um Bedrohungen in Echtzeit zu erkennen, zu dokumentieren und zu melden. Es überwacht den gesamten laufenden Verkehr im OT-Netz, vergleicht ihn mit der Baseline und meldet Abweichungen.

Ein NIDS, das die OT schützt und zugleich die Betreibenden gegenüber der geltenden Rechtsprechung absichert, muss dabei einige spezielle Anforderungen erfüllen:

1. Es darf die OT weder bei der Integration noch im Betrieb beeinträchtigen. Das NIDS agiert passiv und rückwirkungsfrei, um sowohl die limitierte Bandbreite als auch die industriellen Prozesse nicht zu stören.

2. Es muss alle in der OT relevanten industriellen Protokolle analysieren können.

3. Es sollte alle Unregelmäßigkeiten erkennen, inklusive Anomalien, die bislang unbekannt sind oder über autorisierte Kanäle erfolgen, zum Beispiel Admin-Konten, Wartungszugänge, installierte Softwareupdates. Dadurch wird auch die NIS-2-Anforderung erfüllt, andere Sicherheitssysteme wie Firewalls oder Authentifizierungssysteme auf fehlerfreies Funktionieren zu überprüfen (Defense-in-Depth).

4. Es sollte unabhängig von den Systemherstellern sein und funktionieren, um Vendor Lock-in und Überwachungslücken zu vermeiden.

5. Es muss einfach zu bedienen sein. Sinnvolle Filter, aufgeräumte Oberflächen, automatisierte Risikobewertungen und Schnittstellen zu gängigen SIEM-Systemen wie Splunk und IBM QRadar reduzieren den internen Arbeitsaufwand im Betrieb. Treten bei identifizierten Anomalien Fragen auf, sollte ein Supportteam zur Verfügung stehen, um die Meldung zu analysieren.

In der OT (und auch in der IT) gibt es schon lange keine absolute Sicherheit mehr. Mit dem Fokus auf die Sichtbarkeit und Überwachung des Restrisikos schaffen Unternehmen eine Basis, um mit dieser permanenten Unsicherheit umzugehen. Dieses Prinzip des Defense-in-Depth in der OT-Sicherheit schützt die Perimeter mithilfe von bekannten Sicherheitsmechanismen vor gängigen Angriffsmustern, während ein NIDS die innere Sicherheit gewährleistet, erfolgreiche Netzwerkeinbrüche erkennt und alle verdächtigen Veränderungen meldet und dokumentiert. Dieses mehrstufige Sicherheitskonzept schafft nicht nur Rechtssicherheit. Es ist auch eine effektive Antwort auf die Herausforderungen von NIS-2 in der OT und die sich rasant verändernde Gefährdungslandschaft durch staatliche und kriminelle Akteure. ■

UWE DIETZMANN
ist Sales Manager bei der Rhebo GmbH.

IDS-Praxiseinsatz und Penetrationstest

ANGRIFFSERKENNUNG MIT IDS IN ENERGIEANLAGEN

Viele Angreifer haben mittlerweile ein tiefes Verständnis von Steuerungssystemen. Das ist spätestens seit den Cyberangriffen auf das ukrainische Stromnetz 2015, 2016 und 2022 sowie den jüngsten Attacken auf dänische Energieversorger klar. Diese bedrohlichen Entwicklungen erfordern zusätzliche Schutzmechanismen für Energieerzeuger und Umspannwerke. Dabei sind nicht nur rechtliche Rahmenbedingungen zu erfüllen, sondern es ist auch der optimale und effektive Einsatz für das Angriffserkennungssystem (Intrusion Detection System, IDS) umzusetzen. Unser Praxisbeispiel eines Penetrationstests veranschaulicht mögliche Angriffsszenarien und liefert wertvolle Erkenntnisse zur Angriffserkennung/-detektion.

Zur Gewährleistung der Versorgungssicherheit sind Betreiber von Energieversorgungsnetzen und Energieanlagen gemäß § 11 Abs. 1e Energiewirtschaftsgesetz (EnWG) dazu verpflichtet, angemessene Systeme zur Angriffserkennung einzusetzen. Geschützt werden müssen dabei die informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind [1].

Maßgeblich für das Kerngeschäft der Energieversorgung ist vor allem die Primär- und Sekundärtechnik eines Energieversorgungsunternehmens (EVU). Dazu zählen im Bereich der relevanten Komponenten beispielsweise Automatisierungs- und Leittechniksysteme, Schaltanlagen, Schutz- und Steuergeräte und Remote Terminal Units (RTUs). Solche Systeme sind unter anderem Leitstellen-Clients, Admin-Clients, Wartungs- und Prüf-Clients sowie dem OT-Netzwerk vorgelagerte Router, Switches und Firewalls. Diese gilt es, gegen Cyberangriffe und Störungen abzusichern.

Um den besonderen Anforderungen eines OT-Netzwerks gerecht zu werden, sollte ein System zur Angriffserkennung alle oben genannten Komponenten und Systeme, deren Kommunikation und die hierzu genutzten OT-Protokolle detailliert überwachen können.

Die technische Implementierung eines Angriffserkennungssystems ist nur ein Teil des Ganzen. Mindestens ebenso wichtig ist die prozessuale Einbindung. Dazu gehört insbesondere fachlich qualifiziertes Personal sowie die Prozesse des Incident-, Risk- und Business-Continuity-Managements.

Zur Erreichung und Aufrechterhaltung der teils komplexen Anforderungen eines Systems zur Angriffserkennung kann die Orientierungshilfe

des Bundesamtes für Sicherheit in der Informationstechnik (BSI) genutzt werden [2].

EINSATZ VON IDS: UNTERSCHIEDE ZWISCHEN IT UND OT

Vor der Implementierung eines IDS sollten die Verantwortlichen einige wichtige Fragen klären:

- Was soll konkret überwacht werden?
- Welches IDS beziehungsweise welcher Detektionsmechanismus soll verwendet werden?
- Was sind die Vor- und Nachteile eines IDS?

Ein weit verbreiteter Irrtum ist, dass man für das OT-Netzwerk, in dem Schaltbefehle und Steuerungssignale übertragen werden, dieselbe Angriffserkennung verwenden kann wie für das IT-Netz eines Unternehmens. OT- und IT-Netzwerke unterscheiden sich jedoch sehr stark in ihrer Funktionalität und in ihren Anforderungen (siehe Abbildung 1).

OT-Netzwerke müssen oft besonders robust und sicher sein, da ein Ausfall oder eine Störung schwerwiegende, mitunter lebensgefährdende Konsequenzen haben kann. Aus diesem Grund ist in diesen Netzwerken die Verfügbarkeit (Availability) von höchster Priorität, gefolgt von der Integrität (Integrity), welche die Korrektheit der Daten voraussetzt. Die Vertraulichkeit (Confidentiality) wird in einem OT-Netzwerk häufig am geringsten priorisiert. Schalt- oder Steuerbefehle werden meist unverschlüsselt und im Klartext im Netzwerk kommuniziert.

In der IT liegt dagegen der Fokus auf dem Schutz von Informationen und informationsverarbeitenden Systemen. Demzufolge ist die Vertraulichkeit von höchster Bedeutung, denn ein Datenverlust ist eine der häufigsten Bedrohungen in der IT.

Während Systemausfälle in der IT vor allem zu finanziellen Schäden für das Unternehmen führen, können Störungen oder Ausfälle von OT-Komponenten zu weitreichenden Folgen für die Versorgungssicherheit führen.

METHODEN DER ANGRIFFSERKENNUNG EINES IDS

Die Kernkomponente eines IDS ist dessen Detektionsmechanismus. Dazu gibt es verschiedene Ansätze:

- **Baseline-/Lernbasierter Ansatz:** In der Lernphase wird die Netzwerkkommunikation beobachtet und anhand dieser Beobachtungen lernt das System, was innerhalb dieses Netzwerks als normale Netzwerkkommunikation angenommen wird.
  - **Vorteil:** Unbekannte Angriffsmuster werden erkannt.
  - **Nachteil:** Netzwerkkommunikation, die in der Lernphase nicht erkannt wird, beispielsweise Schaltvorgänge oder Wartungsaktivitäten, löst einen Alarm aus. Unerwünschte Netzwerkkommunikation kann als Baseline erlernt werden.
- **Signaturbasierter Ansatz (Denylist):** Das IDS sucht nach Mustern, die es bereits von anderen Angriffen kennt.
  - **Vorteil:** Die Fehlalarmquote ist geringer als bei Systemen mit lernbasiertem Ansatz.
  - **Nachteil:** Angreifer können die Muster jedes Mal geringfügig ändern und damit einer Erkennung entgehen. Um dies zu vermeiden, müssen Signaturen „offener" definiert werden, was wiederum zu einer höheren Anzahl an Fehlalarmen führt.
- **Allowlist-Ansatz:** In OT-Netzwerken, besonders im Stromnetz, ist das Verhalten aller Geräte im Netzwerk klar definiert. Das IDS kann deswegen ein Live-Modell der zu überwachenden Betreiberanlage erstellen.
  - **Vorteil:** Abweichungen von der erlaubten Netzwerkkommunikation sind sofort erkennbar. Auch Signalwerte in den Nachrichten werden überwacht, sodass Cyberbedrohungen und Probleme bei den Funktionen präzise erkannt werden können.
  - **Nachteil:** Initial höherer Aufwand bei der ersten Inbetriebnahme.

VORTEILE UND HERAUSFORDERUNGEN EINES IDS

Intrusion-Detection-Systeme bieten eine Reihe von entscheidenden Sicherheitsvorteilen für OT-Netzwerke. So ist ein IDS in der Lage, Anomalien zu erkennen, die auf ungewöhnliche Aktivitäten oder verdächtige Netzwerkkommunikation hinweisen, noch bevor diese zu ernsthaften Sicherheitsvorfällen führen. Darüber hinaus ermöglicht ein solches System eine Echtzeitüberwachung, wodurch Bedrohungen sofort erkannt und darauf reagiert werden kann, was insbesondere für die Sicherheit von OT-Netzen von entscheidender Bedeutung ist.

Ein weiterer Vorteil ist die Unterstützung bei der Inventarisierung, indem es die automatische Identifizierung, Überwachung und Dokumentation der im OT-Netzwerk vorhandenen Anlagen ermöglicht. Darüber hinaus überwacht ein IDS die Funktionsweise des OT-Netzwerks sowie dessen Betriebsmittel und Assets, um zu gewährleisten, dass diese sicher und korrekt funktionieren. Auf diese Weise lassen sich Netzwerkfehler, Fehlkonfigurationen von Geräten und fehlerhafte Protokollübertragungen sofort feststellen.

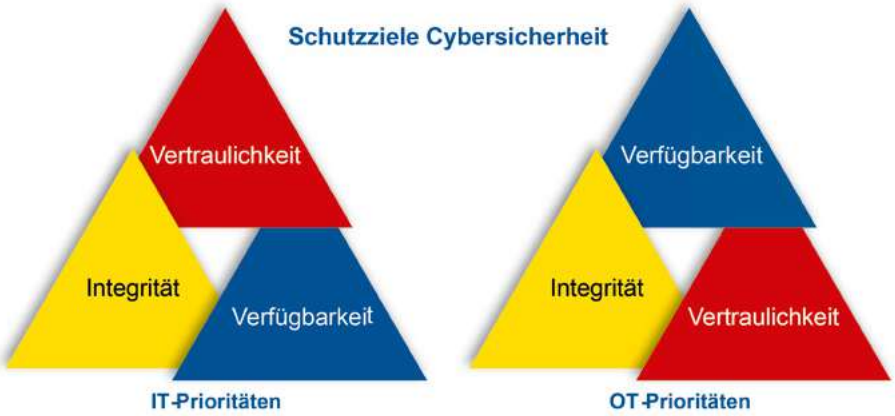


Abbildung 1: Unterschiedliche Prioritäten in IT und OT (Bild: OMICRON)

INSTALLATION VON IDS IM NETZWERK

Um den optimalen Einsatzort für das IDS zu bestimmen, sollten Unternehmen folgende Aspekte berücksichtigen:

- ***Netzwerksegmente:*** *Welche Bereiche des Netzwerks sollen überwacht werden? Sind es nur bestimmte Subnetze oder das gesamte Netzwerk?*
- ***Zentrale Kommunikationspunkte:*** *Wo sind die geeigneten Verbindungspunkte im Netzwerk? Das kann an Router- oder Switch-Schnittstellen, an Firewalls oder anderen kritischen Systemen sein.*
- ***Zugriffsrechte:*** *Welche Zugriffsrechte sind erforderlich, um das IDS zu installieren und zu konfigurieren? Dies sollte im Einklang mit den Sicherheitsrichtlinien des Unternehmens stehen.*
- ***Skalierbarkeit:*** *Ist das Netzwerk skalierbar? Wenn ja, muss das IDS in der Lage sein, mit dem Wachstum des Netzwerks Schritt zu halten.*

Die Wahl des richtigen Einsatzorts ist entscheidend für die Effektivität des IDS und die Sicherheit des gesamten Netzwerks.

Zusätzlich bietet ein IDS die Möglichkeit, das Netzwerk und die Netzwerkkommunikation durch Dashboards zu visualisieren. Das umfasst eine übersichtliche Darstellung von Ereignis- und Alarmmeldungen, die sowohl für IT- als auch für OT-Mitarbeiter leicht verständlich sind.

Eine Herausforderung ist jedoch die Komplexität der Netze. OT-Netzwerke sind oft vielschichtig und heterogen, da sie aus verschiedenen Geräten, Protokollen, Technologien und redundanten Systemen bestehen. Die Implementierung eines IDS erfordert daher eine genaue Kenntnis der Netzwerktopologie. Ein weiteres Problem sind Fehlalarme, die auftreten können, wenn das IDS erlaubte Aktivitäten fälschlicherweise als Angriffe interpretiert. Dies erfordert eine sorgfältige Konfiguration und Feinabstimmung. Darüber hinaus kann ein IDS die Netzwerkperformance beeinträchtigen, besonders wenn es auf älteren oder ressourcenbeschränkten Systemen läuft.

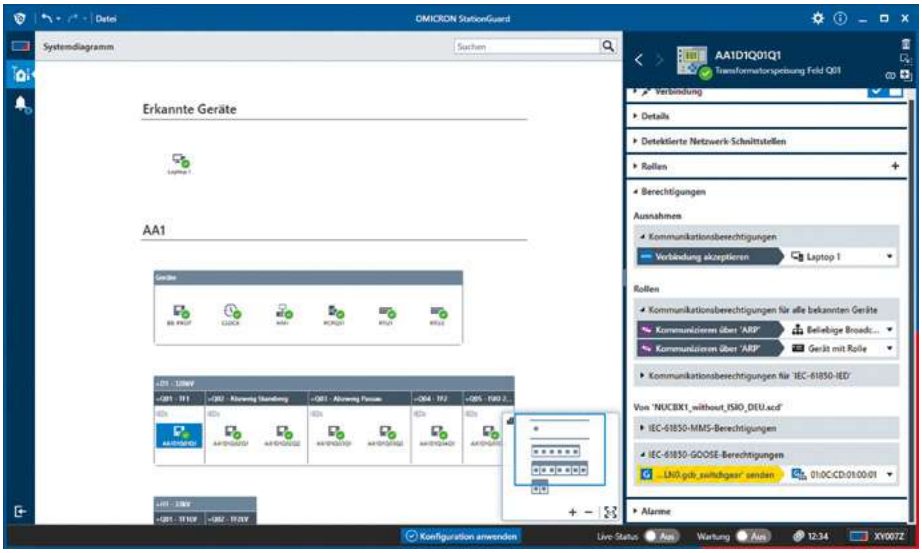


Abbildung 2: Systemdiagramm der betroffenen Anlage (Bild: OMICRON)

Insgesamt ist ein OT-spezifisches IDS für Energieversorger unerlässlich, um die Verfügbarkeit in kritischen Infrastrukturen sicherzustellen. Durch die gezielte Überwachung des OT-Netzes und die frühzeitige Erkennung von Anomalien können Cyberangriffe verhindert oder deren Auswirkungen minimiert werden.

PRAXISBEISPIEL: PENETRATIONSTESTS UND FUNKTIONSWEISE EINES IDS

Im Rahmen eines Proof of Concepts bei einem norwegischen Verteilnetzbetreiber wurden mehrere OT-IDS installiert, konfiguriert und getestet. Der Kunde wollte die IDS hinsichtlich ihres Implementierungsaufwands, ihrer Anwendungsfreundlichkeit und ihrer Effektivität eingehend prüfen. Dazu wurden gezielte Cyberangriffe für verschiedene Angriffsvektoren durchgeführt. Der Energieversorger erhielt dabei Unterstützung von Experten einer externen Firma, die den Penetrationstest in Zusammenarbeit mit dem Verteilnetzbetreiber umsetzten.

Der Penetrationstest fand am 18. und 19. April 2023 statt. Vor Beginn des Tests wurden seitens des Verteilnetzbetreibers einige Konfigurationen an Routern und Switches durchgeführt, um einen reibungslosen Ablauf zu gewährleisten (siehe Abbildung 2). Die beteiligten IDS-Anbieter waren nicht über den Zeitpunkt des Pentests oder über die Art und den Umfang der Angriffsszenarien informiert.

ERSTER TAG DES PENETRATIONSTESTS

Eine deutliche Indikation für den Start der Angriffsserie war das Detektieren neuer IP-Adressen im Netzwerk.

Abbildung 3: Pentest-Timeline (Tag 1) (Bild: OMICRON)

Im Gegensatz zur IT stellen unbekannte IP-Adressen in der OT eine potenzielle Bedrohung dar. Diese sind einer der besten Indikatoren für die frühzeitige Erkennung bestimmter Angriffe.

Abbildung 4: Timeline der TCP-Port-Scans (Bild: OMICRON)

In der nächsten Phase der Angriffsserie wurden verschiedene Scans durchgeführt. Das ist ein übliches Verhalten, wenn Angreifer das Netzwerk genauer verstehen und sich einen Überblick über den Aufbau des Netzwerks und deren Netzwerkteilnehmer verschaffen wollen.

Dazu wurden zunächst mehrere TCP-Port-Scans durchgeführt. Dabei versuchen Angreifer, offene Ports, verwendete Dienste oder Betriebssysteme sowie technische Schwachstellen zu identifizieren. Port-Scans lassen sich gut über die Auslastung des Netzwerkes erkennen. Durch den Allowlist-Ansatz im IDS sind solche Verbindungen ebenfalls verboten und führen zur Alarmierung. Abbildung 4 zeigt eine Timeline der Alarme, welche durch diese Attacken ausgelöst worden sind.

Im weiteren Verlauf wurde ein UDP-Port-Scan und einige Ping-Sweeps vom IDS detektiert. Bei einem UDP-Port-Scan versuchen Angreifer, Rückschlüsse auf den Gerätetyp der Netzwerkteilnehmer zu ziehen. Dazu zählt beispielsweise die Unterscheidung zwischen Client, Server, Schutz- oder Steuergerät. Mithilfe eines Ping-Sweeps werden bestimmte IP-Adressbereiche des Netzwerks kontaktiert. Erhält man eine Antwort von einer IP-Adresse ist dieses Gerät aktiv. Mithilfe dieser Informationen können Angreifer ein Mapping der Ports, der genutzten IP-Adressen, der Dienste, der Betriebssysteme und der Netzwerkteilnehmertypen vornehmen.

In der nächsten Phase des Angriffs wurde eine ARP-Spoofing-Attacke ausgeführt. Hierbei nutzen die Angreifer die fehlende Authentifizierung zwischen den Netzwerkteilnehmern im ARP-Protokoll aus.

Das Address Resolution Protocol (ARP) dient der Zuordnung von IP- zu MAC-Adressen im lokalen Netz. Hierbei kommt ein Request-Response-Schema zum Einsatz, bei dem die erste Antwort (ARP-Response) akzeptiert und in einer ARP-Tabelle gespeichert wird. Dieser Mechanismus birgt jedoch das Risiko, dass auch manipulierte Antworten der Angreifer von den Netzwerkteilnehmern akzeptiert werden. Auf diese Weise können Angreifer ihre MAC-Adresse mit der IP-Adresse eines Zielhosts verknüpfen. Dadurch ist es ihnen möglich, den Datenverkehr, der eigentlich für den Zielhost bestimmt ist, auf das kompromittierte System umzuleiten und zu manipulieren.

Somit entsteht ein manipuliertes IP- zu MAC-Adressen-Mapping, welches es den Angreifern erlaubt, eine Man-in-the-Middle-Attacke zu initialisieren. Abbildung 5 zeigt die Detektion und Alarmierung dieses Verhaltens im ZeroLine-Diagramm.

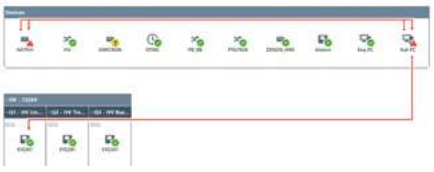


Abbildung 5: ARP-Spoofing im ZeroLine-Diagramm (Bild: OMICRON)

Im Anschluss wurde eine UDP-Traceroute-Attacke ausgeführt. Ähnlich wie bei den vorherigen Scan-Attacken dient diese Methode der detaillierten Untersuchung des Netzwerkaufbaus. Dabei wird versucht, durch gezieltes Setzen der Time-to-live-(TTL)-Variable, den Netzwerkpfad und die Netzwerkteilnehmer samt IP-Adresse und Hostnamen zu identifizieren.

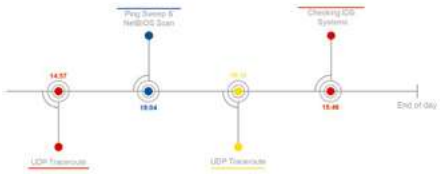


Abbildung 6: Pentest-Timeline 2 (Tag 1, Fortsetzung) (Bild: OMICRON)

Die Erkenntnisse aus den Scans bildeten die Grundlage für eine gezielte Angriffskombination auf die Windows-Geräte im Netzwerk. Zunächst wurde die Aktivität einiger Netzwerkteilnehmer mittels eines Ping Sweep per ICMP überprüft. Bei erfolgreicher Rückmeldung wurde ein NetBIOS-Scan durchgeführt, um die NetBIOS-Informationen der Geräte abzufragen. NetBIOS ist ein Windows-Protokoll, das für den Austausch von Daten wie Dateifreigabe oder Druckerinformationen verwendet wird. Wenn eine Antwort auf die gesendeten NetBIOS-Anfragen empfangen wurde, erfolgten zusätzliche Verbindungsversuche mit Webservern auf den Ports 80, 443 und 8080 mithilfe von TCP-Paketen. Die im IDS protokollierten PCAP-Daten ermöglichten die Analyse und Auswertung der Angriffsmethoden.

Abbildung 7: NetBIOS-Attacke in Wireshark (Bild: OMICRON)

ZWEITER TAG: PHYSISCHE ANGRIFFE

Abbildung 8: Pentest-Timeline (Tag 2) (Bild: OMICRON)

Die Angriffsserie wurde am zweiten Tag mit einer physischen Attacke fortgesetzt. Dafür kopierten die Angreifer eine Hardwarekomponente mit dem beim Verteilnetzbetreiber vorhande-

nen Asset-Management-System funktional und tauschten sie aus. Dabei wurden sowohl die MAC-Adresse als auch die IP-Adresse des Asset-Management-Systems übernommen, inklusive sämtlicher operativer Funktionen.

Das Asset-Management-System ist eine Komponente, die für das Sammeln von Konfigurations- und Fehlerdaten sowie das Erstellen eines Asset-Inventars von Schutzrelais verantwortlich ist.

Das Erkennen solcher physischen Attacken ist sehr kompliziert, und bei sorgfältiger Ausführung ist es nahezu unmöglich. Im Fall dieses Pentests wurden seitens der Angreifer jedoch Spuren hinterlassen. So wurde dem kompromittierten Asset-Management-System nach dem Austausch für eine sehr kurze Zeit eine APIPA-Adresse zugewiesen. Der APIPA-Mechanismus wird von Betriebssystemen verwendet, um selbstständig eine IP-Adresse zu konfigurieren, falls kein DHCP-Server erreichbar ist. Die APIPA-Adresse wird immer im Adressbereich 169.254.x.x vergeben, wodurch sie sich deutlich von den anderen IP-Adressen beziehungsweise IP-Adressbereichen unterscheidet und als Anomalie detektiert werden kann.

Abbildung 9: Detektion einer APIPA-Adresse für das Asset-Management-System (Bild: OMICRON)

Bei der weiteren Analyse wurde festgestellt, dass die periodischen Abfragen des Asset-Management-Systems für eine kurze Zeit unterbrochen wurden. Dies deutete auf den Austausch des kompromittierten Geräts samt Asset-Management-Funktionalität hin.

Nach der Kompromittierung des Asset-Management-Systems wurden unerlaubte HTTP-Nachrichten an mehrere Switches gesendet. Ein Angriff, der HTTP-Verbindungen von OT-Geräten ausnutzt, ist als äußerst kritisch zu bewerten.

Im weiteren Verlauf wurden Verbindungsversuche zu verschiedenen Intelligent Electronic Devices (IEDs) über Port 102 detektiert. Dieser Port wird in der Schutz- und Leittechnik von dem IEC-61850-MMS-Protokoll verwendet und dient zum Austausch von Schaltsignalen, Messwerten, Konfigurationsdaten oder Ereignisberichten. Das IEC-61850-MMS ermöglicht somit eine effiziente Kommunikation zwischen den IEDs und den höheren Entitäten wie RTUs und SCADA-Systemen.

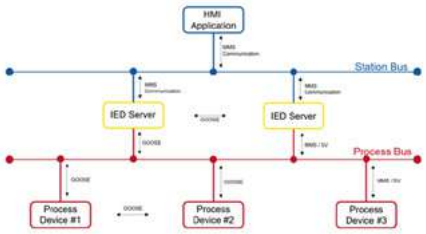


Abbildung 10: Protokollstruktur eines Schutz- und Leittechnik-Netzwerkes (Bild: OMICRON)

Es folgte ein Angriff mittels eines weiteren IEC-61850-Protokolls. Die Analyse ergab, dass nach dem Verbindungsaufbau auf einigen Switches GOOSE-Nachrichten im Netzwerk nicht mehr sichtbar waren und Statuswerte verändert wurden.

GOOSE wird in Schutz- und Leittechnik-Netzwerken für die horizontale Kommunikation zwischen IEDs verwendet. Dazu werden in regelmäßigen Abständen Statuswerte sowie Ereignismeldungen gesendet, zum Beispiel Auslösesignal oder das Einschalten des Leistungsschalters. Das hat zur Folge, dass andere IED oder SCADA-Systeme entsprechende Folgeaktionen ausführen können.

Bei der ausgeführten Attacke wurden diese GOOSE-Nachrichten verändert oder unterbunden. Dadurch sind betriebsrelevante Informationen für die anderen Netzwerkteilnehmer wie unter anderem aktuelle Statuswerte nicht korrekt oder nicht mehr verfügbar. Das kann zu Fehlfunktionen, Störungen bis hin zum Ausfall der Betreiberanlage oder zur Beeinträchtigung der Versorgungssicherheit für Unternehmen und Bürger führen.

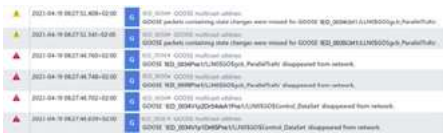


Abbildung 11: Fehlender-GOOSE-Alarm in StationGuard (Bild: OMICRON)

HANDLUNGS-EMPFEHLUNGEN

Die Ergebnisse des Penetrationstests verdeutlichen die Notwendigkeit und Effektivität eines Angriffserkennungssystems (IDS) bei der Identifizierung von Cyberangriffen. Besonders die Auswertung der visualisierten Angriffe hat gezeigt, dass viele dieser Bedrohungen nur durch ein auf OT spezialisiertes IDS erkannt werden können. Die Ergebnisse des Praxistests belegen, dass bereits ein einzelner Alarm ein Hinweis auf einen potenziellen Angriff sein kann.

IDS können Netzwerke in Echtzeit überwachen und dabei helfen, ungewöhnliche Aktivitäten sofort zu erkennen. Zusätzlich zu einem IDS empfehlen wir jedem Energieversorger, sein Netzwerk korrekt zu konfigurieren und zu segmentieren, indem nicht benötigte Dienste oder Applikationen deaktiviert werden. Durch diese Maßnahmen wird der Angriffsvektor erheblich reduziert und potenzielle Attacken werden deutlich erschwert. Das trägt maßgeblich dazu bei, die Sicherheit im Energieversorgungsbereich zu stärken und kritische Infrastrukturen vor Cyberbedrohungen zu schützen. ■

Literatur

[1] *Bundesamt für Justiz, „Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) § 11 Betrieb von Energieversorgungsnetzen," 2024. https://www.gesetze-im-internet.de/enwg_2005/__11.html. [Zugriff am 12. Juni 2024]*

[2] *Bundesamt für Sicherheit in der Informationstechnik, „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung," 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=15. [Zugriff am 12. Juni 2024]*

BENJAMIN TEUDELOFF
ist Cybersecurity Consulting Manager bei OMICRON.
www.omicroncybersecurity.com/de

ERIC HEINDL
ist Cybersecurity Analyst bei OMICRON.
www.omicroncybersecurity.com/de

Mögliche Angriffsziele, mitigierende Maßnahmen und sinnvolle Prüfziele

KUBERNETES SICHER BETREIBEN

Kubernetes ist eine Open-Source-Plattform zur Automatisierung der Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen. Neben den vielen Vorteilen wie Ressourcenmanagement, effiziente Ressourcennutzung und Ausfallsicherheit gibt es auch Herausforderungen, besonders für den sicheren Betrieb. Welchen Angriffen sind Kubernetes-Umgebungen ausgesetzt und wie lassen sie sich schützen? Welche Angriffsziele sollten mit welcher Priorität näher betrachtet werden?

Ein Kubernetes-Cluster besteht aus verschiedenen Komponenten und Diensten, die zusammenarbeiten, um containerisierte Anwendungen zu verwalten und bereitzustellen. Das Cluster steht dabei nicht für sich allein, sondern ist in der Regel in eine komplexe und hochautomatisierte Entwicklungs- und Produktionsumgebung eingebettet. Die wichtigsten Angriffsziele in einer Kubernetes-Umgebung sind die Deployment-Pipeline, die Image-Registry, die Control-Plane/das Cluster, die Worker-Nodes sowie die Anwendungen, die auf dem Kubernetes-Cluster laufen.

DEPLOYMENT-PIPELINE

Die Deployment-Pipeline ist der Prozess, in dem normalerweise der Anwendungscode von Entwicklern getestet und in produktionsbereite Container-Images umgewandelt wird. Anschließend können diese auf einem Kubernetes-Cluster bereitgestellt werden. Ein potenzieller Angreifer kann hier ansetzen und beispielweise versuchen, Schwachstellen im Build-Service oder der zugehörigen Zugangsverwaltung auszunutzen, um Schadcode einzuschleusen oder die Integrität der bereitgestellten Anwendungen zu gefährden. Letztlich ist eine Build-Pipeline nichts anderes als Reihe von Skripten und Abhängigkeiten. Gelingt es Angreifern, Skripte zu verfälschen oder vollständig auszutauschen, können diese Schadcode in die Anwendung einbringen. Alternativ manipulieren Aggressoren Abhängigkeiten der Build-Pipeline, sodass beispielsweise veralte Bibliotheken oder Versionen mit bekannten oder unbekannten Schwachstellen für den Bau des Container-Images verwendet werden.

Beide Varianten zielen darauf ab, die Anwendung oder den Container zu kompromittieren, um Daten direkt abzugreifen oder um auf die dahinter liegenden Cluster-Ressourcen auszubrechen. Angriffe auf die Deployment-Pipeline haben schwerwiegende Folgen, da sie die gesamte Lieferkette einer Anwendung beeinflussen. Im schlimmsten Fall kann ein Angreifer vollen Zugriff auf die Applikation, die verarbeiteten Daten und den Cluster selbst erlangen.

PRÜFUNG DER DEPLOYMENT-PIPELINE

Die Sicherheit der Deployment-Pipeline ist entscheidend, um zu gewährleisten, dass nur vertrauenswürdiger und geprüfter Code in den Produktionscluster gelangt. Genauso wichtig ist es, sicherzustellen, dass ein Angreifer die Abhängigkeiten und Skripte der Build-Pipeline nicht manipulieren kann. Der Build Service sollte einem Penetrationstest (Pentest) oder einem Konfigurationsreview unterzogen werden. Ebenso ist ein Prozessaudit der Entwicklungsprozesse sinnvoll.

IMAGE-REGISTRY

Die Image-Registry ist ein kritisches Element in der Lieferkette von Anwendungen. Sie ist ein zentrales Repository, in dem Container-Images gespeichert und verwaltet werden. Diese Images enthalten alle Komponenten, die zur Ausführung einer Anwendung erforderlich sind, einschließlich des Betriebssystems, der Anwendung und ihrer Abhängigkeiten. Entwickler können diese Container-Images aus öffentlichen Quellen – sogenannten Hubs – in eine interne Image-Registry hochladen oder direkt für den Deployment-Prozess verwenden. Sie können aber auch selbst ein neues Container-Image erstellen und in eine Image-Registry hochladen.

Angreifer könnten versuchen, Schwachstellen in der Image-Registry auszunutzen, um bösartige Images hochzuladen oder legitime Images zu manipulieren. Ein beliebter Angriffsvektor besteht zudem darin, schädliche Container-Images in öffentlichen Hubs zu platzieren. Diese sind mit den vom Entwickler erwarteten Funktionen ausgestattet und beschrieben, enthalten aber zusätzlich vom Angreifer eingebaute Schwachstellen, um Zugriff auf die Betriebsumgebung zu erlangen. Gleiche oder ähnliche Strategien werden vom Angreifer verwendet, wenn er die Möglichkeit hat, auf eine interne Image-Registry zuzugreifen. Es ist daher von entscheidender Bedeutung, die Integrität der Image-Registry sicherzustellen und die zulässigen Quellen für Container-Images einzuschränken.

PRÜFUNG DER IMAGE-REGISTRY

Auch bei der Image-Registry ist eine Prozess- und Konfigurationsüberprüfung der sinnvollste erste Schritt. Es muss sichergestellt sein, dass nur autorisierte Benutzer und Systeme auf die Registry zugreifen und Images hoch- oder herunterladen können. Das Einspielen neuer Images sollte mindestens durch ein Vier-Augen-Prinzip verifiziert und vor dem ersten Upload auf Schwachstellen und Malware überprüft werden.

Zusätzlich sollte man die Images regelmäßig und automatisiert auf bekannte Sicherheitslücken und Malware kontrollieren.

DAS CLUSTER: CONTROL-PLANE UND WORKER-NODES

Die Control-Plane ist das Gehirn eines Kubernetes-Clusters. Sie umfasst Komponenten wie den API-Server, den Scheduler und den Controller-Manager, die für die Verwaltung des Clusters verantwortlich sind. Angriffe auf die Control-Plane können das gesamte Cluster destabilisieren oder zur vollständigen Übernahme führen. Angreifer können probieren, unberechtigten Zugriff auf den API-Server zu erlangen, um administrative Befehle auszuführen oder die Netzwerk-

Bild: Ar_TH - stock.adobe.com

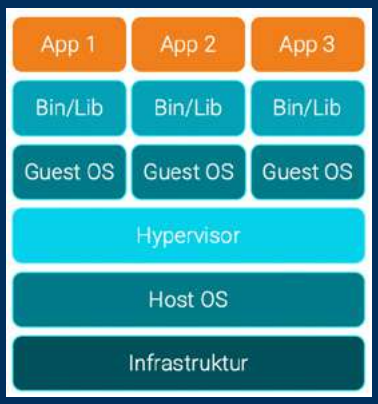
KUBERNETES-GRUNDLAGEN

Die klassische Virtualisierung ist inzwischen der Standard im modernen IT-Betrieb.

Sie ermöglicht es, physische Ressourcen effizienter zu nutzen, die Flexibilität von Anwendungen und Ressourcen zu erhöhen und die Verwaltung von IT-Infrastrukturen zu vereinfachen.

Virtualisierung ist eine Technologie, die es ermöglicht, mehrere virtuelle Maschinen (VMs) auf einer einzigen physischen Maschine (Host) auszuführen. Jede virtuelle Maschine verhält sich wie ein eigenständiger Computer mit eigenem Betriebssystem (OS) und eigenen Anwendungen. Die Virtualisierung wird durch eine Software-Schicht ermöglicht, die als Hypervisor bezeichnet wird.

Jede VM enthält ein vollständiges Betriebssystem und eine virtuelle Kopie der Hardware, die auf dem Hostsystem läuft.



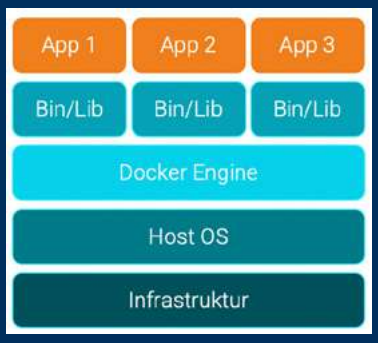
Klassische Virtualisierung mithilfe von virtuellen Maschinen (VMs)

Dadurch ergibt sich bei der klassischen Virtualisierung mithilfe von Hypervisoren eine ineffiziente Ressourcennutzung, da für das Gast-OS viel CPU-Leistung, Hauptspeicher und Speicherplatz benötigt wird.

Docker

Um die Effizienz und Portabilität von Anwendungen zu verbessern, hat sich Docker als Lösung dieser Probleme etabliert. Docker ist eine Open-Source-Plattform, die es ermöglicht, Anwendungen in Container zu verpacken, zu verteilen und auszuführen. Ein Container ist eine standardisierte Einheit der Software, die alles enthält, was zum Ausführen einer Anwendung erforderlich ist, einschließlich Code, Laufzeit, Systemwerkzeuge, Bibliotheken und Einstellungen.

Container teilen sich denselben Kernel des Host-Betriebssystems und laufen als isolierte Prozesse im Userspace. Sie sind „leichter" und starten schneller als VMs, da sie kein vollständiges Betriebssystem benötigen.



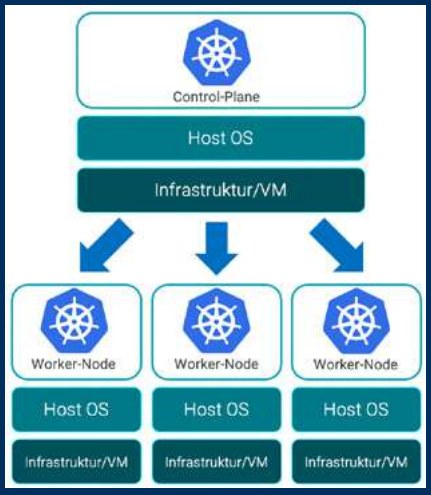
Klassische Virtualisierung mithilfe von Docker Engine und Containern

Kubernetes

Die Verwaltung vieler Container neigt allerdings zu einer gewissen Unübersichtlichkeit. Daher bildeten sich verschiedene Plattformen und Tools heraus, um die Handhabung von Containern zu erleichtern. Einer der bekanntesten Vertreter dafür ist Kubernetes.

Kubernetes ist eine Plattform zur Orchestrierung von Containern, die ursprünglich von Google entwickelt wurde. Sie automatisiert die Bereitstellung, Skalierung und Verwaltung von containerisierten Anwendungen. Kubernetes verwaltet Container-Cluster, überwacht deren Zustand und verteilt den Netzwerkverkehr, um Anwendungen effizient und zuverlässig zu betreiben. Es ermöglicht eine einfache Verwaltung großer Container-Umgebungen und sorgt für hohe Verfügbarkeit und Skalierbarkeit der Anwendungen.

Ein Kubernetes-Cluster besteht immer aus einer Control-Plane – auch bekannt als Master – und einer Reihe von Worker-Nodes. Auf den Worker-Nodes werden Container bereitgestellt, in welchen die Anwendungen laufen. Die Kommunikation mit allen Cluster-Ressourcen und Anwendungen erfolgt ausschließlich über die Control-Plane.



Exemplarischer Aufbau eines Kubernetes-Clusters

kommunikation zu manipulieren. Ebenso kann versucht werden, auf Cluster-Ressourcen wie Persistent Volumes zuzugreifen, um auf diesem Weg an Daten zu gelangen. Auf der Control-Plane werden keine Anwendungen ausgeführt. Sie dient lediglich der Verwaltung und Steuerung der Ressourcen, auf denen die Applikationen bereitgestellt werden. Diese Ressourcen werden Worker-Nodes genannt.

Worker-Nodes sind die Maschinen, auf denen die Pods beziehungsweise Container ausgeführt werden. Sie stellen die Rechenleistung bereit, die erforderlich ist, um Anwendungen in einem Kubernetes-Cluster auszuführen. Angreifer nutzen Schwachstellen in den Worker-Nodes aus, um Zugriff auf die darunter liegenden Betriebssysteme zu erlangen, Container zu kompromittieren oder sensible Daten zu exfiltrieren. Die Sicherheit der Worker-Nodes ist entscheidend, um die Integrität der ausgeführten Anwendungen zu gewährleisten.

Schwachstellen in der Namespace-Konfiguration oder der Pod-Konfiguration sind mögliche Angriffsziele. Ähnlich wie bei Angriffen auf die Control-Plane oder Worker-Nodes ist das Ziel auch hier, unautorisierten Zugriff auf Ressourcen zu erlangen, die dem Angreifer einen möglichst umfassenden Datenzugriff ermöglichen.

PRÜFUNG DER CLUSTER-SICHERHEIT

Die Überprüfung der Clustersicherheit ist die komplexeste und damit auch aufwendigste Methode, um den sicheren Betrieb der Clusterumgebung zu gewährleisten. Verschiedene Konfigurationsdateien der Control-Plane und der Worker-Nodes müssen auf Betriebssystemebene auf Inhalt und Zugriffsberechtigungen überprüft werden. Zusätzlich müssen das Konzept und die Berechtigungen des clusterinternen RBAC und der Namespace-Konfiguration berücksichtigt werden.

Mögliche Prüfverfahren sind automatisierte Tests mit speziellen Test-Pods/-Containern oder ein Konfigurationsaudit des Clusters. Beide Verfahren ergänzen sich und bieten in Kombination eine aussagekräftige Analyse der Clustersicherheit.

ANWENDUNGEN

Die in Kubernetes bereitgestellten Anwendungen sind häufig selbst Angriffsziele. Schwachstellen in der Anwendungslogik, unsichere Konfigurationen oder veraltete Bibliotheken können von Angreifern ausgenutzt werden, um unbefugten Zugriff zu erlangen oder die Anwendung zu stören.

Ein Cyberkrimineller kann probieren, aus einer der Anwendungen auszubrechen. Gelingt dies, befindet sich der Angreifer auf der Virtualisierungsebene (dem Container) und kann von dort aus versuchen, die darunter liegenden Ressourcen zu kompromittieren. Da Kubernetes als Plattform zur Bereitstellung und Verwaltung von Anwendungen dient, ist es wichtig, dass die Applikationen selbst sicher sind und regelmäßig auf Schwachstellen überprüft werden.

ÜBERPRÜFUNG DER ANWENDUNGEN

Ein Pentest der in Kubernetes bereitgestellten Applikation ist notwendig, um sicherzustellen, dass die Anwendungen selbst sicher sind und es einem Angreifer nicht gelingen kann, aus der Anwendung auszubrechen. Der Betrieb einer Anwendung innerhalb eines Kubernetes-Clusters macht einen Pentest nicht obsolet. Ganz im Gegenteil: Empfehlenswert ist ein Grey- oder White-Box-Pentest. Der durchführende Analyst sollte aber wissen, dass die Anwendung in einem Kubernetes-Cluster betrieben wird.

SINNVOLLE PRÜFZIELE

Wie oben gezeigt, gibt es viele Auditziele, aber wo soll eine Organisation zuerst anfangen? Zeit, Personal und Budget sind in der Realität begrenzt. Unabhängig von den individuellen Gegebenheiten einer Organisation lassen sich folgende Faustregeln festhalten: Die aufwendige Überprüfung des Kubernetes-Clusters und seiner Worker-Nodes selbst ist vor allem dann sinnvoll, wenn der Kubernetes-Cluster eine sogenannte Multi-Tenant-Umgebung bereitstellt oder sich Assets mit unterschiedlichem Schutzbedarf in ein und demselben Cluster befinden. Kritische Assets, wie zum Beispiel eine PKI, sollten generell auf einem separaten System oder Cluster betrieben werden.

Vor einer Cluster-Überprüfung ist es in der Regel jedoch effektiver, sich zunächst auf die Sicherheitsprozesse rund um die Deployment-Pipeline, die Image-Registry und die Anwendungs-/Netzwerksicherheit zu konzentrieren. Kurz gesagt, die Wege zum Cluster sollten vorrangig abgesichert werden. Das Cluster beziehungsweise die Control-Plane und die Worker-Nodes sind üblicherweise für einen Angreifer nicht direkt erreichbar. Der Weg zum Cluster ist lang und führt über die Deployment-Strecke, über einen Ausbruch aus der Anwendung oder das vorgelagerte Netzwerk.

Die Netzwerksicherheit ist ein weiterer Bereich, der überprüft werden sollte, um einen sicheren Betrieb eines Kubernetes-Clusters zu gewährleisten. Ob ein klassischer Segmentierungs-Pentest inklusive Firewall-Überprüfung oder eine Konfigurationsanalyse der Public-Cloud-Umgebung notwendig ist, hängt immer von der im Einzelfall eingesetzten Technologie ab.

FAZIT: KUBERNETES KANN NUR GANZHEITLICH SICHER BETRIEBEN WERDEN

Die Sicherheit eines Kubernetes-Clusters erfordert einen ganzheitlichen Blick auf alle Komponenten der Umgebung. Während die Überprüfung der Clusters-Konfiguration vor allem für Multi-Tenant-Umgebungen einen hohen Stellenwert hat, ist es im Standardbetrieb oft effektiver, sich zunächst auf die Sicherheitsprozesse rund um die Deployment-Pipeline und die Image-Registry zu konzentrieren. Durch die Implementierung robuster Zugriffskontrollen, regelmäßiger Sicherheitsscans und umfassender Überprüfungen können Organisationen sicherstellen, dass ihre Kubernetes-Umgebungen widerstandsfähig gegenüber Angriffen sind und die Integrität ihrer Anwendungen gewahrt bleibt. Ein Pentest der Anwendungen und ein Segmentierungstest des Netzwerks sind ebenfalls unerlässlich, um einen sicheren Betrieb der Kubernetes-Umgebung zu gewährleisten. ■

PHILLIP ANSORGE
ist Managing Consultant bei der usd AG. Mit über sechs Jahre Erfahrung in den Bereichen Informations- und IT-Sicherheit unterstützt er nationale und internationale Unternehmen dabei Cloud-Umgebungen sicher aufzubauen und zu betreiben.

Gesundheits-Apps im Sicherheitscheck

DIGITALE GESUNDHEITS-FÖRDERUNG UND MOBILE SICHERHEIT

Eine kritische Betrachtung

Die Gesundheitsförderung durch Apps ist auf mobilen Endgeräten allgegenwärtig geworden. Von Fitnesstracking über Ernährungsberatung bis hin zur Unterstützung bei der Krankheitstherapie – die Bandbreite der angebotenen Funktionen wächst kontinuierlich. Doch mit der Zunahme digitaler Gesundheitsanwendungen steigen auch die Bedenken hinsichtlich der Sicherheit und des Schutzes sensibler Nutzerdaten. Unser Autor wirft einen umfassenden Blick auf die aktuelle Situation der mobilen Sicherheit von Gesundheits-Apps, erörtert Herausforderungen, Standards und Lösungsansätze.

Die Landschaft der Gesundheits-Apps ist vielfältig und differenziert, wobei sie sich hauptsächlich in drei Kategorien einteilen lässt. Zunächst gibt es die sogenannten Lifestyle-Apps, die Nutzern dabei helfen, ein gesünderes Leben zu führen. Diese Kategorie umfasst eine breite Palette von Anwendungen: von Fitnesstrackern, die jeden Schritt zählen und jede verbrannte Kalorie erfassen, bis hin zu Ernährungsberatern, die Tipps für eine ausgewogene Ernährung geben. Diese Apps motivieren Nutzer durch gamifizierte Elemente, sich mehr zu bewegen und gesündere Essgewohnheiten anzunehmen, indem sie Fortschritte verfolgen, visuell aufbereiten und virtuelle Auszeichnungen verleihen.

Die zweite Kategorie bilden die „Digitalen Gesundheitsanwendungen" (DiGAs), auch bekannt als „Apps auf Rezept". Diese sind speziell dafür entwickelt, Patienten in ihren Therapieprozessen zu unterstützen. Sie bieten nicht nur Informationen und Beratung zu verschiedenen Krankheitsbildern, sondern ermöglichen es den Nutzern auch, Symptome zu dokumentieren, Medikationspläne zu verwalten und in einigen Fällen direkt mit medizinischem Fachpersonal zu kommunizieren. Diese Apps können somit eine Brücke zwischen Patienten und Gesundheitsdienstleistern bilden sowie eine kontinuierliche Betreuung sicherstellen, die über den Rahmen herkömmlicher Arztbesuche hinausgeht.

Die dritte Kategorie umfasst Apps, die innerhalb der von der gematik definierten Telematikinfrastruktur (TI) des deutschen Gesundheitswesens eine zentrale Rolle spielen. Diese Apps wurden speziell dafür konzipiert, die digitale Transformation im Gesundheitswesen zu unterstützen. Sie beinhalten unter anderem Lösungen für das elektronische Rezept (E-Rezept) und das Frontend für die elektronische Patientenakte (ePA-FdV), das es dem Versicherten ermöglicht, seine Patientenakte zu verwalten. Sie sind von entscheidender Bedeutung, da sie die Effizienz der Gesundheitsversorgung verbessern, indem sie eine sichere und schnelle Übermittlung von Gesundheitsdaten zwischen Patienten und Anbietern von Gesundheitsdiensten ermöglichen. Diese Anwendungen erfordern eine strenge Zulassung und müssen hohe Sicherheitsstandards erfüllen, um die sensiblen Gesundheitsdaten der Nutzer zu schützen.

Jede dieser Kategorien von Gesundheits-Apps hat das Potenzial, den Nutzern erhebliche Vorteile zu bieten. Indem sie wichtige Gesundheitsdaten sammeln und analysieren, können sie Einzelpersonen dabei unterstützen, informierte Entscheidungen über ihre Gesundheit und ihr Wohlbefinden zu treffen. Darüber hinaus tragen sie dazu bei, die allgemeine Zugänglichkeit und Effizienz der Gesundheitsversorgung zu verbessern, indem sie beispielsweise Wartezeiten reduzieren und die Kommunikation zwischen Patienten und Gesundheitsdienstleistern optimieren. Jedoch stellt die Notwendigkeit, die Privatsphäre und Sicherheit der von diesen Apps gesammelten sensiblen Daten zu gewährleisten, eine erhebliche Herausforderung dar.

DATENSICHERHEIT STEHT ALS KRITISCHER ASPEKT IM FOKUS

Die Bedeutung der Datensicherheit bei der Nutzung von Gesundheits-Apps kann nicht hoch genug eingeschätzt werden, da diese Anwendungen eine Fülle sensibler Informationen von ihren Nutzern sammeln und speichern. Diese reichen von grundlegenden persönlichen Daten bis hin zu detaillierten Gesundheitsinformationen, wie medizinischen Berichten, Diagnosen und Behandlungsplänen. Die Sensibilität dieser Daten macht sie zu einem begehrten Ziel für Cyberkriminelle, die daran interessiert sind, sie für Identitätsdiebstahl, Betrug oder Erpressung zu missbrauchen. Die Gefahren sind vielfältig und umfassen nicht nur den direkten Diebstahl der Daten, sondern auch deren Manipulation, was schwerwiegende Folgen für die Gesundheitsversorgung der Betroffenen haben kann.

Zu den Bedrohungen zählen unter anderem die unerlaubte Einsichtnahme in persönliche Gesundheitsinformationen, die Modifikation von Gesundheitsdaten mit potenziell schädlichen Auswirkungen auf die medizinische Behandlung und die Verbreitung sensibler Informationen ohne die Zustimmung der Betroffenen. Darüber hinaus besteht das Risiko, dass unzureichend gesicherte Apps als Einfallstor für weiterreichende Cyberangriffe auf die Infrastruktur von Gesundheitseinrichtungen genutzt werden, was zu einer umfassenden Kompromittierung der Datensicherheit führen könnte.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinen Untersuchungen von Gesundheits-Apps bereits eine beträchtliche Anzahl an Sicherheitsmängeln festgestellt. Diese reichen von unzureichender Datenverschlüsselung über Schwachstellen in der Authentifizierung bis hin zu Lücken in der Software, die es Angreifern ermöglichen, unbefugt auf Nutzerdaten zuzugreifen oder diese zu manipulieren. Diese Erkenntnisse unterstreichen die Notwen-

digkeit einer umfassenden Herangehensweise an die Sicherheit, die sowohl die App selbst als auch die Übertragung und Speicherung der Daten umfasst.

Die Sicherheit von Gesundheits-Apps ist ein komplexes Feld, das technische, organisatorische und rechtliche Aspekte umfasst. Die Entwickler und Anbieter dieser Anwendungen tragen eine große Verantwortung, die sie zum Beispiel durch die konsequente Anwendung bewährter Sicherheitspraktiken und auch durch die Zusammenarbeit mit Sicherheitsexperten erfüllen können. Nur so lässt sich das Vertrauen der Nutzer gewinnen und erhalten, was für den Erfolg und die Akzeptanz digitaler Gesundheitslösungen entscheidend ist.

Bild: Hengki – stock.adobe.com

HERAUSFORDERUNGEN IM DATENSCHUTZ

Die Gewährleistung der Datensicherheit in Gesundheits-Apps umfasst mehrere Dimensionen. Einerseits müssen Entwickler und Betreiber solcher Anwendungen sicherstellen, dass die erhobenen Daten vor unbefugtem Zugriff geschützt sind. Die Umsetzung der Einhaltung datenschutzrechtlicher Vorgaben wie der Datenschutzgrundverordnung (DSGVO) muss daher integraler Bestandteil der Apps sein. Andererseits ist es ebenso wichtig, dass die Integrität und Verfügbarkeit der Daten gewahrt bleibt, um eine kontinuierliche und fehlerfreie Nutzung zu ermöglichen. Diese Herausforderungen werden durch die Vielfalt und Sensibilität der verarbeiteten Daten noch verstärkt.

Das Risiko von Datenschutzverletzungen ist dabei nicht zu unterschätzen. Denn Vorfälle können zu einem empfindlichen Verlust des Vertrauens in die betreffende App führen, rechtliche Konsequenzen nach sich ziehen und nicht zuletzt ernsthafte Auswirkungen auf die Gesundheit und das Wohlbefinden der betroffenen Personen haben. Zudem könnte die Offenlegung sensibler Gesundheitsinformationen ohne die Zustimmung der Nutzer deren Privatsphäre massiv verletzen und zu sozialen oder beruflichen Nachteilen führen.

Ein weiteres Problem stellt die technische Umsetzung effektiver Datenschutzmaßnahmen dar. Viele Gesundheits-Apps sind auf eine ständige Verbindung mit dem Internet angewiesen, um Daten zu synchronisieren und Updates zu erhalten. Dies eröffnet potenzielle Angriffsflächen für Cyberangreifer, die diese Verbindungen ausnutzen könnten, um Schadsoftware zu verbreiten oder Daten abzugreifen. Zudem erfordert die Absicherung der Kommunikation zwischen der App und zentralen Servern den Einsatz fortschrittlicher Verschlüsselungstechnologien, die sowohl die Datenübertragung als auch die gespeicherten Daten selbst schützen.

STANDARDS FÜR EINE SICHERE ANWENDUNG

Um die Sicherheitsrisiken zu minimieren, ist es daher unerlässlich, dass Entwickler von Gesundheits-Apps eine Reihe von Best Practices in Bezug auf Sicherheit implementieren. Dazu gehört die Anwendung starker Verschlüsselungsverfahren sowie die Gewährleistung einer sicheren Authentifizierung und Autorisierung von Nutzern. Darüber hinaus ist eine kontinuierliche Überwachung und Aktualisierung der Schutzmaßnahmen notwendig, um neu entstehende Bedrohungen abzuwehren und den Schutz der Nutzerdaten zu garantieren.

Um diesen Herausforderungen zu begegnen, ist ein mehrschichtiger Ansatz erforderlich, der diverse Sicherheitsmaßnahmen umfasst. Dazu gehören zum Beispiel die Entwicklung sicherer Vorgehensweisen bei der Implementierung („coding best practices"), die regelmäßige Überprüfung der Sicherheitskonfigurationen und die Implementierung von Zugriffskontrollen.

Konkrete Werkzeuge zur Gewährleistung der App-Security stellt beispielsweise das OWASP Mobile Security Testing Guide (MSTG) zur Verfügung. Das OWASP MSTG ist ein umfassendes Handbuch, das Entwicklern, Testern, Softwarearchitekten und Sicherheitsexperten Richtlinien und Techniken bereitstellt, um die Sicherheit von mobilen Anwendungen zu verbessern. OWASP steht für Open Web Application Security Project, eine internationale gemeinnützige Organisation, die sich der Verbesserung der Sicherheit von Software widmet. Das MSTG konzentriert sich speziell auf mobile Anwendungen und deckt verschiedene Aspekte der Sicherheitsprüfung ab, einschließlich der Architektur mobiler Apps, der Datenhaltung, der Netzwerkkommunikation und der Benutzerauthentifizierung.

Das OWASP MSTG bietet:

- **Prüfstandards für mobile Apps:** eine umfassende Checkliste für die Sicherheitsprüfung mobiler Anwendungen, die Entwicklern und Sicherheitstestern als Leitfaden dient.
- **Praxisorientierte Anleitungen:** detaillierte Beschreibungen von Sicherheitsbedrohungen und Angriffsszenarien sowie entsprechende Gegenmaßnahmen und Best Practices zur Sicherung von mobilen Anwendungen.
- **Tools und Techniken:** Empfehlungen zu Werkzeugen und Methoden für die Durchführung von Sicherheitstests bei mobilen Anwendungen.
- **Fallstudien und Beispiele:** konkrete Beispiele und Fallstudien, die zeigen, wie Sicherheitsprinzipien in der Praxis angewendet werden können.

Das MSTG ist ein lebendiges Dokument, das regelmäßig aktualisiert wird, um neue Sicherheitsbedrohungen und Entwicklungen in der Technologie zu berücksichtigen. Es ist frei verfügbar und wird von der Sicherheitsgemeinschaft, die zu OWASP gehört, kollaborativ entwickelt. Das Ziel des MSTG ist es, einen Industriestandard für die Sicherheit von mobilen Anwendungen zu schaffen und das Bewusstsein für mobile Sicherheitsrisiken zu erhöhen.

Ein weiterer Standard für die Sicherstellung der Cybersecurity von mobilen Gesundheitsanwendungen und zudem von Webanwendungen sowie von Hintergrundsystemen im Gesundheitssektor ergibt sich aus der technischen Richtlinie BSI TR-03161 des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Richtlinie legt ein Set von Mindestanforderungen für die IT-Sicherheit von E-Health-Anwendungen fest und richtet sich an Hersteller solcher Anwendungen für mobile Geräte. Sie kann auch als Leitfaden für mobile Anwendungen verwendet werden, die sensible Daten verarbeiten und speichern. Damit eine DiGA außerdem als erstattungsfähige digitale Gesundheitsanwendung aufgenommen wird, ist eine Zertifizierung der App gemäß BSI TR-03161 zwingend erforderlich.

Die Beachtung und Umsetzung dieser Standards führt bereits zu einem hohen Sicherheitsniveau der mobilen Apps. Zusätzlich ist die Durchführung regelmäßiger Sicherheitsaudits und Penetrationstests von entscheidender Bedeutung, um Schwachstellen von Apps zu identifizieren und zu beheben, bevor sie von Angreifern ausgenutzt werden können. Insgesamt erfordert der Schutz der Privatsphäre und der sensiblen Daten in Gesundheits-Apps ein kontinuierliches Engagement von Entwicklern und Anbietern, um den sich ständig weiterentwickelnden Bedrohungen und regulatorischen Anforderungen gerecht zu werden. Das ist nicht nur eine technische Notwendigkeit, sondern auch eine ethische Verpflichtung gegenüber den Nutzern, deren Gesundheit und Wohlergehen von der Sicherheit und Zuverlässigkeit dieser digitalen Hilfsmittel abhängen.

Bild: drawlab19 - stock.adobe.com

UMSETZUNG MITTELS EXTERNER UNTERSTÜTZUNG

Die Umsetzung adäquater Sicherheitsstandards bei der Entwicklung und dem Betrieb von Gesundheits-Apps erfordert allerdings spezialisiertes Wissen und Ressourcen. Während bei gesetzlich regulierten Apps angesichts der komplexen technischen Anforderungen und der strengen gesetzlichen Regulierungen die Hinzunahme externer Expertise für die Prüfung zwingend erforderlich ist, kann sie außerdem in bislang unregulierten Bereichen einen entscheidenden Unterschied und Erfolgsfaktor darstellen. Denn Experten bringen nicht nur tiefgreifendes Verständnis für Sicherheitsprotokolle und Datenschutzgesetze mit, sondern auch Erfahrungen aus einer Vielzahl von Projekten, die innovative Lösungen für häufig auftretende Probleme bieten können.

Darüber hinaus können externe Sicherheitsexperten technische Unterstützung bei der Implementierung von Sicherheitsmaßnahmen bieten, die speziell auf die Bedrohungslandschaft und die technische Architektur der Gesundheits-App zugeschnitten sind. Dazu gehören die Verschlüsselung von Daten sowohl bei der Übertragung als auch bei der Speicherung, die Entwicklung sicherer Authentifizierungsverfahren und die Implementierung von Systemen zur Erkennung und Reaktion auf Sicherheitsvorfälle. Sie können auch bei der Durchführung von Penetrationstests und Sicherheitsaudits unterstützen.

Ein weiterer Aspekt, bei dem externe Partner eine Rolle spielen, ist die Unterstützung bei der Entwicklung und Implementierung eines effektiven Informationssicherheitsmanagementsystems (ISMS). Ein solches System umfasst nicht nur technische Maßnahmen, sondern auch organisatorische Richtlinien und Verfahren, die darauf abzielen, die Sicherheit der verarbeiteten Daten kontinuierlich zu gewährleisten. Externe Berater können zudem wertvolle Einblicke in Best Practices aus anderen Branchen bieten, die für die spezifischen Anforderungen von Gesundheits-Apps angepasst werden können.

Abschließend ist die Zusammenarbeit mit externen Experten nicht nur eine Maßnahme zur Erfüllung gesetzlicher Anforderungen, sondern stellt auch eine Investition in die Qualität und Sicherheit der Gesundheits-App dar. Durch die Einbindung von Spezialisten können Entwickler und Anbieter von Gesundheits-Apps nicht nur die Sicherheit und den Datenschutz ihrer Anwendungen verbessern, sondern auch das Vertrauen der Nutzer stärken, was in der digitalen Gesundheitsbranche von unschätzbarem Wert ist.

FAZIT

Gesundheits-Apps haben ein erhebliches Potenzial, die Gesundheitsversorgung zu verbessern und den Nutzern dabei zu helfen, ein gesünderes Leben zu führen. Sie reichen von Lifestyle-Apps über Apps auf Rezept bis hin zu Anwendungen, die eine zentrale Rolle in der Telematikinfrastruktur spielen, und können wichtige Gesundheitsdaten sammeln und analysieren, um informierte Entscheidungen zu unterstützen.

Allerdings steht dem Nutzen ein signifikantes Risiko gegenüber: die Sicherheit und der Schutz sensibler Nutzerdaten. Die Zunahme digitaler Gesundheitsanwendungen verstärkt die Bedenken hinsichtlich der Datensicherheit, besonders angesichts der Vielzahl sensibler Informationen, die diese Apps sammeln. Die Bedrohungen sind vielfältig, reichen von Datenschutzverletzungen bis hin zu Cyberkriminalität und können ernsthafte Folgen für die Nutzer haben.

Um die Sicherheitsrisiken zu minimieren, ist eine umfassende Herangehensweise an die Sicherheit erforderlich, die sowohl die App-Entwicklung als auch die Datenübertragung und -speicherung umfasst. Entwickler müssen Best Practices in Bezug auf Sicherheit implementieren, darunter starke Verschlüsselungsverfahren, sichere Authentifizierung, regelmäßige Sicherheitstests sowie die Einhaltung datenschutzrechtlicher Vorgaben wie der DSGVO. Die Einbindung externer Berater kann dabei helfen, die notwendigen Sicherheits- und Datenschutzanforderungen zu erfüllen und gleichzeitig das Vertrauen der Nutzer zu stärken. ■

PETER JUNG
ist Senior Consultant Software Security bei der SRC Security Research & Consulting GmbH.

Sichere Messenger im Business am Beispiel von Signal

E-MAIL WAR GESTERN

In der heutigen Geschäftswelt, in der schnelle und effektive Kommunikation unerlässlich ist, setzen viele Unternehmen neben der guten alten E-Mail auch auf Messenger-Dienste. Doch wie sicher sind diese Kommunikationsmittel? Unser Autor beschreibt anhand von Signal die wichtigsten Funktionen, um Datenlecks zu verhindern und die Integrität der Kommunikation zu gewährleisten.

Messenger sind aus unserem Leben nicht mehr wegzudenken. Das gilt für unser Privatleben, in dem wir mit der Familie, dem Sportverein oder der Kita-Elterngruppe mittlerweile vorwiegend über Messenger kommunizieren. Es gilt aber auch zunehmend für die berufliche Kommunikation. Laut der Studie „Nutzung von Online-Kommunikationsdiensten in Deutschland" der Bundesnetzagentur aus dem Jahr 2023 benutzen 78 Prozent der deutschen Firmen Messenger und Sofortnachrichtendienste für die geschäftliche Kommunikation.

Als meistgenutzte Softwarelösung liegt mit Microsoft Teams zwar ein Businessprodukt auf dem ersten Platz, auf dem zweiten Platz folgt mit WhatsApp allerdings schon ein klassischer Messenger, der nicht dezidiert für den Unternehmensbereich konzipiert wurde. Und auch andere Messenger wie Facebook Messenger, Signal, Threema oder Telegram sind prominent in der Liste vertreten.

Gerade in kleineren Betrieben ersetzen Messenger dabei oft Business-Lösungen wie Teams, Zoom oder Slack. Auch weil Messenger meist kostenlos sind und sich zur gleichzeitigen Kommunikation mit den Kunden eignen.

Aus Sicht der IT-Sicherheit lohnt es sich daher, Messenger in der Unternehmenskommunikation näher zu betrachten. Im Folgenden soll dies exemplarisch am Beispiel von Signal geschehen, da der Messenger ein besonderes Augenmerk auf Datenschutz und Sicherheit legt. Dabei werden die Stärken für den Unternehmenseinsatz aufgezeigt, aber auch wo noch Lücken, Einschränkungen und eventueller Nachholbedarf bestehen.

KERNBESTANDTEILE

Moderne Messenger zeichnen sich durch essenzielle Sicherheitsmerkmale aus, die den Schutz sensibler Daten und die Privatsphäre der Nutzer gewährleisten sollen. Am Beispiel der Funktionsweise von Signal gibt es folgende Kernelemente:

1. Ende-zu-Ende Verschlüsselung

Manch einer erinnert sich vielleicht noch an Pretty Good Privacy (PGP), das sichere, aber recht umständliche Verfahren zur Ende-zu-Ende-Verschlüsselung von E-Mails. Bereits Anfang der 1990er-Jahre entwickelt, konnte sich PGP nie über Nischen hinaus durchsetzen. Während die Transportverschlüsselung im Online-Bereich durch Initiativen wie Let's Encrypt oder HTTPS Everywhere immer mehr zum Standard wurde, blieb das Thema Ende-zu-Ende-Verschlüsselung etwas auf der Strecke.

Das änderte sich erst mit dem Aufkommen der Messenger, die auch die letzte Lücke in der Verschlüsselungskette schlossen und schlussendlich echte Ende-zu-Ende Verschlüsselung für große Kommunikationsbereiche etablierten.

Exkurs: Signal-Protokoll

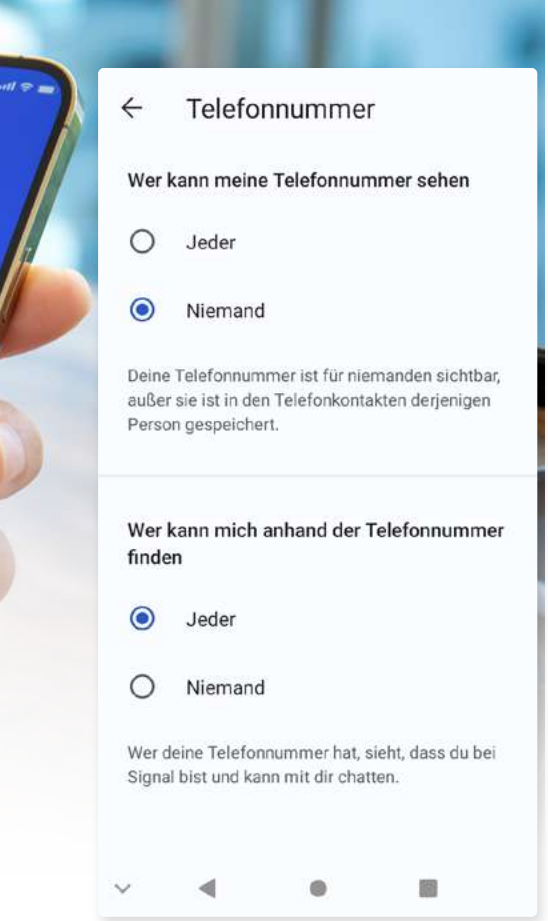
Im Zentrum dieser Entwicklung steht das Signal-Protokoll. Es wurde 2013 von den Signal-Entwicklern Moxie Marlinspike und Trevor Perrin entworfen und seitdem kontinuierlich weiterentwickelt. Es besteht aus einer innovativen Kombination existierender kryptografischer Elemente, um eine sichere asynchrone Kommunikation zwischen zwei oder mehr Teilnehmern zu ermöglichen. Die technischen Spezifikationen des Protokolls finden sich unter https://signal.org/docs/, und der zugehörige Code ist Open Source unter https://github.com/signalapp/libsignal zugänglich.

Kernelemente sind dabei ein Schlüsselaustausch via Extended Triple Diffie-Hellman sowie der „selbstheilende" Double-Ratchet-Algorithmus, der zu einem ständigen Wechsel der Schlüssel führt. Selbst für den unwahrscheinlichen Fall, dass ein Schlüssel von einem Angreifer geknackt werden würde, könnte damit nur eine einzige Nachricht entschlüsselt werden. Alle anderen Nachrichten wären davon nicht betroffen.

2023 wurde das Protokoll schließlich mittels Post-Quantum Extended Diffie-Hellman (PQXDH) um Post-Quanten-Kryptografie erweitert, um vor etwaigen zukünftigen „harvest now, encrypt later"-Angriffen durch Quantencomputer zu schützen.

Heute gilt das Signal-Protokoll als Gold-Standard in Sachen Ende-zu-Ende-Verschlüsselung und wird von allen großen Tech Unternehmen wie Google, Meta und Microsoft zur Verschlüsselung in Produkten wie WhatsApp, Facebook Messenger, Skype oder Google Messages genutzt. Auch

Bild: DenPhoto - stock.adobe.com



In Signal ist es möglich, die eigene Telefonnummer vor anderen zu verbergen. (Bild: Signal Stiftung)

Apple verwendet in iMessage eine Ende-zu-Ende-Verschlüsselung, die sich an der Struktur des Signal-Protokolls orientiert.

2. Schutz von Metadaten

Die Ende-zu-Ende-Verschlüsselung der Kommunikationsinhalte ist jedoch nur ein Aspekt sicherer und geschützter Kommunikation. Von großer Bedeutung sind auch die sogenannten Metadaten, die bei der Kommunikation über Messenger anfallen. Beispielsweise wer mit wem kommuniziert, wer Mitglied welcher Gruppen ist, Profilinformationen oder der Zeitpunkt des Kontakts.

Sichere Messenger wie Signal verschlüsseln und schützen auch diese Daten so gut wie möglich und folgen dem „Zero Knowledge"-Prinzip. So verbirgt beispielsweise das „Sealed Sender"-Verfahren von Signal den Absender einer Nachricht vor dem Signal-Server. Nur der Empfänger kann sehen, wer der Absender ist und kann dies auch durch eine Sicherheitsnummer verifizieren, um Man-in-the-Middle-Angriffe zu verhindern. Auch das Verbergen der eigenen Telefonnummer vor anderen Kommunikationsteilnehmern, wie es mit Signal möglich ist, fällt unter den wichtigen Schutz dieser Metadaten.

3. Open Source

Das Prinzip, so wenig Daten wie möglich zu speichern wird bei sicheren Messengern im Sinne eines Zero-Trust-Ansatzes um den Open-Source-Aspekt erweitert. Denn wenn alle Daten, die über die Server des Anbieters laufen, sicher verschlüsselt werden und gleichzeitig die Verlässlichkeit der eingesetzten Software verifiziert werden kann, dann kann die Sicherheit der Kommunikation weitgehend garantiert werden, ohne dem Messenger-Anbieter selbst vertrauen zu müssen. Deshalb nutzen sichere Messenger wie Signal oder Threema „reproducible builds" und veröffentlichen ihren Code als Open Source – bei Signal gilt das sogar für den serverseitigen Code.

WEITERE VORTEILE: KOSTENLOS UND BEREITS BEKANNT

Neben den sicherheitsrelevanten Vorteilen verschlüsselter Messenger gibt es noch zwei weitere Aspekte die besonders aus wirtschaftlicher Sicht für viele, gerade kleinere Unternehmen, relevant sind. Zum einen ist die Nutzung von Messengern wie Signal in der Regel kostenlos – auch wenn es mit WhatsApp Business oder Threema Work mittlerweile eigene kostenpflichtige Angebote für große Unternehmen gibt. Zum anderen kann die Nutzung von Messengern mittlerweile quasi als bekannt vorausgesetzt werden – sowohl bei Mitarbeitern aber auch bei Kunden. Aufwendige Schulungen oder Maßnahmen zur Etablierung des Kanals entfallen daher in der Regel.

EINSCHRÄNKUNGEN UND AUFHOLBEDARF

Bei all den Vorteilen, die sichere Messenger für die Unternehmenskommunikation mit sich bringen, gibt es aber auch einige Einschränkungen:

- **Offizielle API:** Um bestimmte Abläufe zu automatisieren, benötigen größere Unternehmen in vielen Fällen API-Zugriff für ihre Kommunikationstools. Signal bietet bislang keine offizielle API an, es existiert jedoch eine freie Community-Version einer Signal-API, die auf dem offiziellen Signal-Code basiert. Auch viele Anbieter von Multi-Messenger-Diensten oder Entwickler von Chatbot-Lösungen nutzen diese Community-API. Dabei handelt es sich jedoch nicht um eine offizielle, von Signal unterstützte API mit garantierter Verfügbarkeit und Kompatibilität. Das kann insbesondere für große Unternehmen ein Problem darstellen.

- **Begrenzung der Teilnehmeranzahl:** Um eine effiziente Verschlüsselung zu gewährleisten und um sich auf die Kernfunktionen eines Messengers zu beschränken, ist bei Signal die maximale Teilnehmerzahl in Gruppen auf 1.000 Personen begrenzt. Bei Videoanrufen stehen alle bekannten Funktionen wie das Teilen des Bildschirms, Handheben oder Emoji-Reaktionen zur Verfügung. Allerdings können – ähnlich wie bei WhatsApp – maximal 40 Personen an einer Videokonferenz teilnehmen. Der Einsatz klassischer Messenger eignet sich daher vor allem für kleine und mittlere Unternehmen, die diese Beschränkungen kaum erreichen dürften.

- **Keine Möglichkeit zum Selbst-Hosting:** Die Möglichkeit einer On-Premises-Lösung ist bei Signal und den meisten anderen Messengern nicht vorgesehen. Durch den „Zero Knowledge"-Ansatz von Signal und den Einsatz einer Ende-zu-Ende-Verschlüsselung für alle Inhalte und Metadaten wäre ein Mehr an Datenschutz aber ohnehin nicht gegeben. Für Unternehmen, die jedoch Wert auf diesen Aspekt legen und den erhöhten Administrationsaufwand einer On-Premises-Lösung nicht scheuen, ist ein dezentraler Messenger wie Matrix vermutlich die bessere Wahl.

FAZIT

Wie das Beispiel Signal zeigt, bieten moderne Messenger grundsätzlich viele Möglichkeiten und großes Potenzial für den sicheren Einsatz in Unternehmen. Das Plus an Sicherheit und Datenschutz bei gleichzeitig hoher Benutzerfreundlichkeit macht heutige Messenger gerade für kleine und mittelständische Unternehmen zu einer ernst zu nehmenden Alternative für die interne Kommunikation. Große Unternehmen sind jedoch aufgrund der bestehenden Restriktionen vermutlich weiterhin besser mit klassischen Business-Produkten bedient. ■

DR. MARTIN BARTENBERGER
ist IT-Consultant und DACH-Manager der gemeinnützigen Signal Stiftung, die den Messenger Signal entwickelt und betreibt.

Wie Sender Tracking und Cookies einsetzen

HBBTV UND DIE DATENSAMMELWUT

HbbTV hat sich zu einer beliebten Möglichkeit entwickelt, traditionelles Fernsehen mit internetbasierten Inhalten zu kombinieren. Die Technologie wirft jedoch auch Bedenken hinsichtlich des Schutzes der Privatsphäre der Nutzer auf. Eine Studie hat nun untersucht, wie Daten gesammelt und Nutzer getrackt werden – mit alarmierenden Ergebnissen.

Trotz der wachsenden Beliebtheit moderner Streaming-Dienste ist das Fernsehen nach wie vor ein wichtiges Kommunikations- und Unterhaltungsmedium. Seit der Einführung des HbbTV-Standards im Jahr 2006 hat sich das traditionelle lineare Fernsehen stark weiterentwickelt. Hybrid Broadcast Broadband TV (HbbTV) kombiniert klassisches Fernsehen mit On-Demand-HTML5-Inhalten. Die Technologie, die eine Internetverbindung voraussetzt, bietet zusätzliche Funktionen wie Hintergrundinformationen zu Sendungen und den Zugang zu Mediatheken. HbbTV hat sich vor allem in Europa und besonders in Deutschland etabliert.

HbbTV wirft jedoch auch Fragen der Sicherheit und des Datenschutzes auf. Die Nutzung dieser Technologie ermöglicht es den Kanalbetreibern, Informationen über ihre Zuschauer zu sammeln und zu verfolgen, was zur Erstellung detaillierter „Zuschauerprofile" führt. In der Europäischen Union sind die Anbieter verpflichtet, Datenschutzgesetze wie die Datenschutz-Grundverordnung (DSGVO) einzuhalten, um die Privatsphäre der Nutzerinnen und Nutzer zu schützen.

Obwohl sich frühere Studien mit den Sicherheits- und Datenschutzaspekten von HbbTV befasst haben, wurden das HbbTV-Tracking-Ökosystem und die damit verbundenen Datenschutzfragen bisher kaum umfassend untersucht. Eine groß angelegte Untersuchung von 391 europäischen HbbTV-Kanälen hat nun herausgefunden, wie Daten gesammelt und Nutzerinnen und Nutzer getrackt werden. Darüber hinaus wurden die Datenschutzrichtlinien bewertet und die Einwilligungserklärungen analysiert.

DAS MESS-FRAMEWORK

Die Studie erforderte eine präzise und sorgfältig konzipierte Messinfrastruktur – Abbildung 1 stellt einen Überblick über den verwendeten Versuchsaufbau dar. Für die Untersuchung wurde ein LG 43UK6300 LLB-Fernseher mit HbbTV-Unterstützung verwendet, der mit dem RootMyTV 2.0 Rootkit [8] gerootet wurde. Das ermöglichte die Installation eines Zertifikats im Zertifikatsspeicher des Fernsehers, um TLS-geschützten Netzwerkverkehr abzufangen und zu entschlüsseln. Mit der aktualisierten Version der LG-Firmware funktioniert dieses Rootkit allerdings nicht mehr.

Als Analysegerät diente ein Desktop-Computer, der den Fernseher über einen Wi-Fi-Hotspot mit dem Internet verband. Mit dem HTTP(S)-Proxy mitmproxy (Version 9.0) [1] ließ sich dann der HTTP(S)-Verkehr abfangen. Das Proxy-Zertifikat wurde auf dem gerooteten TV-Gerät installiert, sodass die Forscher den größten Teil des HbbTV-Datenverkehrs entschlüsseln konnten. Aufgrund der fehlenden Zertifikatsvalidierung durch die analysierten Sender war es möglich, den gesamten HTTP(S)-Verkehr zu erfassen. Zusätzlich wurde die webOS TV Developer API [4] verwendet, um Informationen über den aktuellen Sender zu sammeln und Screenshots der angezeigten Inhalte zu erstellen. Auch Daten aus dem Cookie-Speicher und dem lokalen Speicher des Fernsehers wurden erfasst.

Der Fernsehempfang erfolgte über eine Parabolantenne, die Signale von drei Satelliten empfing: Astra 1L (19,2°O), Hot Bird 13E (13,0°O) und Eutelsat (16,0°O). Diese ermöglichten den Empfang von Fernsehsendern aus verschiedenen europäischen Ländern, wobei der physische Standort der Studie in Deutschland war.

Das anfänglich empfangene Signal umfasste 3.575 Sender. Viele davon waren jedoch ungeeignet, da sie entweder keine Programme ausstrahlten, verschlüsselt waren oder Radiosender darstellten. Am Ende des Filterprozesses verblieben 391 Fernsehsender.

Das „Fernbedienungsskript" implementierte fünf Profile, die verschiedene Benutzerinteraktionen mit dem Fernseher simulierten, um unterschiedliche HbbTV-Anwendungen für jeden Kanal auszulösen.

- **Profil ohne simulierte Benutzerinteraktion (General):** Beobachtete jeden Kanal 900 Sekunden lang ohne weitere Interaktionen.
- **Farbtasten-Profile (Rot, Blau, Gelb und Grün):** Jedes Profil beinhaltete geskriptete Interaktionen mit der jeweiligen farbigen Taste. Nach dem Kanalwechsel wartete das Skript zehn Sekunden und drückte dann die jeweilige Farbtaste. Anschließend wurden zufällig Navigationsknöpfe gedrückt, um mit dem möglicherweise geladenen neuen Inhalt zu interagieren.

Diese detaillierte und methodische Herangehensweise ermöglichte eine umfassende Erfassung und Analyse des HbbTV-Datenverkehrs und der damit verbundenen Datenschutzpraktiken.

ERGEBNISSE: TRACKING UND 1.700 COOKIES

Die Messungen ergaben, dass 1.705 verschiedene Cookies über HTTP(S) gesetzt wurden. Durchschnittlich wurden pro Kanal 4,1 Cookies gesetzt, wobei 166 unterschiedliche Drittanbieter beteiligt waren. Bemerkenswert ist, dass nur 20,5 Prozent der Cookies von Cookiepedia klassifiziert werden konnten, was darauf hindeutet, dass sich das HbbTV-Ökosystem stark vom Web-Ökosystem unterscheidet.

Verbreitung von Third-Party-Cookies

Cookies von Drittanbietern sind im HbbTV-Ökosystem mit durchschnittlich 3,1 Cookies pro Kanal weit verbreitet. Eine signifikante Anzahl dieser Cookies wird für Trackingzwecke verwendet. Die häufigste Third-Party-Domain war xiti.com, die auf 119 Kanälen beobachtet wurde. Insgesamt zeigen die Ergebnisse, dass HbbTV-Kanäle häufig auf Third-Party-Dienste und Cookies zurückgreifen, was auf umfangreiche Tracking-Praktiken hindeutet. Nur 25 Drittparteien wurden auf mehr als zehn Kanälen verwendet, was

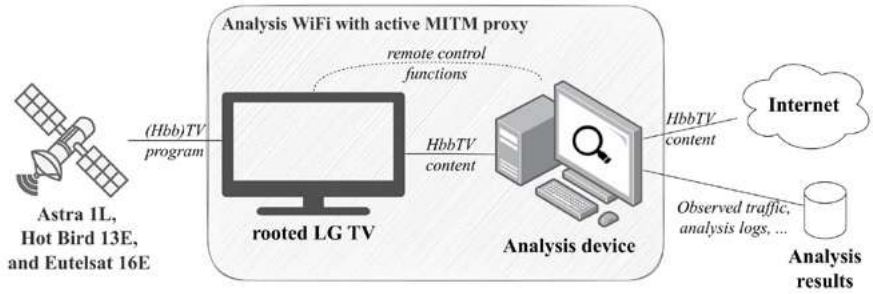


Abbildung 1: Messframework HbbTV (Bild: if(is))

Bild: Robert Daly/KOTO - stock.adobe.com

auf ein verstreutes Third-Party-Cookie-Ökosystem hinweist, im Gegensatz zum Web, das von wenigen großen Akteuren dominiert wird. Tabelle 1 gibt einen Überblick, über die Anzahl der Third-Parties und die Anzahl der Cookies, die diese bei jedem Profil setzen.

PROFIL	# 3PS	# 3P COOKIES	MEAN	MIN	MAX	SD
GENERAL	36	167	2,31	1	8	1,74
ROT	107	560	3,59	1	22	5,82
GRÜN	77	287	3,69	1	21	4,27
BLAU	47	189	2,04	1	16	2,34
GELB	88	300	3,2	1	24	4,16

Tabelle 1: Cookies von Third Parties nach Profilen

Kommunikation zwischen Third-Parties: Cookie-Syncing

Während viele Drittanbieter direkt auf mehreren Kanälen eingebettet sind, bleibt unklar, ob sie untereinander Daten austauschen. Cookie-Syncing, ein zweistufiger Prozess, ermöglicht den Datenaustausch zwischen Drittparteien. Dabei lädt eine Website zunächst ein Drittanbieter-Skript, welches dann an einen Synchronisierungspartner weitergeleitet wird. Diese weitergeleitete Anfrage enthält beispielsweise eine Benutzer-ID.

Um Cookie-Syncing in den Daten zu identifizieren, analysierte man, ob eine Drittpartei eine HTTP-Anfrage mit einem (Cookie-)Identifikator an eine andere Partei sendete. Dazu adaptierten die Forscher eine Methode von Acar et al. zur Identifizierung von Cookies, die möglicherweise eine ID enthalten könnten. Dabei betrachtet man einen Cookie-Wert als einen Identifikator, wenn er: (1) zwischen 10 und 25 Zeichen lang war (d. h. genügend Entropie für eine ID aufwies) und (2) kein gültiger Unix-Zeitstempel innerhalb des Messzeitraums war. Viele Cookie-Werte enthalten solche Zeitstempel für unterschiedliche Zwecke, zum Beispiel zur Einholung von Einwilligungen oder beim Kanalwechsel.

Diese Methode identifizierte 14.236 Cookie-Werte, die potenziell eine ID sein könnten. Von diesen wurden 25 Werte in einer HTTP-Anfrage an eine andere Partei übertragen. Die meiste Synchronisierungsaktivität fand im Rot-Profil statt, während im Allgemeinen und im Gelben Profil keine einzige Instanz beobachtetet wurde. Nur zwei Domains (nach eTLD+1) verursachten Synchronisierungsaktivitäten, wobei die Cookies Benutzer-IDs enthielten. Diese Domains waren adform.net mit 22 (88 %) Synchronisierungsaktivitäten (Cookie-Name: uid) und arte.tv mit drei (12 %) Synchronisierungsaktivitäten (Cookie-Name: deviceId).

Insgesamt beobachteten die Autoren der Studie Cookie-Syncing-Aktivitäten auf 20 Kanälen. Im Vergleich zu Cookie-Syncing im Web, wo etwa 500 Synchronisierungsverbindungen identifiziert wurden [9], ist die Technologie in HbbTV-Anwendungen weniger verbreitet.

Tracking-Methoden und ihre Verbreitung

Tracking ist ein weit verbreitetes Phänomen in vielen digitalen Diensten. Um zu bewerten, inwieweit HbbTV-Anwendungen solche Techniken nutzen, wurden alle vollständigen URLs aus dem HTTP-Verkehr mit Filterlisten wie EasyList [2] und der Pi-hole-Blockliste [7] verglichen. Es stellte sich heraus, dass nur 0,5 Prozent der URLs von EasyList und 1,17 Prozent von Pi-hole markiert wurden (siehe Tabelle 2). Dies könnte darauf hindeuten, dass Tracking in HbbTV-Anwendungen entweder weniger verbreitet ist oder von anderen Parteien durchgeführt wird als im Web.

Einsatz von Tracking-Pixeln

Tracking-Pixel sind nahezu unsichtbare Bilder, die verwendet werden, um Nutzer zu verfolgen. Die Studienautoren identifizierten Tracking-Pixel anhand von drei Kriterien: (1) Der HTTP-Content-Typ zeigt ein Bild an, (2) die Datenmenge ist kleiner als 45 Byte und (3) der HTTP-Response-Code ist 200 (OK). Es konnten so insgesamt 277.574 Tracking-Anfragen identifiziert werden, von denen nur 0,2 Prozent von EasyList markiert wurden. Diese Anfragen stammten von 47 verschiedenen eTLD+1, wobei acht (17 %) auf EasyList standen.

Fingerprinting-Techniken

Fingerprinting wird häufig verwendet, um Nutzende ohne Cookies zu verfolgen. Die Studienautoren untersuchten Antworten, die JavaScript-Code enthielten und Skripte, die APIs wie Canvas oder WebGL nutzen. Dieser Ansatz identifizierte 60 (15 %) Sender, die Fingerprinting-Techniken verwendeten, was mit dem Anteil der Websites vergleichbar ist, auf denen diese Technik genutzt wird. Von allen identifizierten Fingerprinting-Anfragen wurde nur eine eTLD+1 von EasyList markiert.

Unzureichende Blocklisten für Smart TVs und HbbTV

Spezielle Blocklisten für Smart-TVs und HbbTV, wie die von Perflyst [6] und Kamran [5], blockierten deutlich weniger Tracking-Anfragen als die reguläre Pi-hole-Filterliste. Dies zeigt, dass diese Listen Nutzer nicht ausreichend vor HbbTV-spezifischem Tracking schützen. Häufig verwendete Tracker wie tvping.com fehlen auf diesen Listen, was darauf hinweist, dass der Fokus dieser Listen auf Anwendungen wie Netflix liegt und nicht auf HbbTV.

PROFILE	PI-HOLE	EASY LIST	TRACKING PIXEL	FINGERPRINTS
GENERAL	203	6	80.960	51
ROT	2.120	1.375	90.199	536
GRÜN	1.051	463	14.593	161
BLAU	313	8	5.925	179
GELB	1.668	660	85.897	151

Tabelle 2: Tracking in HbbTV Profilen

Besonders kritisch ist das Tracking auf Kinderkanälen. Gemäß der DSGVO [3] müssen Kanäle, die Programme für Kinder anbieten, ihre Datenpraktiken anpassen. In der Untersuchung wiesen zwölf Kinderkanäle 2.214 Tracking-Anfragen auf und setzten 97 Drittanbieter-„Targeting/Advertising"-Cookies. Das könnte gegen die DSGVO verstoßen. In der statistischen Analyse trat jedoch kein signifikanter Unterschied im Tracking-Verhalten zwischen Kinderkanälen und anderen Kanälen auf.

Das HbbTV-Tracking-Ökosystem

Das HbbTV-Tracking-Ökosystem unterscheidet sich signifikant vom Web-Ökosystem. Ein Netzwerkgraph basierend auf dem beobachteten HbbTV-Verkehr offenbarte ein gut vernetztes System mit 429 Knoten und 675 Kanten. Die am stärksten verbundenen Knoten waren ard.de, redbutton.de und rtl-hbbtv.de, die alle zu deutschen TV-Netzwerken gehören. Diese Ergebnisse werfen die Frage auf, ob HbbTV-Kanäle transparent über ihr Tracking informieren und den Nutzenden Wahlmöglichkeiten bieten. Abbildung 2 stellt das HbbTV-Tracking-Ökosystem dar, in dem blaue Knoten die Kanäle und rote Knoten die First- und Third-Parties repräsentieren. Die Knotengröße gibt die Anzahl der Verbindungen an.

Kanalbasierte Analysen

Die vorangegangene Analyse konzentrierte sich auf verschiedene Messprofile, die die Interaktion der Nutzer mit HbbTV-Anwendungen simulierten. Darüber hinaus wurden die Datenschutzpraktiken der einzelnen Sender untersucht, um

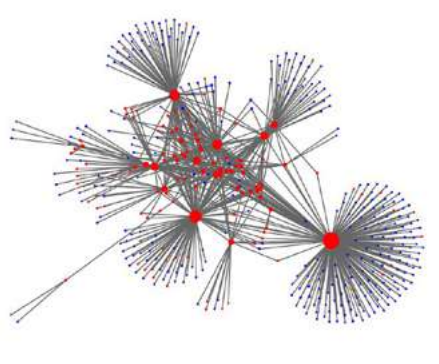


Abbildung 2: Das HbbTV-Tracking-Ökosystem, blaue Knoten repräsentieren die Kanäle, rote Knoten die First- und Third-Parties. Die Größe eines Knotens zeigt die Anzahl seiner Kanten an. (Bild: if(is))

festzustellen, ob einige Sender die Privatsphäre der Zuschauer stärker beeinträchtigen, indem sie

HBBTV: REVOLUTION DES FERNSEHENS DURCH HYBRIDTECHNOLOGIE

Hybrid Broadcast Broadband TV (HbbTV) ist ein Industriestandard, entwickelt vom Europäischen Institut für Telekommunikationsnormen (ETSI), der darauf abzielt, internetbasierte Inhalte nahtlos mit linearen TV-Programmen zu verbinden. HbbTV ermöglicht es Geräten, die einen Decoder für digitales Fernsehen (Broadcast) und einen Internetzugang (Breitband) besitzen, interaktive Anwendungen zu nutzen. Diese Anwendungen bieten Zusatzelemente zum TV-Programm, wie Video-on-Demand-Dienste, elektronische Programmführer oder interaktive Werbung.

Beispielsweise können solche Inhalte als Overlay über das laufende TV-Programm eingeblendet oder das Programm vollständig ersetzt werden, sodass es nicht mehr sichtbar oder hörbar ist. Kanäle bieten oft einen Einstiegspunkt zu diesen zusätzlichen Inhalten, wenn der Nutzer den Kanal wechselt.

Ein wesentlicher Meilenstein für HbbTV war die Veröffentlichung der Hauptversion 2.0 im Jahr 2015, die bedeutenden Änderungen im HbbTV-Ökosystem einführte, darunter die Fähigkeit, HTML5-Inhalte auf Fernsehgeräten darzustellen. Diese Weiterentwicklung hat die Möglichkeiten für interaktive Inhalte erheblich erweitert und das Nutzerlebnis verbessert.

Um HbbTV-Inhalte anzubieten, wird die URL jeder Anwendung, die ein Kanal bereitstellt, im linearen Broadcast-Signal kodiert. Unterstützt ein Fernseher den HbbTV-Standard, kann er sich mit diesem Endpunkt verbinden und die entsprechende Anwendung laden. Die Übertragung der Anwendungen erfolgt üblicherweise über das HTTP-Protokoll. Für die Darstellung und Ausführung der Anwendungen muss jeder Fernseher eine geeignete Laufzeitumgebung implementieren, die browserähnlich ist und HTML5-Seiten anzeigen, JavaScript-Code ausführen und andere Elemente von Webanwendungen verarbeiten kann.

HbbTV eröffnet neue Möglichkeiten der Interaktion und Informationsbereitstellung und trägt dazu bei, das Fernsehen in das digitale Zeitalter zu führen. Abbildung 1 zeigt ein Beispiel für HbbTV-Inhalte, während Abbildung 2 einen allgemeinen Ablauf darstellt, wie HbbTV-Inhalte über dem linearen TV-Programm angezeigt und aus dem Internet geladen werden.

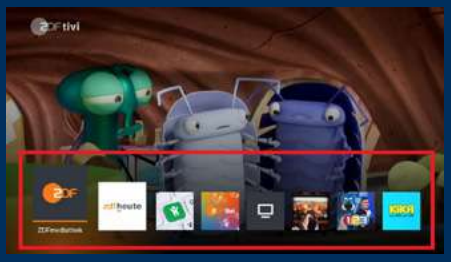


Abbildung 1: Beispiel für HbbTV-Elemente (Bild: if(is))

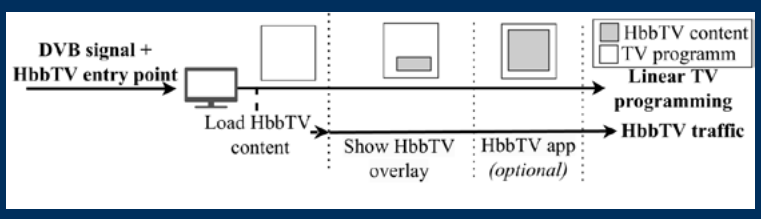


Abbildung 2: HbbTV-Ablauf für das Laden von linearem TV und interaktiven Elementen aus dem Internet (Bild: if(is))

beispielsweise mehr personenbezogene Daten sammeln. Dabei wurden nur Kanäle berücksichtigt, bei denen mindestens eine Tracking-Anfrage beobachtet wurde.

Durchschnittlich sendete ein Kanal 1.132 Tracking-Anfragen, wobei die Spannweite von 1 bis 59.499 reichte. Ein einzelner Kanal stellte dabei 59.499 Tracking-Anfragen, von denen 99,7 Prozent an tvping.com gingen – und das ausschließlich im Rot-Profil. Im Schnitt kontaktierten die Kanäle 7,25 Tracker. Die zehn Kanäle mit den meisten Trackern machten 6,34 Prozent der gesamten Tracking-Anfragen aus. Das verdeutlicht, dass nicht nur wenige Kanäle, sondern viele für die Tracking-Anfragen verantwortlich sind. Statistische Analysen ergaben, dass die Anzahl der verwendeten Tracker stark vom jeweiligen Kanal abhängt. Bestimmte Kanäle verfolgen Nutzer intensiver als andere, aber Tracking ist generell auf allen präsent. Zudem hatte das Benutzerprofil, also welcher Knopf gedrückt wurde, einen größeren Einfluss auf das Tracking-Verhalten als der Kanal selbst. Dies bedeutet, dass die Benutzerinteraktion das Ausmaß des Trackings stärker beeinflusst als der betrachtete Kanal.

EMPFEHLUNGEN: DATENSCHUTZ VERBESSERN

Die Studie hat den Datenschutz im europäischen HbbTV-Bereich unter die Lupe genommen. Anhand eines Messrahmens sammelten die Forscher den HTTP(S)-Datenverkehr von 391 HbbTV-Kanälen und bewerteten deren Datenschutzpraktiken in drei wesentlichen Bereichen: Nutzende-Tracking, Einwilligungskontrollen und Datenschutzrichtlinien. Die Ergebnisse sind alarmierend: Die überwiegende Mehrheit (95 %) der analysierten Kanäle verfolgt ihre Zuschauer mittels Tracking-Pixeln oder Geräte-Fingerprinting.

Dabei unterscheidet sich das HbbTV-Tracking-Ökosystem deutlich vom Web-Ökosystem und bezieht weitere Akteure ein. Trotz der verbreiteten Nutzung von Tracking-Technologien sind diese Praktiken oft schlecht dokumentiert oder nicht offengelegt. Besonders bedenklich ist das Tracking auf Kanälen, die sich an Kinder richten, da hier besondere Datenschutzanforderungen gemäß der DSGVO gelten.

Von den 57 untersuchten Datenschutzrichtlinien wiesen viele erhebliche Mängel auf, darunter nicht deklariertes Tracking und inkonsistente Offenlegungen. Die Zuschauer können sich derzeit nicht darauf verlassen, dass die Standardfilterlisten sie vor Tracking im HbbTV-Bereich schützen.

Angesichts der Ergebnisse sollten die Verantwortlichen maßgeschneiderte Filterlisten für HbbTV entwickeln, die spezifisch auf die Tracking-Praktiken in diesem Bereich abgestimmt sind, um so einen besseren Schutz der Privatsphäre der Zuschauer zu gewährleisten. Zudem ist es essenziell, dass HbbTV-Anbieter ihre Datenschutzpraktiken überarbeiten und für mehr Transparenz sorgen. Das umfasst klare und vollständige Datenschutzrichtlinien sowie effektive Einwilligungskontrollen, die den Zuschauern echte Wahlmöglichkeiten bieten.

Die Umsetzung dieser Maßnahmen würde dazu beitragen, den Datenschutz im Bereich HbbTV deutlich zu verbessern und das Vertrauen der Zuschauer in die Nutzung dieser Dienste zu stärken. ■

Literatur

[1] Cortesi, A., Hils, M., Kriechbaumer, T., and contributors. 2010. mitmproxy: A free and open source interactive HTTPS proxy. https://mitmproxy.org/.

[2] EasyList. 2023. EasyPrivacy.

[3] European Parliament and the Council of the European Union, The. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[4] Iyer, S. 2023. pywebostv 0.8.2.

[5] Kamran, H. 2023. Blocklists.

[6] Perflyst. 2018. PiHoleBlocklist.

[7] Pi-hole. 2023. StevenBlack/hosts.

[8] RootMyTV. 2023. RootMyTV 2.0.

[9] Urban, T., Tatang, D., Holz, T., and Pohlmann, N. 2018. Towards Understanding Privacy Implications of Adware and Potentially Unwanted Programs. In esorics. ESORICS, 449–469. DOI=10.1007/978-3-319-99073-6_22.

CHRISTIAN BÖTTGER
Doktorand im Themenschwerpunkt „Privatsphäre im Internet" im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen.

NURULLAH DEMIR
Post-Doc mit dem Schwerpunkt „Web-Analyse und -Auswertung" im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen.

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

TOBIAS URBAN
ist Professor für Cyber-Sicherheit mit dem Forschungsschwerpunkt „Schutz von Online-Anwendungen und Verbesserung der Privatsphäre im Internet" im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen.

VORSCHAU Ausgabe 5|24 OKTOBER/ NOVEMBER

IT-SA, NÜRNBERG, 22. BIS 24. OKTOBER 2024

Nürnberg, die Hochburg der Cybersicherheit: Die it-sa Expo&Congress ist der Pflichttermin für alle Experten, die ihr Unternehmen gegen die Bedrohungen der digitalen Welt rüsten wollen. Hier vereint sich die Crème de la Crème der IT-Sicherheitsbranche, um Lösungen für die drängendsten Herausforderungen unserer Zeit zu präsentieren: Cloud und Mobile Security, der Schutz von Daten und Netzwerken sowie die Abwehr von Angriffen auf kritische Infrastrukturen und die Industrie 4.0.

19.449 Fachbesucher aus 55 Ländern und 795 Aussteller aus 30 Nationen kamen 2023 zur Messe – das sind Zahlen, die für sich sprechen.

In unserem großen it-sa-Special in der nächsten Ausgabe erfahren Sie alles, was Sie für Ihren Messebesuch wissen müssen.

Weitere geplante Themen:

- Mit DevSecOps zu sicherer Software: Zusammenarbeit und Kommunikation bei der Softwareentwicklung
- Die TLS-Testsuite des KoTeBi-Projekts
- Stolperfallen und Streitpunkte zwischen Versicherer und Versicherungsnehmer bei der Schadenregulierung
- ...

IN UNSEREM VERLAG ERSCHEINEN AUßERDEM NOCH FOLGENDE ZEITSCHRIFTEN

IT-SICHERHEIT
Management und Technik

Verlag:
DATAKONTEXT GmbH
Standort Frechen
Augustinusstr. 11 A · 50226 Frechen
www.datakontext.com

Chefredaktion:
Sebastian Frank (S.F.)
E-Mail: s.frank@kes.de

Online-Redaktion:
Jessica Herz
Leitung Online
herz@datakontext.com
+49 2234 98949-80
Lisa Bieder
Konstantin Falke
Silvia Klüglich
Janek Mazac
Philip Meyer
Chiara Schönbrunn

Content von The Hacker News (THN)

Grafik/Layout/Satz:
Michael Paffenholz
Tel.: +49 173 8382572
E-Mail: michael.paffenholz@gmx.de

Objekt- und Anzeigenleitung:
Wolfgang Scharf
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 30

Vertrieb/Herstellung:
Dieter Schulz
Tel.: +49 2234 98949-99
dieter.schulz@datakontext.com

Abonnement:
Jahresabonnement € 139,- inkl. VK (Inland)

Erscheinungsweise: sechs Ausgaben
Alle Preise verstehen sich inkl. MwSt. Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Erscheinungsweise, Bezugspreise und -bedingungen:
Abonnement und Bezugspreis beinhalten die Print-Ausgabe sowie eine Lizenz für das Online-Archiv. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Der Preisanteil des Online-Archivs ist auf der Abonnementrechnung separat ausgewiesen.

Aboservice:
Hüthig Jehle Rehm GmbH, München,
Tel.: +49 89 21 83-7110

Druck: Grafisches Centrum Cuno GmbH & Co. KG, Calbe (Saale)

Genderhinweis: Gleichberechtigung ist uns wichtig! Für eine bessere Lesbarkeit unserer Fachtexte verzichten wir jedoch auf die gendergerechte Schreibweise und nutzen das generische Maskulinum als neutrale grammatikalische Form. Personenbezeichnungen beziehen sich auf alle Geschlechter.

Beilagen: DATAKONTEXT GmbH, Frechen

Titelbild: Vitor Miranda - stock.adobe.com

Fotos: Firmenbilder; DATAKONTEXT; DALL·E; (2rogan, ALL YOU NEED studio, andrew_shots, Andrii, Ar_TH, B Studio, DenPhoto, drawlab19, Dzianis Vasilyeu, DzRareStock, growth.ai, H. Brauer, Hengki, Kampan, klyaksun, Mister G.C., orbcat, Robert Daly/KOTO, tippapatt, VRVIRUS, Who is Danny) - stock.adobe.com

30. Jahrgang 2024 · ISSN: 1868-5757

© Gorodenkoff - stock.adobe.com

Verantwortliche für IT-Sicherheit direkt erreichen

- Newsletter
- Content-Marketing
- Webinare & Webkonferenzen

Schreiben Sie uns: **wolfgang.scharf@datakontext.com**

www.itsicherheit-online.com | www.kes-informationssicherheit.de


itsa EXPO CONGRESS
PLAY HARD.
PROTECT SMART.
HOME OF IT SECURITY
JETZT GRATIS-TICKET SICHERN!
22. – 24. Oktober 2024
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE