HZ219244 · ISSN 1868-5757 · www.itsicherheit-online.com August/September 4/2025

IT-SICHERHEIT

Management und Technik

Schwerpunkt Malware

Cyberresilienz gegen Ransomware

Wie Unternehmen Schäden und Ausfallzeiten minimieren

- **Zu klein für ein Ziel?**
  Ransomware trifft den Mittelstand mit voller Wucht
- **Backup neu gedacht**
  Die letzte Bastion gegen den Totalausfall
- **Lieferkette im Visier**
  Wie Ransomware über Drittanbieter zuschlägt
- **Android-Malware boomt**
  Neue Tricks mit Virtualisierung, NFC und Overlay-Angriffen

CISO-Weiterbildung
Welche Skills jetzt zählen

Krankenhäuser ohne Schutz
Warum viele Kliniken keine Cyberversicherung bekommen

EU Cyber Resilience Act
Neue Pflichten für Open Source

DATAKONTEXT


itsa
HOME OF
IT SECURITY
Jetzt mehr erfahren!
7. – 9. Oktober 2025
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE

Liebe Leserinnen, liebe Leser,

Ransomware – man möchte das Wort schon fast nicht mehr hören. Aber es nützt ja nichts: Die Angreifer schlafen nicht – sie organisieren und professionalisieren sich immer weiter. Früher waren es einzelne Virenautoren mit zweifelhafter Berühmtheit; seit Mitte der 2000er haben sich daraus arbeitsteilig organisierte Ransomware-as-a-Service-(RaaS)-Ökosysteme mit Support-Hotline, Franchise-Logistik und betriebswirtschaftlicher Effizienz entwickelt.

Unser Schwerpunkt „Malware | Ransomware" in dieser Ausgabe beleuchtet die ganze Bandbreite dieser Gefahr. Der Mittelstand steht dabei besonders im Fokus, denn Ransomware ist längst kein Spezialproblem von Konzernen mehr, sondern ein systemisches Risiko. In vielen kleinen und mittleren Unternehmen reichen Basisschutz und gelegentliche IT-Wartung nicht mehr aus. Gerade hier droht die Diskrepanz zwischen Bedrohungslage und Sicherheitsniveau zum existenzbedrohenden Faktor zu werden (Seite 16).

Ein anderer Artikel nimmt Android-Malware unter die Lupe – mit Virtualisierung, Overlays und NFC-Betrug (Seite 12). Während die öffentliche Vorstellung von Ransomware-Angriffen oft beim E-Mail-Anhang mit verseuchter Datei endet, zeigen Analysen von dateilosen Angriffen und Supply-Chain-Kompromittierungen ein anderes Bild: Es geht längst um tief integrierte, schwer erkennbare Mechanismen – oft ohne klassische Malware (Seite 18). Besonders perfide: Angreifer zielen systematisch auf Backup-Repositories, um auch die letzte Verteidigungslinie zu kompromittieren (Seite 15).

Doch nicht nur Technik ist gefragt. Die forensische Rekonstruktion eines Angriffs macht deutlich: Entscheidend ist nicht nur, ob eine Attacke erfolgt, sondern wie schnell und koordiniert Unternehmen reagieren. Notfallhandbücher, psychologische Resilienz und Kommunikationsprozesse sind ebenso wichtig wie technische Schutzmaßnahmen (Seite 8).

Ein etwas ungewöhnlicher, aber umso spannenderer Blick auf das Thema Resilienz kommt aus dem Qualitätsmanagement: Im Beitrag ab Seite 42 zeigen die Autoren, wie sich Strukturen der ISO 9001 nutzen lassen, um Risiken frühzeitig zu erkennen, Führungsverantwortung zu verankern und Prozesse widerstandsfähiger zu gestalten. Ihre These: Qualität ist nicht nur ein Audit-Thema, sondern eine Voraussetzung für wirksame und steuerbare Sicherheitsarchitektur. Gerade in Zeiten wachsender regulatorischer Anforderungen könnte das der Missing Link zwischen Governance und operativer Abwehr sein.

Genau hier setzt auch unser Beitrag zur CISO-Weiterbildung an (Seite 22). Zwischen Cloud-Diensten, NIS-2 und KI-Revolution brauchen Sicherheitsverantwortliche mehr als Tool-Wissen: Sie müssen kommunizieren, vernetzen, priorisieren. Denn: IT-Sicherheit ist längst keine technische Aufgabe mehr, sondern eine Führungsdisziplin.

Vielleicht ist das auch die stille Hoffnung, die sich durch diese Ausgabe zieht: Die Angriffe sind oft nicht zu verhindern. Aber ihr Erfolg ist es. Je mehr Unternehmen erkennen, dass Cyberresilienz nicht nur ein technisches Update, sondern ein kultureller Wandel ist, desto seltener erreichen Kriminelle und andere Akteure das, was sie am meisten wollen: Kontrolle und Geld.

Viel Spaß bei der Lektüre wünscht Ihnen
Sebastian Frank

www.itsicherheit-online.com/newsletter

INHALT

8 CYBERRESILIENZ GEGEN RANSOMWARE
WIE UNTERNEHMEN SCHÄDEN UND AUSFALLZEITEN MINIMIEREN

LEVELBLUE WIRD GRÖßTER REINER MSSP

LevelBlue, Anbieter von cloudbasierten, KI-gestützten Managed Security Services, übernimmt Trustwave, einen globalen Anbieter von Cybersicherheits- und Managed-Detection-and-Response-(MDR)-Dienstleistungen. Durch die Übernahme entsteht der weltgrößte reine Managed Security Service Provider (MSSP).

„Die Übernahme von Trustwave ist ein entscheidender Moment für LevelBlue und die Cybersicherheitsbranche", erklärt Robert McCullen, Vorsitzender und CEO von LevelBlue. Das Unternehmen stärkt damit seine globalen Markteinführungskapazitäten und seine Position auf den Märkten der US-Behörden. Trustwave, mit Sitz in Chicago, beschäftigt mehr als 1.000 Sicherheitsexperten und ist für seine Bedrohungsforschung und Threat Intelligence bekannt. ■

KI-AGENTEN FÜR NETZWERKE

Extreme Networks hat seine neue Plattform „Extreme Platform ONE" allgemein verfügbar gemacht. Die Lösung integriert dialogorientierte, multimodale und agentenbasierte künstliche Intelligenz (KI) vollständig in Netzwerke. Laut Hersteller können Unternehmen damit den manuellen Aufwand um bis zu 90 Prozent senken und die Zeit zur Problemlösung um bis zu 98 Prozent verkürzen.

Die Plattform bietet Echtzeit-Einblicke in die Netzwerktopologie und ermöglicht automatisierte Anpassungen an Bandbreitenspitzen und Sicherheitsbedrohungen. Administratoren definieren dabei Leitplanken für Richtlinien und Risiken, während KI-Agenten autonom zur Optimierung agieren. Andrew Smith vom West Suffolk NHS Foundation Trust berichtet, dass seine Organisation in nur 47 Minuten auf die neue Plattform migrieren konnte. „Die KI-Agenten erkennen Unregelmäßigkeiten direkt – schneller und zuverlässiger als es manuell möglich wäre", so Smith. Die Plattform konsolidiert zudem Lizenz-, Vertrags- und Asset-Management in einem Dashboard und bietet Echtzeit-Transparenz über Nutzung und Support-Abdeckung. ■

AUTOMATISIERTE CYBERSICHERHEIT FÜR FAHRZEUGE

Die asvin GmbH präsentierte auf dem Transformationsgipfel Cars 2.0 am 17. Juli in Stuttgart Lösungen zur Automatisierung von Cybersicherheitsprozessen für die Automobilindustrie. Mit zunehmender Vernetzung und KI-Einsatz in Fahrzeugen wächst die Angriffsfläche für Cyberangriffe. In Partnerschaft mit Dekra digitalisiert asvin die cybersicherheitsrelevanten Zulassungsverfahren beim Kraftfahrtbundesamt. „Damit wird die Typenprüfung von komplexen Systemen nicht nur sicherer, sondern auch effizienter", erklärt Gerhard Steininger, VP Sales bei asvin. Im Forschungsverbund „KI Fogger" mit TRUMPF Deutschland entwickelt das Unternehmen zudem Verfahren zum Schutz von Unternehmens-Know-how in KI-Trainingsdaten. Durch steganografische Methoden werden sinnvolle mit unsinnigen Daten vermischt, die nur mit dem passenden kryptografischen Schlüssel unterscheidbar sind. ■

BITDEFENDER ÜBERNIMMT **MESH SECURITY**

Bitdefender hat eine Vereinbarung zur Übernahme von Mesh Security Limited getroffen. Das Unternehmen integriert damit die E-Mail-Sicherheitstechnologie von Mesh in seine Extended-Detection-and-Response-(XDR)-Plattform und Managed-Detection-and-Response-(MDR)-Dienste.

Mesh verfolgt einen zweistufigen Ansatz für E-Mail-Sicherheit: perimetrischer Schutz über ein Secure E-Mail Gateway kombiniert mit Verteidigung auf Mailbox-Ebene durch API-basierte Bereitstellung. Die Lösung bietet eine für Managed Service Provider optimierte Multi-Tenant-Plattform mit automatisierter Richtliniendurchsetzung und Echtzeit-Einblicken.

Das 2020 gegründete Unternehmen Mesh wird von Elkstone und Enterprise Ireland unterstützt und hat sich als E-Mail-Sicherheitsanbieter für Hunderte von MSP-Partnern etabliert. Die Transaktion unterliegt den üblichen Abschlussbedingungen. Die finanziellen Details wurden nicht veröffentlicht. ■

AUTONOME SICHERHEITSAGENTEN

Cycode hat in seiner KI-gestützten Anwendungssicherheitsplattform ein neues agentenbasiertes Framework namens „AI Teammates" eingeführt. Die KI-Agenten sollen komplexe Cyberangriffe auf die Software-Supply-Chain abwehren. Die autonomen Systeme analysieren detaillierte Daten über Prozesse, Code und sicherheitsrelevante Vorgänge. Durch Graph-Intelligence-Fähigkeiten können die Agenten komplexe Zusammenhänge zwischen Datenpunkten erkennen.

Derzeit stehen vier spezialisierte KI-Agenten zur Verfügung: Der „Risk Intelligence Graph"-Agent greift auf Informationen über Code-Repositories zu, der „Change Impact Analysis"-Agent überwacht Code-Änderungen, der Exploitability-Agent unterscheidet zwischen theoretischen und tatsächlich ausnutzbaren Schwachstellen, und der „Fix & Remediation"-Agent schlägt kontextbezogene Code-Korrekturen vor. Die Basis bildet das „Model Context Protocol", das laut Cycode als Betriebssystem für die KI-Agenten fungiert und ihnen Zugriff auf den organisatorischen Kontext ermöglicht. ■

IFS ÜBERNIMMT KI-SPEZIALIST **THELOOPS**

IFS, Anbieter von Cloud-Enterprise-Software, hat das Unternehmen TheLoops akquiriert und bringt damit eine spezialisierte KI-Agenten-Plattform für Industrieunternehmen auf den Markt. Die Integration der agentenbasierten Technologie von TheLoops in die IFS-Software soll den Wandel von nachverfolgender zu aktiv handelnder Business-Software einleiten.

Die neue Plattform bietet eine Multi-Agenten-Umgebung, deren KI-Komponenten nicht nur kombiniert und gesteuert, sondern auch semantisch über ihre Betriebsumgebung informiert werden können. Im Gegensatz zu herkömmlichen KI-Systemen, die auf Mustererkennung und Vorhersagen beschränkt sind, können die intelligenten Agenten kontinuierlich suchen, denken und selbstständig handeln.

„Mit den agentenbasierten Funktionen können Anwenderunternehmen intelligente digitale Teammitglieder einsetzen, die ihr Geschäft vom ersten Tag an verstehen", erklärt Mark Moffat, CEO von IFS. Somya Kapoor, CEO von TheLoops, ergänzt: „Es war schon immer unsere Mission, eine KI bereitzustellen, die nicht nur Erkenntnisse liefert, sondern Aufgaben voranbringt." ■

SOPHOS ERWEITERT RISIKOMANAGEMENT

Sophos hat sein Managed-Risk-Service-Angebot um Internal Attack Surface Management (IASM) erweitert. Der neue Dienst basiert auf der Technologie des Exposure-Management-Unternehmens Tenable, mit dem Sophos bereits Anfang 2024 eine Kooperation startete.

Laut dem Sophos State of Ransomware Report 2025 wurden 40 Prozent der von Ransomware betroffenen Organisationen Opfer aufgrund unbekannter Risiken. IASM führt internes Scanning ein, bei dem Systeme aus der Perspektive eines externen Angreifers ohne Benutzeranmeldedaten bewertet werden. So können Unternehmen risikoreiche Schwachstellen wie offene Ports, exponierte Dienste und Fehlkonfigurationen identifizieren.

Die Funktionen umfassen umfangreiches Schwachstellenmanagement durch regelmäßiges automatisches Scannen, KI-unterstützte Priorisierung der gefundenen Schwachstellen und Nutzung der Nessus-Scanner von Tenable zur Erkennung interner Netzwerkprobleme. ■

IDENTITÄTSDATEN-BACKUP FÜR MICROSOFT-UMGEBUNGEN

Barracuda Networks hat mit „Entra ID Backup Premium" eine Lösung zum Schutz von Microsoft Entra ID-Umgebungen vor Datenverlust eingeführt. Die in die BarracudaONE-Plattform integrierte Lösung sichert 13 wichtige Identitätskomponenten, darunter Nutzer-, Gruppen- und Rolleninformationen sowie Authentifizierungs- und Zugriffsrichtlinien.

Die cloudbasierte Software-as-a-Service-Lösung schließt eine kritische Sicherheitslücke, da Microsoft Entra ID-Daten standardmäßig nur 30 Tage lang speichert und Drittanbieter-Backups empfiehlt. Die Lösung unterstützt sowohl Einzel- als auch Multi-Tenant-Umgebungen und richtet sich an IT-Teams und Managed Service Provider. Kunden können ihren Microsoft-365-Mandanten verbinden und innerhalb weniger Minuten mit der Sicherung ihrer Entra ID-Daten beginnen. ■

TANIUM ERHÄLT ANSSI-CSPN-ZERTIFIZIERUNG

Das Unternehmen Tanium hat die Certification de Sécurité de Premier Niveau (CSPN) von Frankreichs nationaler Cybersicherheitsbehörde ANSSI erhalten. Die Zertifizierung in der Kategorie „Sicherheitsverwaltung und -überwachung" bestätigt, dass die Tanium On-Premises-Plattform die französischen Cybersicherheitsstandards erfüllt.

Nach einer umfassenden Prüfung durch einen akkreditierten externen Prüfer erhielt Tanium die ANSSI-CSPN-Zertifizierung (ANSSI-CSPN-2025/04), die für drei Jahre gültig ist. Besonders wertvoll ist die automatische Zulassung in Deutschland durch das CSPN-BSI-Abkommen. „Dank dieser Anerkennung durch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) erstreckt sich die Gültigkeit der Zertifizierung auf Deutschland, wodurch wir unsere Position als vertrauenswürdiger Technologiepartner in zwei Schlüsselmärkten Europas festigen", erklärt Zac Warren, Chief Security Advisor EMEA bei Tanium. ■

NINA-APP ERHÄLT POLIZEIWARNUNGEN

Die Warn-App NINA des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) wird mit einem umfangreichen Update erweitert. Ab sofort erhalten die über 12 Millionen Nutzer auch Warnmeldungen der Polizeibehörden von Bund und Ländern in einem eigenen Warnbereich mit spezifischem Icon. Dies verbessert die behördenübergreifende Warnung bei besonderen polizeilichen Lagen.

Ein neuer Bereich „Themen" bündelt die bekannten „Notfalltipps" des BBK mit den neuen „Polizeitipps" zur Kriminalprävention. Diese werden vom Programm Polizeiliche Kriminalprävention der Länder und des Bundes bereitgestellt.

Technische Optimierungen im Hintergrund reduzieren die Datenmengen für Push-Nachrichten, was die Zuverlässigkeit bei Massenbenachrichtigungen erhöht. Die Neuerungen wurden im Juli auf dem Bevölkerungsschutztag in Rostock vorgestellt. BBK-Präsident Ralph Tiesler betont: „Viele Anpassungen der letzten Jahre gingen auf das Feedback von Nutzerinnen und Nutzern zurück." Die kostenlose App steht in den gängigen App-Stores zur Verfügung. ■

ANDROID-SECURITY IM LANGZEITTEST

Vier Security-Apps für Android haben im sechsmonatigen Dauertest des AV-TEST-Labors mit maximaler Punktzahl abgeschnitten. Die Lösungen von Bitdefender, F-Secure, Kaspersky und Sophos erkannten alle über 18.000 getesteten Schad-Apps und verursachten dabei keine nennenswerte Systemlast auf den Geräten.

Der Test unter Android 12 prüfte, wie zuverlässig die Schutzlösungen gegen Bedrohungen wie die Vapor-Kampagne schützen, bei der Kriminelle über 300 Apps im Google Play Store platzierten, die erst nach der Installation Malware nachgeladen haben. Diese Apps wurden laut AV-TEST über 60 Millionen Mal heruntergeladen.

Fünf weitere getestete Lösungen erreichten mit 17,7 von 18 möglichen Punkten ebenfalls sehr gute Ergebnisse. Selbst der in Android integrierte Google Play Protect-Mechanismus erzielte mit 17 Punkten ein gutes Resultat, wenngleich mit etwas schwächerer Erkennungsrate von 99,4 bis 99,6 Prozent. Die Tester überprüften auch, ob die Sicherheits-Apps harmlose Anwendungen fälschlich als gefährlich einstufen. Hier zeigten besonders Bitdefender, F-Secure, Kaspersky und Sophos eine präzise Unterscheidung. ■

Cyberresilienz gegen Ransomware

WIE UNTERNEHMEN SCHÄDEN UND AUSFALL-ZEITEN MINIMIEREN

Ransomware-Angriffe treffen längst nicht nur unvorsichtige Firmen, sondern auch gut aufgestellte Organisationen mit modernen Abwehrsystemen. Doch nicht der Angriff selbst entscheidet über das Schicksal eines Unternehmens, sondern wie schnell es wieder handlungsfähig wird. Moderne Cyberresilienz-Systeme helfen, Daten schneller wiederherzustellen und Angriffe dank künstlicher Intelligenz (KI) früher zu erkennen.

Endlich kam die E-Mail mit der erwarteten Rechnung an. Der Anhang war per Link auf dem Server der Lieferantenfirma hinterlegt. Die E-Mail passte zum Vorgang, zudem enthielt die Betreffzeile den Vermerk der internen Security-Lösung, dass sie ungefährlich sei. Der Link zum Download der Rechnung – in einem neuen Dokumentenablagesystem anstelle eines PDF-Anhangs – zerstreute auch die letzten Zweifel, ob die E-Mail echt ist.

Da der Jahresabschluss bevorstand und die Leistung noch auf das Vorjahr gebucht werden sollte, klickte der Empfänger in der Hektik auf den Link, öffnete die PDF-Datei, prüfte sie kurz und legte sie anschließend im Projekt-Share ab. Diese kleine Nachlässigkeit öffnete den Angreifern die Tür ins Unternehmensnetzwerk, erfuhr der IT-Leiter von den Forensikern des Landeskriminalamtes – drei Monate nach den für ihn schlimmsten Wochen in zwanzig Jahren Unternehmenszugehörigkeit.

TIME BOMBING UND LIVING OFF THE LAND

Die Attacke basierte auf dem „Time Bombing"-Verfahren, bei dem der Schadcode erst zu einem bestimmten Zeitpunkt aktiviert wird. So konnte die manipulierte PDF-Datei unerkannt das Security-Gateway passieren und selbst einen erfahrenen IT-Fachmann täuschen. Für die Angreifer war der IT-Leiter mit seinen umfangreichen Domänen-Adminrechten ein ideales Opfer. Sie nutzten den Zugriff vorerst nur zur Beobachtung und Ausbreitung auf weitere Systeme.

Die forensische Analyse zeigte später: Die Hacker beobachteten zwei Monate lang die Systemarchitektur, die Geschäftsprozesse und potenzielle Angriffsziele im Unternehmen. Anschließend verwendeten sie die „Living off the Land"-Methode. Diese Cyberangriffstechnik nutzt legitime Tools und Funktionen des Zielsystems, um unentdeckt Schaden anzurichten oder sich weiter im Netzwerk auszubreiten, während kaum oder gar keine zusätzliche Schadsoftware eingesetzt wird.

Nach dieser intensiven Vorbereitung starteten die Angreifer schließlich ihre Attacke an einem langen Wochenende. Sie verschlüsselten alle Daten und ersetzten die Unternehmenswebsite durch eine vorgefertigte Lösegeldforderung. Somit wurde der Angriff öffentlich und Lösegeld über zwei Millionen Euro gefordert.

BETROFFEN TROTZ SCHUTZ

Der Fall verdeutlicht: Jedes Unternehmen kann betroffen sein – unabhängig von seinen Sicherheitsvorkehrungen. Es gibt keinen Grund, sich zu schämen, wenn man Opfer einer Cyberattacke wird, denn trotz jahrelanger Investitionen in Cybersicherheit, Awareness-Schulungen und Penetrationstests steigt die Anzahl erfolgreicher Angriffe weiter an. Die Dunkelziffer liegt vermutlich noch deutlich höher.

Die gute Nachricht ist, dass Cyberangriffe heute früher erkannt und die Schäden besser eingedämmt werden können, sodass weniger Daten oder Umsätze verloren gehen. Der Reputationsverlust bleibt jedoch bestehen.

Cybersicherheit ist zugleich ein stetiger Kostentreiber: „There is no glory in prevention" lautet ein bekanntes Bonmot der Branche. Denn wirkungsvolle Sicherheitsmaßnahmen verhindern zwar Angriffe, bringen jedoch oft spürbare Einschränkungen im Alltag mit sich – von komplexen Anmeldeprozessen über eingeschränkte Zugriffsrechte bis hin zu umfassenden Dokumentationspflichten. Hinzu kommt ein psychologischer Effekt: Je erfolgreicher die Prävention wirkt, desto weniger sichtbar wird ihr Nutzen – und desto eher zweifeln manche an ihrem Wert.

Durch NIS-2 oder DORA regulierte Unternehmen unterliegen zudem umfassenden Meldepflichten, welche bei Versäumnissen zu empfindlichen Strafen führen können. Und trotz aller Maßnahmen kann schon eine einzige Schwachstelle in der sorgfältig aufgebauten Verteidigung das gesamte Unternehmensnetzwerk kompromittieren.

FALLSTRICKE EINER ERFOLGREICHEN WIEDERHERSTELLUNG UND DER FAKTOR ZEIT

Im beschriebenen Fall entschied das Unternehmen, nicht auf die Lösegeldforderung einzugehen, da Notfallpläne und regelmäßige Datensicherungen vorhanden waren. Man meldete den Vorfall bei der Polizei und bei der Cyberversicherung. Überdies wurde ein externer Security-Dienstleister zur Unterstützung herangezogen. Am Samstagmorgen war man optimistisch, die verschlüsselten Daten über das Wochenende wiederherstellen zu können. Hierzu mussten der Backup-Server neu aufgebaut und die Bänder eingelesen werden.

Doch am Sonntag folgte die Ernüchterung: Viele kleine Dateien auf den Dateiservern verlangsamten die Wiederherstellung auf etwa 250 Gigabyte pro Stunde. Die Geschäftsführer mussten die Produktionsschichten bis einschließlich Mittwoch absagen.

Um das Risiko einer Reinfektion zu minimieren, beschaffte das Unternehmen neue Netzwerk-Infrastruktur, Server und Speichersysteme. Alle Bestandssysteme wurden abgeschaltet. Zusätzlich überprüfte man alle wiederhergestellten Daten und Systeme mit mehreren Virenscannern. Das Sicherheitsteam hatte mittlerweile für den Angriff eine YARA-Regel erstellt – ein spezifisches Suchmuster, mit dem Dateien gezielt auf charakteristische Merkmale der eingesetzten Schadsoftware geprüft werden können – die anschließend auf allen wiederhergestellten Systemen in einer Green Zone angewendet wurde.

Auf Basis der neu eingerichteten Infrastruktur gelang es, bis zum Ende der Woche einen Notbetrieb herzustellen. Die Wiederherstellung von Daten in der Cloud stellte jedoch eine zusätzliche Herausforderung dar, da die Snapshot-Backups in Azure aus dem kompromittierten Tenant nicht verwendet werden konnten. Stattdessen mussten die Verantwortlichen virtuelle Maschinen und Daten aus dem Backup-System zurückspielen, während Web-Services und serverlose Anwendungen mithilfe bestehender Automatisierungen neu eingerichtet wurden. Nach weiteren zwei Wochen konnte die Firma schließlich den regulären Betrieb wieder aufnehmen.

ÜBER DIE PRÄVENTION HINAUSDENKEN

Im Anschluss begann die Ursachenanalyse und die Bewertung des entstandenen Schadens:

- Der Schaden durch ausgefallene Produktionszeiten, Neuanschaffungen, Überstunden und externe Unterstützung belief sich auf insgesamt zehn Millionen Euro. Die ausgenutzte Lücke wurde durch eine neue Version der Mail-Security-Software geschlossen.
- Die Notfallhandbücher waren erst vor drei Monaten auditiert worden. Hier griffen alle Prozeduren.
- Das Backup-System ermöglichte grundsätzlich eine Wiederherstellung, offenbarte jedoch erhebliche Schwächen bei der Performance, da die primären Sicherungskopien ebenfalls verschlüsselt waren.

Als Konsequenz startete das Unternehmen ein Resilienz-Projekt. Denn während klassische Cy-

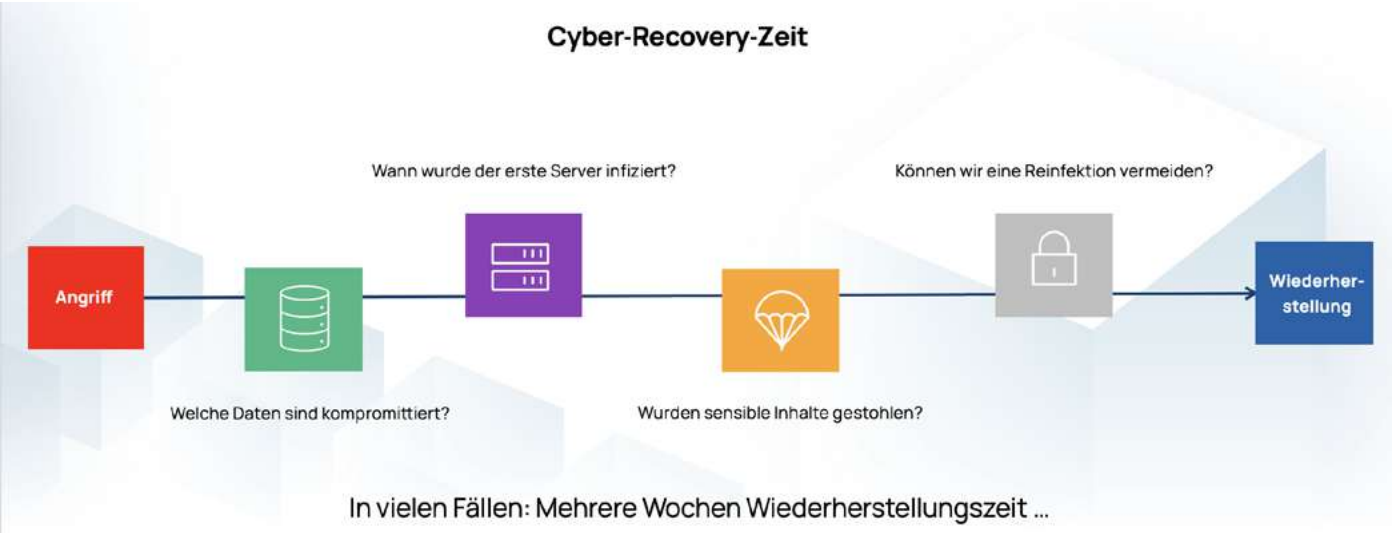


Abbildung 1: Die Wiederherstellung nach einem Cyberangriff dauert oft mehrere Wochen und erfordert eine systematische Analyse der Kompromittierung, vom initialen Angriff bis zur vollständigen Wiederherstellung unter Berücksichtigung von Reinfektionsrisiken. (Bild: Empalis)

Abbildung 2: Cyberresilienz entsteht durch die Kombination präventiver Sicherheitsmaßnahmen mit effektiven Wiederherstellungsprozessen, was Unternehmen robuster gegen digitale Bedrohungen macht. (Bild: Empalis)

bersicherheit darauf abzielt, Angriffe zu verhindern, geht Cyberresilienz davon aus, dass auch die beste Verteidigung irgendwann überwunden werden kann.

Der Wechsel vom Backup- zum Cyberresilienz-System verlagert den Fokus von der Effizienz im Normalbetrieb und Kosteneffektivität hin zu Wiederherstellungsfunktionen. Diese Systeme unterstützen aktiv die Angriffsabwehr eines Unternehmens durch:

- Analyse der Datenströme nach Bedrohungen bereits beim Speichern
- Indizierung der Backup-Inhalte
- leistungsstarke Massenwiederherstellung
- Anomalieerkennung und Datenklassifizierung
- Anbindung über Programmierschnittstellen (API) an andere Cybersicherheitssysteme

Mit indizierten Backup-Daten, skalierbaren Cluster-Architekturen und Cloud-Anbindung zur Orchestrierung und Analyse der Backups bieten diese Systeme einen neuen, ungenutzten Data Lake, der nicht nur den Istzustand, sondern auch eine Historie zu den Daten ermöglicht. Ein Data Lake ist ein zentrales Repository, das große Mengen strukturierter, semistrukturierter und unstrukturierter Daten in ihrem Rohformat speichert und damit flexible Analysen erlaubt. Die Verschlagwortung und Anreicherung dieser Daten mit Metadaten bildet die Grundlage für den größten zentralen Datenbestand eines Unternehmens.

DER WERT DER DATEN UND WERTSCHÖPFUNG DURCH KI

Heutzutage sind solche Daten mehr denn je eine wertvolle Währung – auch die künstliche Intelligenz dürstet nach Trainingsdaten. Damit rücken Backup-Lösungen in eine neue, strategisch wichtige Rolle.

Mithilfe von KI können künftig nicht nur Bedrohungen besser erkannt und gezieltere Aussagen über die zu erwartende Wiederherstellungszeit (Recovery Time Objective, RTO) und den möglichen Datenverlust (Recovery Point Objective, RPO) gemacht werden – abhängig vom Alter der Daten aus dem verfügbaren aktuellsten Wiederherstellungspunkt. Es eröffnen sich zudem komplett neue Anwendungsmöglichkeiten: In naher Zukunft können wir Fragen an das Cyberresilienz-System stellen wie „Wie viele E-Mails wurden an externe Benutzer geschickt, die einen PDF-Anhang enthielten, der Rechnungen enthielt?“ oder „Welche Benutzer haben im letzten Monat mehr als 100 GB neue Daten erzeugt – über alle Quellen hinweg?“.

Damit entwickeln sich Cyberresilienz-Systeme zu allwissenden Systemen, die sowohl aus dem aktuellen Bestand als auch aus der Vergangenheit heraus antworten können. All diese Technologien stärken die Angriffsabwehr, verbessern die Früherkennung und unterstützen fundierte Entscheidungen im Fall eines Cyber Incidents. Zwar verhindert Cyberresilienz keinen Angriff, sie trägt jedoch entscheidend dazu bei, Schäden wirksam zu begrenzen – und bildet damit die Basis für eine möglichst schnelle und erfolgreiche Wiederherstellung. ■

HERAUSFORDERUNGEN BEI DER WIEDERHERSTELLUNG

Nach einem Cybervorfall ist die Wiederherstellung oft komplizierter und zeitaufwendiger als erwartet. Typische Stolpersteine sind:

- ***Zugriff auf Daten:*** *Die Sicherungsdaten müssen verfügbar und erreichbar sein.*
- ***Kompromittierte Backups:*** *Wurden auch Backup-Systeme infiziert, bleiben oft nur entfernte Sicherungsmedien, die erst katalogisiert und eingelesen werden müssen.*
- ***Datenmengen:*** *Im Unterschied zu alltäglichen Wiederherstellungen werden oft riesige Datenmengen gleichzeitig benötigt, was die Systeme stark belastet.*
- ***Limitierte Performance:*** *Viele Backup-Architekturen sind nur für inkrementelle Sicherungen im Tagesbetrieb ausgelegt und schaffen die hohe Last einer umfassenden Recovery nicht.*
- ***Fehlerfreie Restore-Punkte:*** *Der letzte „saubere“ Wiederherstellungspunkt muss gefunden werden, um keine kompromittierten Daten einzuspielen.*
- ***Gefahr erneuter Infektion:*** *Der Schadcode darf nicht unbemerkt mit wiederhergestellt werden. Alle Daten müssen gründlich geprüft werden.*
- ***Prüfung der Daten:*** *Wiederhergestellte Systeme und Dateien müssen umfassend kontrolliert werden, bevor sie erneut produktiv genutzt werden dürfen.*

MARKUS STUMPF
hat den Bereich Data Protection Services der Empalis Consulting aufgebaut und ist heute Business Development Manager der Empalis.

Ceylon Frames - stock.adobe.com

Gefragt: Neue Qualifikationen für KI-gestützte IT-Sicherheit

Der deutsche **Markt für IT, Telekommunikation und Unterhaltungselektronik (ITK-Markt) wächst 2025 um 4,4 Prozent** auf 235,8 Milliarden Euro. Besonders dynamisch zeigt sich der Softwarebereich mit einem Plus von 9,5 Prozent auf 52,7 Milliarden Euro, angetrieben durch Cloud-Technologien und künstliche Intelligenz (KI). Das Geschäft mit KI-Plattformen legt sogar um 50 Prozent auf 2,3 Milliarden Euro zu. Parallel dazu entstehen rund **9.000 neue Arbeitsplätze** in der Digitalwirtschaft – **so das Ergebnis einer aktuellen Bitkom-Studie.**

KI als Chance und Risiko zugleich

KI eröffnet der IT-Sicherheit neue Möglichkeiten: Sie kann Muster in Datenmengen in Echtzeit analysieren, potenzielle Angriffe frühzeitig erkennen und Abwehrmaßnahmen automatisiert einleiten. Gleichzeitig vergrößert sie aber auch die Angriffsfläche. Selbstlernende Systeme können fehlerhafte Entscheidungen treffen oder von außen manipuliert werden, neue Angriffstechniken entstehen, die klassische Schutzmechanismen an ihre Grenzen bringen.

Technologisches Verständnis allein reicht nicht mehr aus

Die zunehmende Komplexität macht deutlich: Technisches Grundwissen allein ist nicht mehr ausreichend. Gefragt ist die Fähigkeit, **KI-Modelle ganzheitlich zu verstehen, zu bewerten und kontinuierlich zu überwachen.** Beschäftigte müssen algorithmische Risiken einschätzen können und wissen, wie sich Datenflüsse, Modellentscheidungen und Sicherheitsarchitekturen gegenseitig beeinflussen.

Neben tiefem technologischen Know-how werden **analytische Fähigkeiten** immer wichtiger. Sicherheitsverantwortliche müssen in der Lage sein, große Datenmengen effizient zu bewerten, ungewöhnliche Muster zu erkennen und daraus Handlungsempfehlungen abzuleiten.

Regulatorische Anforderungen und ethisches Bewusstsein rücken in den Fokus

Mit Vorgaben wie dem AI Act und der DSGVO gewinnen rechtliche und ethische Aspekte stark an Bedeutung. Sicherheitsverantwortliche sollten nicht nur über technisches Fachwissen verfügen, sondern auch regulatorische Anforderungen sicher anwenden können. Ebenso wichtig ist es, Sicherheitsstrategien klar zu vermitteln und das Vertrauen von Mitarbeitenden, Kunden und Partnern zu stärken.

Darüber hinaus ist **Kommunikationsfähigkeit** entscheidend: Sicherheitsstrategien und Maßnahmen müssen transparent vermittelt werden, um das Vertrauen von Mitarbeitenden, Kunden und Partnern aufzubauen.

Spezielle Weiterbildungsmaßnahmen

Unternehmen, die diese vielseitigen Fähigkeiten in ihren Teams systematisch aufbauen, können neue Bedrohungen frühzeitig erkennen, regulatorische Risiken reduzieren und gleichzeitig die Innovationskraft ihrer KI-Anwendungen stärken.

Seminare der Bitkom Akademie wie „KI-Compliance-Beauftragter", „Cybersecurity 2.0: KI in der IT-Sicherheit" oder „Cybersecurity Awareness Expert" helfen dabei, technisches Wissen mit regulatorischem und ethischem Verständnis zu verknüpfen – und so die Grundlage für eine zukunftsfähige Sicherheitsstrategie zu schaffen. ■

Haben Sie Fragen zu unseren Seminaren und Inhouse-Angeboten im Bereich IT-Sicherheit? Dann kontaktieren Sie **Nicole Stoitschew: n.stoitschew@bitkom-service.de**

Mehr dazu hier

bitkom-akademie.de/seminare

bitkom akademie

Struktur und Arbeitsweise moderner Android-Malware

WIE OVERLAYS, VIRTUALISIERUNG UND NFC-BETRUG MOBILES ARBEITEN BEDROHEN

Immer mehr neue Techniken machen Smartphones zur lukrativen Zielscheibe von Cyberkriminellen. Die Schadprogramme AntiDot, GodFather und SuperCard X demonstrieren, wie organisierte Angreifer systematisch Daten stehlen, Geräte kontrollieren und Finanzbetrug durchführen.

Android-Malware wird immer raffinierter – statt einfacher Phishing-Apps setzen Cyberkriminelle inzwischen auf hoch entwickelte Techniken wie Virtualisierung, Fernsteuerung und gezielte App-Manipulation. Aktuelle Schadprogramme zeigen eindrucksvoll, wie professionell organisierte Angreifer bereits vorgehen, um Daten zu stehlen, Geräte zu kontrollieren und Finanzbetrug in Echtzeit durchzuführen. Die Bedrohung geht dabei längst über klassische Methoden hinaus – und stellt Sicherheitslösungen vor neue Herausforderungen.

1. ANTIDOT: SPIONAGE-KAMPAGNE MIT MALWARE-AS-A-SERVICE

Die Android-Malware AntiDot wird vom Bedrohungsakteur LARVA-398 entwickelt und auf Untergrundmärkten als Malware-as-a-Service (MaaS) angeboten. Laut den Schweizer Sicherheitsanalysten von PRODAFT kommt AntiDot bereits in mindestens 273 Kampagnen mit über 3.775 infizierten Geräten weltweit zum Einsatz.

Die Malware wird in einschlägigen Foren als „Drei-in-eins-Lösung“ beworben und nutzt gezielt Androids Barrierefreiheitsdienste, um

Bildschirmaktivitäten aufzuzeichnen, SMS-Nachrichten abzufangen und sensible Daten aus Drittanbieter-Apps zu extrahieren.

AntiDot verbreitet sich nach aktuellen Erkenntnissen vor allem über infizierte Werbenetzwerke oder über maßgeschneiderte Phishing-Kampagnen aus, die auf die Sprache und den Standort der Opfer abgestimmt sind. Erste Hinweise auf die Malware tauchten im Mai 2024 auf, als sie sich als vermeintliche Google-Play-Updates tarnte. Die Maskierung als System- oder App-Update gilt offenbar als bevorzugte Methode der Täuschung. Wer darauf hereinfällt, wird gezielt über Social Engineering dazu gebracht, Sonderberechtigungen zu erteilen. In einem dreistufigen Installationsprozess entpackt die Malware ihre Funktionalität – verschlüsselt, fragmentiert und erst zur Laufzeit aktiviert –, um statische Analysen und Signatur-Scans zu umgehen.

Aus technischer Sicht handelt es sich bei AntiDot um eine auf Java basierende Malware, die stark verschleiert arbeitet. Die drei Schritte, mit denen sich die Schadsoftware auf einem Android-Smartphone installiert, sind:

1. Start über eine APK-Datei (Android Package Kit, das Installationspaket für Android-Anwendungen),
2. Packen durch einen kommerziellen Packer, der zur Laufzeit Schadfunktionen nachlädt,
3. Entpacken eines DEX-Moduls, das die Botnet-Funktionalitäten bereitstellt.

Bei der Analyse der Datei AndroidManifest.xml fällt auf, dass zahlreiche Klassennamen im ursprünglichen APK-Paket nicht enthalten sind. Diese werden erst zur Laufzeit dynamisch nachgeladen, was eine effektive Methode darstellt, um Virenscanner zu umgehen.

ECHTZEITÜBERWACHUNG UND C2-INFRASTRUKTUR

Ein wesentliches Kennzeichen von AntiDot ist die Möglichkeit, kompromittierte Geräte aus der Ferne zu steuern. Die Malware nutzt die MediaProjection-API, um Bildschirminhalte auszulesen, und setzt WebSocket-Verbindungen für eine bidirektionale Echtzeitkommunikation mit der Command-and-Control-(C2)-Infrastruktur ein. Laut Experten wurden mindestens elf aktive C2-Server identifiziert, die alle derzeit bekannten 3.775 kompromittierten Geräte steuern. Das zugehörige Steuerpanel basiert auf dem JavaScript-Framework MeteorJS und bietet:

- **Bots:** Übersicht über alle infizierten Geräte
- **Injects:** Liste der Zielanwendungen für Overlay-Angriffe mit Vorlagen
- **Analytic:** Analyse der installierten Apps zur Identifikation neuer Ziele
- **Settings:** Konfiguration der Injects und anderer Parameter
- **Gates:** Verwaltung der Endpunkte, mit denen die Bots kommunizieren
- **Help:** Support-Funktionen für Betreiber

Nach der Installation blendet AntiDot ein gefälschtes Update-Fenster ein, das die Nutzer dazu bewegen soll, die Barrierefreiheitsrechte freizugeben. Sofort wenn diese Rechte erteilt sind, beginnt die Malware mit ihren Spionageaktivitäten.

Sobald AntiDot aktiv ist, überwacht die Malware kontinuierlich, welche Anwendungen geöffnet werden. Startet das Opfer beispielsweise eine Krypto-Wallet oder eine Zahlungs-App, legt sich eine täuschend echte Overlay-Oberfläche über die Originalansicht. Die Eingaben, etwa Zugangsdaten für Wallets, werden direkt an die Angreifer übermittelt. Weitere Angriffsvektoren umfassen das Abfangen von SMS-Nachrichten, das Abhören oder Umleiten von Anrufen, die Überwachung aktiver Bildschirminhalte und die Unterdrückung von Systembenachrichtigungen.

Diese Funktionen machen AntiDot zu einer besonders gefährlichen Schadsoftware: Sie eignet sich nicht nur für den Diebstahl sensibler Daten und betrügerische Aktivitäten, sondern ermöglicht auch die vollständige Fernsteuerung infizierter Geräte.

Im Dezember 2024 tauchte außerdem eine neue Variante der Malware auf. Unter dem Namen AppLite Banker verbreitete sich AntiDot über eine Phishing-Kampagne, die vorgeblich Stellenangebote enthielt. Die Angreifer täuschten Bewerbungen oder Jobanzeigen vor, um Nutzer dazu zu bewegen, die infizierte App eigenständig auf ihren Geräten zu installieren.

AntiDot ist nicht nur ein gewöhnlicher Android-Trojaner, sondern eine vollständig ausgebaute Malware-as-a-Service-(MaaS)-Plattform, die auf finanziellen Gewinn durch umfassende Kontrolle mobiler Geräte abzielt. Die Kombination aus Overlay-Techniken, WebView-Injects, Echtzeitkommunikation und Verschleierung macht diese Malware zu einer erheblichen Bedrohung für die Privatsphäre und die Sicherheit.

2. GODFATHER SETZT AUF VIRTUALISIERUNG FÜR BANKING-BETRUG

Neben AntiDot sorgt auch eine weitere Malware-Familie für zunehmende Besorgnis in der Android-Welt: GodFather. Wie Sicherheitsanalysten von Zimperium zLabs berichten, ist eine neue, technisch deutlich weiterentwickelte Variante des GodFather-Bankingtrojaners für Android aufgetaucht. Die Schadsoftware nutzt nun Virtualisierung direkt auf dem Gerät, um Banking- und Krypto-Apps zu kapern und in Echtzeit betrügerische Aktionen auszuführen.

Im Unterschied zu klassischen Android-Trojanern, die lediglich gefälschte Login-Fenster einblenden, installiert GodFather eine sogenannte Host-Anwendung, die ein vollständiges Virtualisierungs-Framework enthält. Diese Anwendung lädt gezielt Kopien legitimer Banking- oder Kryptowährungs-Apps herunter und führt sie in einer isolierten, kontrollierten Umgebung aus – für den Nutzer bleibt das unbemerkt. Sobald eine Ziel-App gestartet wird, leitet GodFather den Aufruf in die manipulierte virtuelle Instanz um. Dort kann das Nutzerverhalten vollständig überwacht und in Echtzeit manipuliert werden, beispielsweise um Anmeldedaten oder Transaktionen abzugreifen.

Die aktuelle Version von GodFather bringt außerdem neue Funktionen mit, um statische Analysen gezielt zu umgehen. Dazu zählen unter anderem

- die Manipulation von ZIP-Dateien innerhalb der App sowie
- das Befüllen des AndroidManifest-Files mit irrelevanten Berechtigungen, um forensische Analysen zu erschweren.

Wie bereits bei AntiDot setzt auch GodFather auf die Barrierefreiheitsdienste von Android, um Informationen vom Gerät abzugreifen und

Nutzerinteraktionen zu kontrollieren. Zwar hat Google mit Android 13 neue Schutzmechanismen eingeführt, die verhindern sollen, dass manuell installierte Anwendungen auf diese Dienste zugreifen können, doch umgeht die Malware dies durch eine sogenannte sitzungsbasierte Installation – ein Verfahren, das auch von App-Stores und Browsern zur Installation von APK-Dateien genutzt wird.

VIRTUALISIERUNGS-TECHNIK IM DETAIL

Im ersten Schritt prüft die Malware, welche Apps auf dem Gerät installiert sind, und gleicht diese mit einer internen Zielliste ab. Erkennt GodFather eine Anwendung, für die bereits Vorbereitungen getroffen wurden, lädt die Malware eine Kopie dieser App in die virtuelle Umgebung innerhalb der Schadsoftware. Sobald der Nutzer die echte App startet, wird er unbemerkt in die manipulierte Sandbox umgeleitet.

Dieses Vorgehen stellt einen Paradigmenwechsel im Bereich mobiler Bedrohungen dar. Anstatt sich auf klassische Overlay-Techniken zu verlassen, übernehmen Angreifer nun direkt die Original-Anwendung – einschließlich ihrer Benutzeroberfläche und Funktionen. Ein ähnliches Vorgehen wurde bereits im Dezember 2023 bei einer anderen Android-Malware namens Fjord-Phantom beobachtet, die ebenfalls mit virtuellen App-Umgebungen arbeitete.

Laut Analysten richtet sich die aktuelle GodFather-Kampagne gegen rund 500 Anwendungen weltweit, darunter Banking- und Krypto-Apps. Besonders besorgniserregend ist eine neue Fähigkeit der Malware: Sie kann Gerätesperrcodes auslesen, unabhängig davon, ob Nutzer ein Muster, eine PIN oder ein Passwort verwenden. Dadurch ist nicht nur das Nutzerkonto gefährdet, sondern auch die physische Sicherheit des Geräts.

Die missbräuchliche Nutzung der Barrierefreiheitsdienste gehört zu den wichtigsten Techniken, mit denen Android-Malware ihre Zugriffsrechte erweitert. Dabei verschaffen sich Schad-Apps Berechtigungen, die weit über ihren eigentlichen Funktionsumfang hinausgehen, beispielsweise durch die Ausnutzung von herstellerspezifischen Berechtigungen (OEM-Privilegien) oder durch Sicherheitslücken in vorinstallierten System-Apps, die sich vom Nutzer nicht deinstallieren lassen.

3. SUPERCARD X: NFC-BETRUG MIT UMGELEITETEN DATENSTRÖMEN

Eine weitere Angriffswelle richtet sich gegen die NFC-Funktion moderner Smartphones. Die Malware SuperCard X, die von der russischen Sicherheitsfirma F6 entdeckt wurde, basiert auf einer modifizierten Version des Open-Source-Tools NFCGate. Ihr Ziel ist es, die NFC-Kommunikation in Echtzeit umzuleiten, beispielsweise beim kontaktlosen Bezahlen oder beim Auslesen von EMV-Chips.

Im Angriffsszenario liest die Malware NFC-Daten von Bankkarten aus, überträgt diese in Echtzeit an ein angreiferkontrolliertes Gerät und nutzt sie dort für Zahlungen an POS-Terminals oder Bargeldabhebungen an Geldautomaten.

SuperCard X kam zunächst bei Angriffen in Italien und Russland zum Einsatz. Inzwischen existieren Varianten, die gezielt Nutzer in Australien, Europa und den Vereinigten Staaten ansprechen. Technisch basiert die Malware auf der chinesischen Plattform NGate, einer NFC-fähigen Malware-Suite, die ebenfalls bereits in Tschechien aktiv war.

4. BEDROHUNGEN AUS OFFIZIELLEN APP-STORES

Während alle zuvor genannten Malware-Varianten darauf angewiesen sind, dass Nutzer infizierte Anwendungen manuell, etwa per Sideloading, auf ihren Geräten installieren, zeigen neue Untersuchungen nun auch das Vorhandensein schädlicher Apps in den offiziellen Stores von Google Play und Apple. Diese Anwendungen können persönliche Daten ausspähen und mnemonische Wiederherstellungsphrasen von Kryptowallets stehlen, um digitale Vermögenswerte der Nutzer zu kompromittieren.

Eine der betroffenen Anwendungen, RapiPlata, wurde Schätzungen zufolge rund 150.000 Mal auf Android- und iOS-Geräten heruntergeladen – ein deutliches Zeichen für die Ernsthaftigkeit der Bedrohung. Bei der App handelt es sich um eine sogenannte SpyLoan-Malware: Sie lockt Nutzer mit angeblich günstigen Kreditangeboten, um sie anschließend zu erpressen, auszuspionieren und ihre Daten zu stehlen.

Laut dem Sicherheitsunternehmen Check Point zielt RapiPlata insbesondere auf Nutzer in Kolumbien ab. Die App verspricht schnelle Kleinkredite, erfasst tatsächlich jedoch umfangreiche persönliche Informationen, darunter SMS-Nachrichten, Anruflisten, Kalendereinträge und Daten zu installierten Anwendungen. Diese Daten werden anschließend an externe Server übertragen.

Im Gegensatz dazu schleusten Angreifer Krypto-Phishing-Apps über kompromittierte Entwicklerkonten in die offiziellen Stores ein. Diese Apps nutzen WebView, um gefälschte Webseiten anzuzeigen und die Wiederherstellungsphrasen von Kryptowallets abzugreifen – mit dem Ziel, die digitalen Guthaben der Opfer zu entwenden.

Auch wenn diese Apps inzwischen aus den offiziellen App-Stores entfernt wurden, besteht die Gefahr weiterhin: Die Android-Versionen könnten nach wie vor über inoffizielle Drittanbieter-Marktplätze erhältlich sein. Nutzer sollten daher besonders vorsichtig sein, wenn sie Finanz- oder Kredit-Apps herunterladen.

ANDROID-SICHERHEIT STEHT AM SCHEIDEWEG

Die Kombination aus Overlay-Angriffen, Virtualisierungs-Frameworks, NFC-Manipulation und Store-Bypassing vergrößert die Angriffsfläche für Android-Geräte dramatisch. Angreifer erlangen tiefe Systemzugriffe – oft ohne Root-Access oder sichtbare Warnungen.

„Die Abwehr von Rechteausweitungen und die Absicherung des Android-Ökosystems gegen überprivilegierte oder schadhafte Apps erfordert mehr als nur Nutzeraufklärung oder reaktive Sicherheitsupdates", so Ziv Zeira von Zimperium. „Es braucht proaktive, skalierbare und intelligente Schutzmechanismen."

Notwendig sind verhaltensbasierte Erkennungsmethoden, systemweite Überwachung privilegierter API-Zugriffe, stärkere Kontrolle über App-Installationen aus alternativen Quellen, regelmäßige Auditierung vorinstallierter Apps und engere Zusammenarbeit zwischen Plattformbetreibern, App Stores und Cybersicherheitsanbietern. ■

THN / Stefan Mutschler, freier Journalist

Wie moderne Backup-Systeme Unternehmen vor dem Totalausfall schützen

DIE LETZTE BASTION

Aktuelle Backup-Technologien bieten weit mehr als nur Datensicherung. Sie werden zunehmend zu einem zentralen Element der Unternehmenssicherheit und können im Ernstfall über die Existenz eines Unternehmens entscheiden.

Ein mittelständischer Serviettenhersteller aus Euskirchen musste kürzlich Insolvenz anmelden, nachdem ein Cyberangriff zu drei Tagen Produktionsstillstand und drei Wochen eingeschränktem Betrieb geführt hatte. Dem Unternehmen blieben lediglich drei Monate zur Bewältigung des Millionenschadens. Das Beispiel zeigt, dass nicht nur große Konzerne oder KRITIS-Unternehmen sich Gedanken über ihre Cyberresilienz machen müssen. Die Gefahr existenzbedrohender Angriffe betrifft Unternehmen aller Größenordnungen.

Das Bewusstsein für diese Bedrohungen ist in den vergangenen Jahren deutlich gestiegen. Unternehmen investieren mittlerweile fast 20 Prozent ihrer IT-Budgets in Cybersicherheit. Dennoch bleiben Ransomware und Malware die häufigsten Angriffsformen. Wenn die primären Sicherheitsmaßnahmen versagen, bildet ein zuverlässiges Backup-System die letzte Verteidigungslinie. Dabei bieten Backup-Tools heutzutage mehr Funktionen, als nur die einfache Sicherheitskopie von Dateien in einem gesicherten Speicher. Diese grundlegende Funktionalität zur Wiederherstellung defekter Dateien wurde in den letzten Jahren konsequent ausgebaut.

BACKUP IST MEHR ALS NUR BACKUP

Zeitgemäße Backup-Infrastrukturen verstärken die Unternehmensresilienz bereits vor dem eigentlichen Sicherungsprozess. Sie arbeiten mit Zero-Trust-Netzwerkstrukturen zusammen und nutzen Informationen aus Security-Tools, um die Widerstandsfähigkeit des Gesamtsystems zu verbessern. Aber auch während der Sicherung wird den Datenflüssen im Backup immer mehr Aufmerksamkeit gewidmet. Transport-Layer-Security-(TLS)-Verschlüsselung ist inzwischen Standard. Zudem analysieren die Systeme mittels Entropiemessungen die Daten während des Backups, um möglicherweise kompromittierte Inhalte zu identifizieren. Solche Messungen sind statistische Verfahren zur Vorhersage nutzbarer Dateninhalte, die veränderte Daten erkennen können.

Darüber hinaus werden die Daten indiziert, um Threat Hunting zu betreiben. Dabei kommen aktuelle YARA Rules, Dateimuster und Hashes zum Einsatz, um die Qualität der gesicherten Daten zu überprüfen. Aus diesen Ergebnissen können exakte Wiederherstellungspunkte für „saubere" Restores identifiziert werden. Für die Überprüfung der Wiederherstellungsfähigkeit werden sogenannte Cleanrooms eingesetzt. Früher waren diese Restore-Tests auf einzelne virtuelle Maschinen begrenzt – heute lassen sich in vielen der neuen Lösungen zusammenhängende Tests auf Applikationsbasis durchführen.

Mithilfe dieser Techniken bieten aktuelle Backup-Tools eine genaue Vorhersage über das Recovery Time Objective (RTO) und das Recovery Point Objective (RPO) sowie zur Datenqualität. Derzeit erleben wir, wie künstliche Intelligenz diese Analysen immer weiter verbessert.

Backup-Systeme sind heute ein unverzichtbarer und strategisch wichtiger Bestandteil moderner Sicherheitsarchitekturen und leisten einen entscheidenden Beitrag zur Cyberresilienz – vorausgesetzt, Unternehmen nutzen konsequent die darin enthaltenen Analyse- und Erkenntnismöglichkeiten. Während das Management Backups früher oft nur als ungeliebten „Kostenfresser" betrachtet hat, hat sich diese Sichtweise inzwischen gewandelt. Unter dem Stichwort Business Continuity und Risikomanagement gelten sie mittlerweile als tragendes Fundament für die Verfügbarkeit und Sicherheit von Unternehmensdaten. ■

ANDREAS WAGENER
leitet den Bereich Data Protection Consulting der Empalis Consulting.

Gezielte Maßnahmen, aktuelle Zahlen und Praxistipps

RANSOMWARE-SCHUTZ FÜR DEN MITTELSTAND OHNE MILLIONENBUDGET

Ransomware-Angriffe treffen den deutschen Mittelstand mit voller Wucht. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zählen diese Attacken zu den größten Cyberrisiken weltweit. Besonders kleine und mittlere Unternehmen (KMU) werden immer häufiger zur Zielscheibe, da sie oft wertvolle Daten besitzen, aber weniger in Sicherheit investieren als Großkonzerne. Mit gezielten Maßnahmen können sich jedoch auch KMU wirksam schützen.

Allein im Oktober vergangenen Jahres waren laut einem Lagebericht des BSI in Deutschland 72 Kommunen von Ransomware-Angriffen betroffen, was sich direkt auf etwa 20.000 Arbeitsplätze auswirkte. Die durch Ransomware verursachten finanziellen Schäden weltweit lagen bei mehr als 1,1 Milliarden US-Dollar.

Die Gefahr durch Ransomware ist allgegenwärtig und betrifft längst nicht mehr nur Großkonzerne. Cyberattacken werden zunehmend gezielter, ausgeklügelter und wirkungsvoller. Ob ein Unternehmen global oder lokal agiert, ist dabei unerheblich – entscheidend bleibt, ob es Schwachstellen aufweist. Genau hier liegt häufig das Problem vieler mittelständischer Betriebe: unzureichend geschützte Systeme, veraltete Technik sowie ein fehlendes Problembewusstsein der Angestellten für die Risiken öffnen Hackern die Türen.

WARUM DER MITTELSTAND BESONDERS GEFÄHRDET IST

Aus Sicht von Tätern ist der Mittelstand ausgesprochen attraktiv. Einerseits verfügen mittelständische Unternehmen über wertvolle Daten, technisches Fachwissen und lukrative Geschäftsbeziehungen. Andererseits mangelt es oft an umfassenden IT-Sicherheitsmaßnahmen. Während Großkonzerne erhebliche Summen in ihre Verteidigung investieren, befinden sich viele Mittelständler noch im Aufbau ihrer Sicherheitsstrukturen oder verlassen sich lediglich auf einen Basisschutz wie Antivirenprogramme und einfache Firewalls.

Hinzu kommt die fortschreitende Digitalisierung – sei es durch Cloud-Dienste, flexible Arbeitsmodelle oder automatisierte Prozesse. Sie erhöht die Komplexität der IT-Systeme und somit auch die Anzahl potenzieller Schwachstellen. Oft bleiben die Sicherheitsmaßnahmen jedoch hinter dieser Entwicklung zurück. Der klassische „IT-Mitarbeiter, der die Aufgabe nur nebenbei übernimmt", oder eine aus Kostengründen ausgelagerte IT-Betreuung reicht in vielen Fällen nicht mehr aus, um moderne Angriffe rechtzeitig zu erkennen und zu stoppen.

Ransomware-Gruppen operieren heute wie Unternehmen: Sie haben klare Aufgabenverteilungen, technischen Support, Vertriebskanäle im Darknet und nutzen professionelle Tools, um ihre Schadsoftware zu verbreiten. Der Mittelstand muss einsehen, dass er nicht zu klein ist,

Bild: Pixel Studio - stock.adobe.com

um ins Visier zu geraten – im Gegenteil: Er ist vielmehr „klein genug", um angreifbar zu sein, und gleichzeitig „groß genug", um sich als Ziel zu lohnen.

FÜNF SCHUTZMAßNAHMEN MIT BEGRENZTEM BUDGET

Die gute Nachricht lautet: Um sich wirksam vor Ransomware zu schützen, braucht es kein riesiges Budget, sondern vor allem ein durchdachtes Vorgehen. Fünf Maßnahmen stehen dabei im Fokus – sie lassen sich auch mit begrenzten Mitteln umsetzen, vorausgesetzt, es gibt eine klare Strategie und ein ausgeprägtes Verantwortungsbewusstsein.

1. Mitarbeitersensibilisierung: Zuallererst ist es wichtig, dass Firmen ihre Belegschaft in den Mittelpunkt stellen. Der Mensch stellt nach wie vor die größte Angriffsfläche im Bereich der Informationssicherheit dar. Angreifer setzen gezielt auf Methoden wie Phishing, gefälschte Webseiten oder Social Engineering, um menschliches Fehlverhalten auszunutzen. Durch wiederkehrende Trainings – sei es online oder in Seminaren – kann man das Bewusstsein der Mitarbeiter schärfen und sie auf typische Angriffe vorbereiten. Das ist nicht teuer, bringt aber deutliche Pluspunkte im Hinblick auf Sicherheit.

2. Systematische Datensicherung: Ein weiterer wichtiger Punkt ist ein durchdachtes Konzept für Datensicherungen. Nur wer regelmäßig Backups macht – und zwar getrennt vom normalen Netzwerk – kann im Notfall Daten zurückspielen, ohne auf die Forderungen von Hackern einzugehen. Oft reichen einfache Cloud-Lösungen oder externe Festplatten aus, wenn sie klug eingesetzt und regelmäßig überprüft werden.

3. Berechtigungsmanagement: Auch die Frage, wer auf was zugreifen darf, muss neu bewertet werden. In vielen Betrieben haben zu viele Benutzer Adminrechte, obwohl diese für ihre Arbeit nicht erforderlich sind. Das Zero-Trust-Prinzip besagt, dass jeder Nutzer nur die Berechtigungen erhält, die er für seine jeweilige Tätigkeit wirklich benötigt – und nicht mehr. So verhindert man, dass sich Angreifer frei im System bewegen können.

4. Konsequentes Patchmanagement: Auch das Patchmanagement darf nicht vernachlässigt werden. Veraltete Software stellt ein erhebliches Einfallstor für Angreifer dar. Deshalb sollten Sicherheitsupdates stets zeitnah und möglichst automatisiert installiert werden. Dies lässt sich entweder über einfache Werkzeuge oder durch die Unterstützung eines IT-Dienstleisters umsetzen. Der Aufwand bleibt dabei überschaubar, während der Sicherheitsgewinn erheblich ist.

5. Moderne Systeme: Schließlich sind moderne Schutzsysteme wie Endpoint Detection and Response (EDR) sinnvoll, die ungewöhnliche Aktivitäten auf Endgeräten erkennen und automatisch Gegenmaßnahmen einleiten können. Früher waren solche Technologien vor allem großen Konzernen vorbehalten, inzwischen existieren jedoch auch bezahlbare Varianten für kleinere Unternehmen – beispielsweise als Cloud-Dienste mit kalkulierbaren monatlichen Kosten.

DER NOTFALLPLAN: VORBEREITET SEIN, WENN ES ERNST WIRD

Trotz aller Vorsichtsmaßnahmen kann es dennoch vorkommen, dass das System blockiert wird, man nicht mehr an seine Daten herankommt und sich ein Erpresser meldet. Jetzt ist entschlossenes Handeln gefragt – jedoch keinesfalls planlos. Ein durchdachter Notfallplan ist das A und O, um in so einer Lage die Nerven zu behalten.

Schon bei den Vorbereitungen muss klar sein, wer zuständig ist. Wer gehört zum Krisenstab? Wer redet mit Angestellten, Kunden, Behörden und der Presse? Welche Systeme müssen als Allererstes wieder laufen? Welche externen Fachleute – zum Beispiel IT-Forensiker oder Security-Berater – kann man im Notfall dazuholen?

Bei einem erkannten Angriff müssen zunächst die betroffenen Systeme isoliert werden: Netzwerkverbindungen kappen, Server herunterfahren und sichergehen, dass sich der Schaden nicht weiter ausbreitet. Parallel dazu beginnt die Spurensuche: Was genau ist passiert? Auf welchem Weg konnten die Angreifer eindringen? Wurden möglicherweise Daten gestohlen?

Die Kommunikation über den Vorfall muss ehrlich und offen sein – intern wie extern. Die Angestellten sollten sofort Bescheid wissen, damit keine Panik entsteht oder jemand Fehler macht. Auch Kunden und Partner müssen erfahren, ob und wie sie betroffen sind. Dabei ist jedoch Vorsicht geboten: Alle Informationen sollten vorab rechtlich und technisch geprüft werden, um Fehlinformationen oder rechtliche Konsequenzen zu verhindern.

Parallel dazu beginnt die Wiederherstellung. Im Idealfall hat man aktuelle, funktionierende Backups zur Verfügung, mit denen sich der ursprüngliche Systemzustand wiederherstellen lässt, ohne auf die finanziellen Forderungen der Erpresser einzugehen. Zahlungen an Angreifer sollte man generell sehr kritisch sehen – sie sind rechtlich heikel, befeuern das Geschäft der Kriminellen und garantieren keine erfolgreiche Entschlüsselung.

Ein guter Notfallplan endet mit einer gründlichen Nachbereitung. Welche Schwachstellen wurden ausgenutzt? Welche Abläufe müssen angepasst werden? Wie lassen sich solche Zwischenfälle in Zukunft verhindern? Diese Erkenntnisse sollten dokumentiert und in die Sicherheitsstrategie integriert werden.

SICHERHEIT ALS TEIL DER UNTERNEHMENSKULTUR

Ransomware betrifft nicht nur die anderen – der Mittelstand steckt längst mittendrin. Doch wer vorbereitet ist, kann sich wirksam schützen. Dafür braucht es keine riesigen Investitionen, sondern nur den Willen, Verantwortung zu übernehmen, eine realistische Einschätzung der Risiken und den Mut, Sicherheit als Teil der Firmenkultur zu sehen.

Auch kleine Schritte können viel bewirken – solange sie gut geplant sind. Unternehmen, die ihre Mitarbeiter einbinden, ihre IT-Landschaft genau kennen und auf den Ernstfall vorbereitet sind, haben oft bereits einen entscheidenden Vorsprung gegenüber vielen Wettbewerbern. Denn effektiver Schutz fängt nicht bei der Technik an, sondern bei der Einstellung. ■

ANNA LISA YANG
ist Informationssicherheitsexpertin bei der Abass GmbH.

Dateilose Taktiken, persistente Bedrohungen

SUPPLY-CHAIN-ANGRIFFE ALS EINSTIEGSPUNKT FÜR RANSOMWARE

Angriffe über die Lieferkette sind längst kein Randphänomen mehr. Sie verbinden subtile Manipulationen mit modernen, dateilosen Angriffstechniken und umgehen klassische Schutzmechanismen. Unternehmen müssen ihre Abwehrstrategien anpassen – schneller denn je.

Angriffe auf Softwarelieferketten gehören inzwischen zur Spitze moderner Ransomware-Kampagnen. Anstelle einer direkten Infektion des Zielsystems attackieren Täter gezielt Drittanbieter, Bibliotheken oder hardwarenahe Komponenten und schaffen auf diese Weise verdeckte Eintrittswege in Unternehmensnetze. Diese indirekte Vorgehensweise macht nicht nur die Zuordnung schwieriger, sondern unterläuft etablierte Verteidigungsmechanismen. Kombiniert mit dateilosen Techniken führt das zu einer Bedrohungslage, die sich nur schwer erkennen lässt: Eine Kompromittierung erfolgt heute häufig nicht mehr durch klassische Schadsoftware, sondern über Speicheroperationen, legitime Tools und standardisierte Betriebssystemkomponenten.

Die Sicherheitsarchitektur vieler Unternehmen ist auf solche Szenarien nicht vorbereitet. Besonders in vernetzten Branchen mit langen Produktlebenszyklen, komplexen Abhängigkeiten zwischen Komponenten und einer hohen Dichte an Embedded-Systemen finden Angreifer günstige Bedingungen vor. Dass etwa 69 Prozent aller Organisationen im vergangenen Jahr mindestens einen erfolgreichen Ransomware-Angriff meldeten (laut Veeam Ransomware Trends Report, www.veeam.com/blog/ransomware-trends.html), überrascht vor diesem Hintergrund kaum. Noch gravierender ist, dass sich bei über 89 Prozent dieser Vorfälle der Angriff gezielt gegen Backup-Repositories richtete – in 34 Prozent der Fälle mit zumindest teilweisem Erfolg. Die oft zitierte Vorstellung, Ransomware beginne stets mit einem Dateianhang in einer E-Mail, greift in diesem Kontext deutlich zu kurz.

LIEFERKETTEN ALS ACHILLESFERSE

Das eigentliche Einfallstor liegt in den vorgelagerten Abhängigkeiten. Ob Remote-Update, Drittanbieter-SDK oder generisch eingebundene Firmware, der eigentliche Angriff erfolgt upstream. Erst nach erfolgreicher Modifikation gelangt die manipulierte Komponente mit regulären Prozessen zum eigentlichen Ziel. Dieser Downstream-Angriff wirkt dann wie ein legitimes Update, ein vertrauliches Logistiksystem oder ein langjährig genutztes Embedded-Modul. Prominente Vorfälle wie bei SolarWinds, Kaseya, MOVEit oder ASUS Live Update haben gezeigt, wie wirkungsvoll dieser Mechanismus funktioniert. Es genügt, einen einzigen, zentralen Update-Prozess zu kompromittieren, um anschließend zehntausende Zielsysteme simultan zu infizieren.

Dabei geraten längst nicht nur klassische IT-Komponenten ins Visier. Besonders industriell eingesetzte Steuerungen und Geräte mit Echtzeitbetriebssystemen (RTOS), die selten aktualisiert werden und häufig Open-Source-Komponenten wie BusyBox oder OpenSSL enthalten, sind lohnende Ziele. Angreifer nutzen hier fehlende Integritätsprüfungen, eingebettete Bibliotheken oder selten dokumentierte Firmwarepfade, um Schadcode über längere Zeiträume unerkannt zu verteilen. Die Tatsache, dass rund 80 Prozent aller industriellen Firmware-Stacks quelloffene Module enthalten, erhöht das Risiko signifikant.

DATEILOSE ANGRIFFE ERSCHWEREN ERKENNUNG

Einmal in der Zielumgebung angelangt, verzichten moderne Angreifer zunehmend auf klassische Malware. Stattdessen arbeiten sie mit

dateilosen Techniken, bei denen keine ausführbare Datei auf der Festplatte abgelegt wird. Die Nutzlast existiert ausschließlich im Arbeitsspeicher oder in persistenten Konfigurationselementen wie dem Windows-Management-Instrumentation-(WMI)-Repository, der Windows-Registrierung oder in geplanten Aufgaben. Diese Strategie hat zwei Vorteile: Sie vermeidet signaturbasierte Erkennungsmethoden und erschwert die forensische Nachverfolgung. In einer Illumio-Studie (www.illumio.com/resource-center/cost-of-ransomware) gaben 56 Prozent der Befragten an, Opfer eines Angriffs geworden zu sein, bei dem Daten exfiltriert, aber keine Malware sichtbar hinterlassen wurde.

Die technische Umsetzung dieser Angriffe variiert. Bei Typ-I-Angriffen erfolgt keine Dateinutzung, wie bei DoublePulsar, das per EternalBlue-Schwachstelle direkt in den Kernelspeicher injiziert wird. Andere Varianten wie Kovter (Typ III) nutzen Registrierungseinträge zur Steuerung, legen aber keine verwertbare Datei auf dem Datenträger ab. Dazwischen liegt Typ II, hier werden Skripte oder Shellcode im WMI oder als Autorun definiert, ohne je als Datei aufzutreten. Die Folge: selbst gründliche Antivirenscans erkennen die Bedrohung nicht, weil schlicht nichts zum Scannen existiert.

ANGRIFF MIT BORDMITTELN

Ergänzt wird dieses Arsenal durch sogenannte Living-off-the-Land-Techniken (LOTL). Angreifer nutzen dabei legitime, signierte Systemtools wie regsvr32.exe, powershell.exe oder mshta.exe zur Ausführung ihrer Schadlogik. Der gesamte Angriff findet so im Rahmen gültiger Systemprozesse statt, ohne verdächtige Binärdateien, ohne auffällige Prozesse. Besonders perfide: Viele dieser Tools sind in Whitelists enthalten oder werden in produktiven Umgebungen aktiv genutzt. Ein Exploit, der über PowerShell eine Registry-Backdoor setzt, ist schwerer zu entdecken als ein klassischer Dropper.

Diese Methoden sind nicht nur raffinierter, sondern auch effektiver. Die Illumio-Studie beziffert den durchschnittlichen finanziellen Schaden eines einzelnen Ransomware-Vorfalls auf 146.685 US-Dollar, bei nur 13 Prozent vollständiger Datenwiederherstellung nach Lösegeldzahlung. Immer häufiger arbeiten Angreifer in mehreren Phasen: zunächst der Zugriff über ein legitimes Tool, dann laterales Vorgehen (lateral movement) mit gestohlenen Credentials, schließlich Datenexfiltration oder Kryptolocker. In 47 Prozent der Fälle dient die Exfiltration erbeuteter Daten der Erpressung.

LIEFERKETTE UNTER RECHTLICHEM DRUCK

Mit dem Cyber Resilience Act (CRA) und der Radio Equipment Directive (EN18031) führt die EU eine Herstellerhaftung für unsichere Produkte ein. Gleichzeitig wächst die internationale Zusammenarbeit: Der US-amerikanischen Counter-Ransomware-Initiative gehören inzwischen über 60 Staaten an, mehrere Länder verbieten öffentliche Lösegeldzahlungen.

Die technischen Herausforderungen bleiben jedoch bestehen, besonders in komplexen Lieferketten mit unsicheren Komponenten. Ransomware-Gruppen agieren heute schneller und gezielter. Die durchschnittliche „Dwell Time" – die Zeitspanne zwischen initialem Zugriff und aktiver Schadensausführung – liegt laut Veeam mittlerweile unter 24 Stunden.

Gleichzeitig hat sich die Erkennungsqualität verbessert. Das Antimalware Scan Interface (AMSI) von Microsoft ermöglicht die Analyse von Skript-Inhalten zur Laufzeit, selbst bei starker Verschleierung. In Microsofts Sharpshooter-Fallbeispiel wurde .NET-Shellcode direkt aus dem Arbeitsspeicher blockiert, ohne dass eine Datei vorhanden war.

Microsofts Defender ATP nutzt zusätzlich Speicherscans, Verhaltensüberwachung und kontrollierte Zugriffsmechanismen, um auch verschachtelte Makro-Payloads wie Ursnif oder Fileless-Trojaner wie Powemet zu erkennen. Entscheidender Vorteil: Durch Multi-Process-Correlation lässt sich auch lateral eingeschleuste Malware rekonstruieren, zum Beispiel wenn ein initiales Makro ein Kommandozeilenprogramm auslöst, das wiederum über powershell.exe ein Remote-Skript lädt.

LÜCKEN IN DER VERTEIDIGUNG

Trotz wachsender Awareness bleibt die Abwehr fragmentiert. Nur 42 Prozent der Unternehmen setzen laut Illumio gezielt KI-gestützte Verteidigungsmechanismen gegen Ransomware ein. Die Hälfte der Unternehmen beklagt eine erschwerte Reaktionsfähigkeit durch interne Nachlässigkeit, unzureichende Prozesse oder fehlende Sichtbarkeit. Segmentierung, Zero Trust und Multi-Faktor-Authentifizierung (MFA) gelten zwar als etablierte Bausteine, entfalten jedoch nur Wirkung in Kombination mit präziser Netzwerktransparenz, Angriffserkennung und automatisierter Isolation.

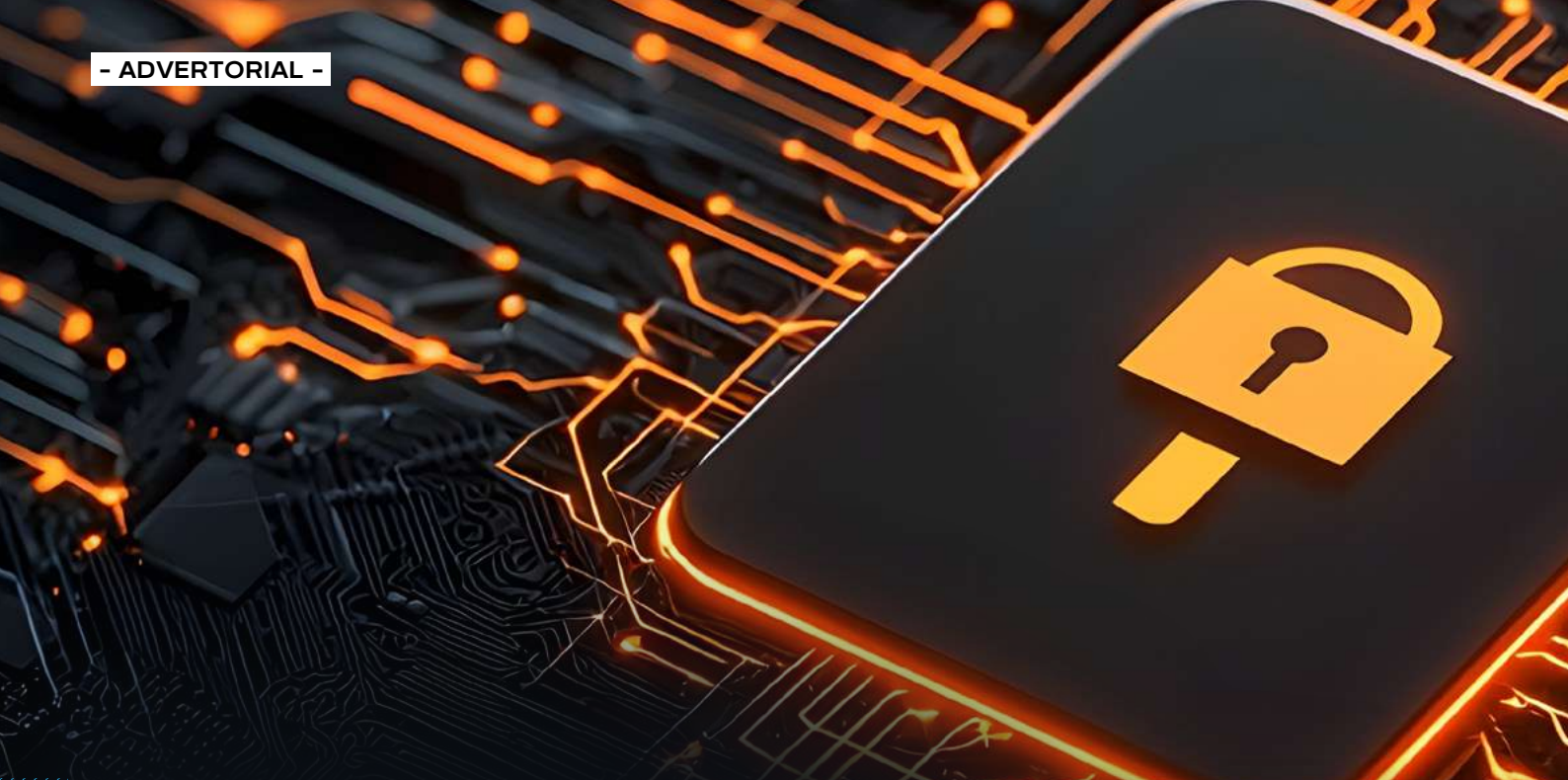
Ein zentraler Schwachpunkt bleibt der Mensch. Social Engineering liefert auch 2025 den Einstiegspunkt für viele dateilose Kampagnen. In 58 Prozent der Fälle beginnt der Angriff laut Illumio mit einer Phishing-E-Mail, häufig gefolgt von der Aktivierung eines Makros oder dem Klick auf einen präparierten Link. Dass Windows S-Mode Skriptausführung unterbindet, ist ein Schritt, schützt jedoch nur einzelne Nutzersegmente. In realen Infrastrukturen helfen nur Awareness, Angriffssimulationen und robuste Endpoint-Detection-and-Response-(EDR)-Systeme.

FAZIT

Moderne Ransomware-Operationen nutzen gezielt die Schwächen der Softwarelieferkette und kombinieren sie mit dateilosen Persistenzmechanismen. Dies erfordert ein neues Verteidigungsparadigma: weg von signaturbasierten Modellen, hin zu verhaltensbasierter Erkennung, Speicheranalyse und tiefgreifender Integritätsprüfung in allen Stufen der IT- und OT-Infrastruktur.

Angreifer agieren heute methodisch und kennen die eingesetzten Tools, die Systemlandschaft und typische menschliche Fehler. Die nächste Supply-Chain-Attacke wird nicht durch eine verdächtige Datei auffallen – sie kommt als scheinbar harmloses, digital signiertes Update. ■

THOMAS JOOS
ist freier Journalist.



Zwischen Angriff und Abwehr: Deutschlands IT steht unter Druck – sind Sie vorbereitet? Wir helfen.

In Deutschland werden täglich Hunderttausende Angriffe auf die digitale Infrastruktur registriert und weltweit sogar Millionen.

Wir möchten Ihnen helfen. Technikbegeistert und sicher!

Cyberangriffe gehören heute zum Alltag – egal ob es um Ihr Unternehmen geht oder Sie als Privatperson. Laut dem Sicherheitstacho der Deutschen Telekom werden allein in Deutschland innerhalb von 30 Tagen 130 Millionen Angriffsversuche registriert. Weltweit sind es sogar mehrere Hundert Millionen. Die Bedrohung ist real.

abass GmbH – Ihr Partner für IT-Sicherheit und smarte Technologie

Als IT-Systemhaus mit Sitz in Langen (Hessen) unterstützen wir unsere Kunden seit über 30 Jahren bei der sicheren und effizienten Digitalisierung. Unsere Leidenschaft gilt der Technik – aber die höchste Priorität ist die Sicherheit unserer Kunden. Mit maßgeschneiderten IT-Lösungen, proaktivem Monitoring und individuellem Support helfen wir Ihnen, Ihre digitale Infrastruktur zu schützen.

Wurden Sie gehackt oder sind Ihre Systeme verschlüsselt worden?

Wir lassen Sie nicht allein - wir bauen Ihre IT wieder auf.

Ein Cyberangriff kann alles lahmlegen: Server, Arbeitsplätze, die Kommunikation – und oft sind alle Daten unzugänglich. Doch keine Panik! Wir helfen Ihnen nicht nur im Vorfeld, sondern auch im Anschluss. Ob Ransomware-Angriff, Datenverschlüsselung oder Systemkompromittierung – wir analysieren und rekonstruieren Ihre IT-Infrastruktur mit Know-how und Erfahrung. Unser Ziel: minimaler Ausfall und die schnelle Wiederherstellung der Systeme.

- Soforthilfe bei IT-Notfällen
- Systemwiederherstellung
- Schutz vor künftigen Angriffen

Bild: Kunchan - stock.adobe.com

Unternehmensprofil: abass GmbH

Als erfahrenes IT-Systemhaus mit klarem Fokus auf Informationssicherheit haben wir es uns zur Aufgabe gemacht, Unternehmen vor den immer komplexer werdenden Cyberbedrohungen zu schützen. Schutzmaßnahmen schützen nicht nur, Technik allein reicht nicht aus. Die abass GmbH versteht diese Dynamik und entwickelt ganzheitliche Sicherheitsstrategien, die sowohl technische Lösungen als auch die Sensibilisierung und Schulung von Mitarbeitern umfassen.

Wir möchten IT-Sicherheitslösungen in Kombination mit Informationssicherheit individuell für Sie kreieren, um Sie gezielt vor digitalen Bedrohungen zu schützen und die Angriffsfläche deutlich zu reduzieren.

Wir sind keine reinen Technikdienstleister; wir sind strategische Partner, die Ihre individuellen Geschäftsabläufe verstehen und maßgeschneiderte Sicherheitskonzepte entwickeln.

Unsere Kernkompetenzen umfassen:

Sicherheitsberatung und -strategie

Wir analysieren Ihre bestehende IT-Infrastruktur, identifizieren Schwachstellen und entwickeln eine maßgeschneiderte Sicherheitsstrategie, die den aktuellen Bedrohungslandschaften gerecht wird. Dazu gehören Risikoanalysen, Compliance-Beratung (zum Beispiel gemäß ISO 27001) und die Erstellung von Notfallplänen.

Technische Sicherheitslösungen

Von der Implementierung modernster Firewalls und Intrusion-Detection-/-Prevention-Systeme über Endpoint-Security-Lösungen bis hin zu Cloud-Sicherheitslösungen – wir sorgen für eine robuste technische Abwehr. Wir arbeiten mit führenden Herstellern zusammen und integrieren Lösungen, die optimal zu Ihren Anforderungen passen.

Schwachstellenanalyse

Wir testen die Widerstandsfähigkeit Ihrer Systeme durch simulierte Angriffe und identifizieren so potenzielle Einfallstore, bevor sie von Cyberkriminellen ausgenutzt werden können.

Mitarbeitersensibilisierung und Schulungen

Der Fall von Sarah Mustermann unterstreicht die Bedeutung dieses Bereichs. Wir bieten maßgeschneiderte Schulungen und Workshops an, die Ihre Mitarbeiter für Social Engineering, Phishing, CEO-Fraud und andere gängige Angriffsmethoden sensibilisieren. Unser Ziel ist es, ein starkes Sicherheitsbewusstsein in Ihrem Unternehmen zu verankern und Ihre Mitarbeiter zu Ihrer ersten Verteidigungslinie zu machen.

Incident Response und Krisenmanagement

Im Fall eines Sicherheitsvorfalls sind schnelle und professionelle Reaktionen entscheidend. Wir unterstützen Sie bei der Bewältigung von Cyberangriffen, der Minimierung von Schäden und der Wiederherstellung des Normalbetriebs.

Wir arbeiten proaktiv und legen den Fokus auf vorbeugende Maßnahmen, um Angriffe von vornherein zu vermindern oder die Folgen zu minimieren. Unser Unternehmen sieht Informationssicherheit als Prozess an, der dauerhaft betreut werden muss, und verbessert seine Sicherheitsstrategien sowie -lösungen dementsprechend ständig weiter, um Ihnen stets den besten Schutz bieten zu können.

Ohne Vertrag, ohne laufende Kosten - wir unterstützen Sie sofort.

Wenn Sie sich hiermit identifizieren können, dann steht Ihnen die abass GmbH mit ihrer langen Erfahrung in Sachen IT-Sicherheit zur Seite. Schützen Sie Ihr Unternehmen - ansonsten könnten sich die Risiken als real herausstellen.

abass GmbH
Robert-Bosch-Straße 25a
63225 Langen
+49 6103 404566-0
+49 6103 404566-6
info@abass.de
www.abass.de

Mehr dazu hier

abass technikbegeistert

Kompetenzerhalt für CISOs

WEITERBILDUNGS-STRATEGIEN ZWISCHEN REGULATORIK UND PRAXIS

Die Anforderungen an Chief Information Security Officers (CISOs) wachsen stetig. Neue Regulierungen, technologische Entwicklungen und komplexe Bedrohungen erfordern gezielte Weiterbildungsstrategien. Ein Überblick über Formate, Inhalte und Methoden für Sicherheitsverantwortliche.

Bild: ChatGPT Image

Die Position des Chief Information Security Officer hat sich grundlegend gewandelt: Sie ist längst nicht mehr auf technische Aspekte beschränkt. Genau genommen war sie das nie, wurde jedoch lange Zeit vor allem als eine technische Funktion verstanden. Heute gilt der CISO als zentrale Figur für die unternehmerische Resilienz.

Angetrieben von immer komplexeren Regulierungen wie NIS-2, DORA oder dem Cyber Resilience Act sowie flankiert von disruptiven Technologien wie künstlicher Intelligenz (KI), Cloud-Diensten oder Post-Quantum-Kryptografie und einer zunehmend aktiven Bedrohungslandschaft, wächst der Druck auf die Sicherheitsverantwortlichen in den Unternehmen spürbar.

Es genügt längst nicht mehr, lediglich über Sicherheitsmaßnahmen zu wachen. CISOs müssen strategisch agieren, rechtliche Zusammenhänge bewerten, technische Entwicklungen im Blick behalten und kommunikativ überzeugen, um ihre Organisationen widerstandsfähig aufzustellen.

Doch wie sollen sie in diesem anspruchsvollen Umfeld den Anschluss halten? Die Antwort ist eindeutig: durch gezielte, kontinuierliche und praxisnahe Weiterbildung. Diese darf kein bloßes Zusatzangebot sein, sondern muss integraler Bestandteil der Aufgabe sein – unterstützt durch die Geschäftsleitung.

Im Kontext der CISO-Aufgaben geht es schon längst nicht mehr darum, ein einfaches „Mensch ärgere Dich nicht" zu spielen. Stattdessen gleicht der Job einer Schachpartie auf höchstem Niveau – und das auf mehreren Ebenen gleichzeitig.

MODERNE WEITERBILDUNGSFORMATE

Die Weiterbildung für CISOs ist heute ebenso vielfältig wie ihre Aufgaben. Zwar bilden klassische Formate wie Zertifikatskurse – etwa CISM, CISSP oder ISO/IEC 27001 – weiterhin eine wichtige Grundlage. Doch oft genügt das allein nicht mehr. Erst praxisnahe Ansätze schaffen echten Mehrwert, denn nur wer die zugrunde liegenden Prinzipien und Zusammenhänge wirklich versteht, kann im Ernstfall gezielt handeln – und auch in ruhigeren Zeiten strategisch sinnvoll und nachhaltig agieren.

Gefragt sind heute Formate, die realistische Anforderungen praxisnah simulieren, von der Führungsebene verstanden werden und zugleich ein passendes Wording vermitteln. Sie müssen sowohl technologische als auch regulatorische Entwicklungen reflektieren.

Solche Formate sind zum Beispiel:

- kompakte Online-Seminare mit Live-Simulationen zu Themen wie KI-Risiken, Cyberkrisen oder Lieferkettenanalyse
- Tabletop-Übungen mit Relevanz für Vorstände und Geschäftsführung – zum Beispiel nach Ransomware-Angriffen oder DORA-Stresstests. Der perfekte erste Ansatz, um grundlegende Vorgehensweisen einzuschleifen, ohne direkt ans Eingemachte zu gehen.
- Peer-Gruppenformate mit anderen CISOs, zum Beispiel European Cyber Security Organisation (ECSO), KRITIS-Beirat oder der Allianz für Cyber-Sicherheit. Der Austausch von Erfahrungen, Perspektiven und Lösungsansätzen ist heute wichtiger denn je.
- Führungskräftetraining zur Kommunikation mit Gremien, Umgang mit Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) sowie mit weiteren Stakeholdern. Der CISO sollte immer auch Dolmetscher zwischen der Technik und der Geschäftsleitung sein.
- Inhouse-Schulungen oder Shadowing im eigenen Unternehmen zu Themen wie DevSecOps, Cloud-Sicherheitsprüfungen oder Data Loss Prevention.
- Zunehmend etabliert sich zudem das Format hybrider Programme mit Leadership-Komponenten.

WAS CISOS WISSEN MÜSSEN – HEUTE UND MORGEN

Das Lernspektrum für CISOs ist breit und reicht von rechtlichen Anforderungen über technische Innovationen bis hin zu strategischen und psychologischen Aspekten. Die Übersicht in Tabelle 1 zeigt zentrale Themen, die für Sicherheitsverantwortliche heute und in Zukunft relevant sind.

Im Training haben sich besonders Inhalte als wirksam erwiesen, die reale Szenarien praxisnah abbilden. Dazu zählen beispielsweise Übungen auf Basis des MITRE ATT&CK-Frameworks (https://attack.mitre.org), die mit realistischen Angriffsszenarien arbeiten. Wer die Angriffswege versteht, kann sich gezielter schützen und erkennt offene Schwachstellen deutlich schneller. Der CISO übernimmt dabei auch die Rolle eines Verteidigungsstrategen, wobei der Fokus nicht nur auf digitalen Angriffen liegen sollte,

Themenfeld	Lernfokus
Regulatorik und Compliance	Umsetzung der Network and Information Security Directive 2 (NIS-2), Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA), Datenschutzaufsicht, Lieferkettensorgfaltspflichten
Strategie und Governance	Informationssicherheits-Managementsysteme (ISMS), Definition der Risikoakzeptanz (Risk Appetite), Zero-Trust-Strategie, Abstimmung mit Business-Continuity-Planungen
Technologie und Innovation	Sicherheit im Umfeld von künstlicher Intelligenz, Risiken durch Post-Quantum-Kryptografie, sichere Cloud-Architekturen, Implementierung von Extended Detection and Response (XDR)
Krisenmanagement	Entwicklung und Anwendung von Incident-Response-Playbooks, Strukturen zur Cyberabwehr, Kommunikation in Krisensituationen
Führung und Kommunikation	Berichterstattung an Aufsichts- und Entscheidungsgremien, Entscheidungspsychologie, Etablierung von Sicherheitsbewusstsein als kulturelles Prinzip

Tabelle 1: Zentrale Themen, die für Sicherheitsverantwortliche heute und in Zukunft relevant sind.

sondern ebenso physische oder kombinierte physisch-digitale Angriffsvektoren einbezogen werden sollten.

Ebenfalls hilfreich sind Simulationen von Audits, Krisen- oder Reportingsituationen, um die Kommunikation auf Vorstandsebene zu trainieren. Frühzeitig aufgedeckte und beseitigte Kommunikationslücken sorgen im Ernstfall für deutlich schnellere Reaktionen. Zudem bieten Fallstudienanalysen realer Sicherheitsvorfälle, wie etwa bei Colonial Pipeline, Swissport oder MOVEit, wertvolle Erkenntnisse. Anstatt das Rad immer wieder neu zu erfinden, können CISOs so aus den Fehlern und Erfahrungen anderer Organisationen lernen.

LERNEN IM ALLTAG

Aber Weiterbildung findet längst nicht nur im Seminarraum statt, sondern geschieht vielfach unbemerkt im Arbeitsalltag. CISOs, die regelmäßig aus Audits, Vorfällen oder Benchmarks lernen, bauen ihre Kompetenz systematisch aus, zum Beispiel durch:

- „Lessons Learned"-Zyklen nach Sicherheitsvorfällen, sowohl intern als auch im Austausch mit Netzwerken
- Auditvorbereitung als Kompetenztest, da jedes Audit bisher unbekannte Schwachstellen aufdeckt
- Review-Meetings mit Stakeholdern aus Bereichen wie IT, Einkauf oder Rechtsabteilung, um potenzielle Reibungsverluste frühzeitig zu erkennen
- Self-Assessments, beispielsweise auf Basis von BSI-Checklisten oder NIS-2-Reifegradmodellen, um den eigenen Status zu prüfen

Entscheidend dabei ist: Die besten CISOs verstehen Lernen als Teil ihrer Führungskultur. Sie fordern es aktiv von sich selbst ein und machen es in ihrer Organisation sichtbar. Sie lesen Berichte nicht nur, sondern übersetzen deren Inhalte. Sie führen nicht nur, sondern reflektieren ihr Handeln kontinuierlich.

DIE ROLLE DER PEER-LEARNINGS

„Man muss nicht jeden Fehler selbst machen, aber man muss jemanden kennen, der ihn gemacht hat." So oder so ähnlich wird es schon an der Uni gelehrt. Peer-Learning ist einer der unterschätzten Hebel für das CISO-Wachstum. Gerade industrieübergreifend, aber auch in spezifischen Runden aus der eigenen Branche kann hier ein enormer Mehrwert geschaffen werden. Aber wonach soll man konkret Ausschau halten? Gerade im Security-Umfeld ist das gezielte Netzwerken bei vielen keine Stärke. Umso wichtiger sind klare Strukturen und Formate, die diesen Austausch erleichtern.

Geeignete Plattformen für Peer-Learning sind zum Beispiel:

- Teilnahme an CISO-Roundtables und Boards
- Vertrauliche Austauschgruppen („Trust Circles")
- Teilnahme an „Threat Intelligence Sharing"-Plattformen
- Veröffentlichung eigener Lessons Learned in Fachtagungen oder Whitepapers

Diese Formate ermöglichen gezielte Kompetenzspiegelung und realistische Standortbestimmung.

Auch das Mentoring gewinnt an Bedeutung: Junge CISOs profitieren enorm von erfahreneren Sparringspartnern. Dabei ist es erst einmal nachgeordnet, ob formal im Verband oder informell. Hier ein paar Beispiele für entsprechende Netzwerke:

- **Allianz für Cyber-Sicherheit – CISO-Community:** www.allianz-fuer-cybersicherheit.de
- **CISO Alliance:** www.ciso-alliance.de/
- **ECSO:** https://ecs-org.eu/
- LinkedIn-Gruppen zum Thema

UND WAS IST MIT KI?

Künstliche Intelligenz verändert auch die Weiterbildung selbst. CISOs nutzen KI-basierte Plattformen zur Simulation von Vorfällen, zur Entwicklung individueller Lernpfade oder zur automatisierten Analyse von Audit-Ergebnissen. Zum Einsatz kommen dabei etwa adaptive Learning-Tools, die eine Risikobewertung nach DORA oder NIS-2 ermöglichen, ebenso wie KI-generierte Bedrohungsszenarien für Trainings im Bereich Incident Response. Auch Sprachmodelle – sogenannte Large Language Models (LLMs) – dienen inzwischen als interaktive Coaching-Partner, während KI-gestütztes Red- und Blue-Teaming praxisnahe Übungen zur Erkennung von Sicherheitslücken erlaubt.

Allerdings gilt es, bei der Nutzung von KI stets kritisch zu bleiben. Nicht jeder Output einer KI ist verlässlich – sogenannte Halluzinationen, also falsche oder erfundene Inhalte, treten nach wie vor regelmäßig auf. Weiterbildung bleibt deshalb ein Führungsthema, das menschliche Expertise und kritische Reflexion erfordert. Ein Chatbot allein ersetzt keinen erfahrenen Lehrmeister.

FAZIT

CISOs, die den Anspruch haben, ihre Organisation resilient zu halten, müssen bei sich selbst anfangen. Weiterbildung ist dabei kein Luxus und keine stumpfe HR-Maßnahme – sie ist strategisches Rüstzeug – also Hilfe zur Selbsthilfe. Heute und in Zukunft. Wer sich als Sicherheitsverantwortlicher nicht selbst regelmäßig weiterentwickelt, verliert den Anschluss – technisch, kommunikativ und menschlich.

Ein moderner CISO lernt nicht „on top", sondern „mittendrin". Genau darin liegt die Zukunft der Sicherheitsführung: Dranbleiben – mit der nötigen Leidenschaft für kontinuierliches Lernen. ■

ALEXANDER JABER
ist Chief Executive Officer der Compliant Business Solutions GmbH.

10 % Rabatt für <kes>+ Abonnenten

ISO/IEC 27001 Lead Implementer – PECB zertifiziert

Wie implementiert man ein ISMS nach ISO 27001?
Erhalten Sie praxisnahes Wissen
und sichern Sie sich die PECB-Zertifizierung.

10.–13.11.2025 | Frankfurt/M. + Onlineprüfung
Referent: Alexander Jaber

Schwerpunkte:

- ✓ Anwendung und Verständnis der ISO/IEC 27001 Anforderungen
- ✓ Planung, Implementierung und kontinuierliche Verbesserung eines ISMS
- ✓ Praktische Übungen, Fallstudien und Quizfragen zur realitätsnahen Wissensvermittlung
- ✓ Vorbereitung auf die PECB Zertifizierungsprüfung zum ISO/IEC 27001 Lead Implementer

Jetzt anmelden: **www.datakontext.com/it-sicherheit**

Fünf Stufen auf
dem Weg zur Cyberresilienz

DIE EVOLUTION DES CISO

Chief Information Security Officers (CISOs) müssen heute eine zentrale Rolle bei der Entwicklung wirksamer Cyberresilienz einnehmen. Der Weg dorthin folgt einem fünfstufigen Evolutionsprozess, der die Position des CISO von einem einfachen Sicherheitsbeauftragten zu einem strategischen Entscheider transformiert. Angesichts steigender Cyberbedrohungen wird diese Entwicklung für Unternehmen überlebenswichtig.

Laut einer Studie von Check Point steigt die Verantwortung der CISOs mit den neuen Rekordausmaßen der globalen Cyberangriffe.[1] So haben globale Cyberangriffe im dritten Quartal 2024 um 75 Prozent zugenommen. Gleichzeitig fühlen sich viele Unternehmen unzureichend vorbereitet: Eine Commvault-Umfrage vom Juni 2024 zeigt, dass nur 13 Prozent der befragten Organisationen sich die nötige Reife attestieren, um einen Angriff effektiv abzuwehren und sich schnell davon zu erholen.[2]

Einige Unternehmen stellen Systeme und Daten deutlich schneller wieder her als andere. Der Grund liegt oft in der richtigen Haltung zur Cybersicherheit: Reife Firmen kalkulieren das Scheitern der IT-Abwehr ein und schaffen präventiv Strukturen und Maßnahmen. Sie setzen Tools ein, die Bedrohungen frühzeitig erkennen, und arbeiten nach definierten Prozessen und Rollen, um Vorfälle gezielt einzudämmen.

Unverzichtbar für eine resiliente IT ist eine isolierte Backup-Umgebung – oft als „Dark Site" bezeichnet – die als sicherer Aufbewahrungsort für nicht manipulierbare Sicherungskopien unternehmenskritischer Daten und Anwendungen dient. Echte Reife erreichen Organisationen jedoch erst, wenn sie ihre Wiederherstellungsprozesse regelmäßig testen.

DEN EVOLUTIONSGRAD DER CYBERRESILIENZ BESTIMMEN

Es ist die Aufgabe der CISOs, notwendige Maßnahmen zur Stärkung der Cyberresilienz umzusetzen und regelmäßig auf ihre Wirksamkeit zu überprüfen. Doch nicht jeder CISO verfügt im Unternehmensgefüge über die gleichen Entscheidungsbefugnisse und Kompetenzen. In Organisationen mit geringer Widerstandsfähigkeit im Krisenfall wird die Sicherheitsverantwortung häufig Mitarbeitern übertragen, die lediglich Anweisungen ausführen können und dürfen. Das notwendige Idealbild einer fortgeschrittenen Abwehrstruktur sind hingegen CISOs, die

Bild: Li - stock.adobe.com

eng mit der Geschäftsführung zusammenarbeiten und dafür sorgen, dass Cybersicherheit im gesamten Unternehmen eine feste und zentrale Rolle spielt.

Die Evolutionsgrade der Cyberresilienz lassen sich idealtypisch in fünf Stufen beschreiben.

Stufe 1: Sicherheit zum Abhaken

Auf dieser niedrigen Entwicklungsstufe fehlt ein dedizierter CISO. Cybersicherheit wird lediglich als Teilaufgabe eines ohnehin ausgelasteten IT-Teams behandelt. Sicherheitsverantwortliche haben kaum Entscheidungskompetenzen und folgen meist einem Checklisten-Ansatz.

Stufe 2: Neue Planstelle CISO

Mit dem Unternehmen wächst auch seine Angriffsfläche. Aus einer wachsenden Zahl an Mitarbeitern, Kunden, Partnern und einer Supply Chain resultieren immer neue und komplexe Prozesse, die wiederum potenzielle Angriffspunkte für Angreifer sind. Auf dieser Stufe stellen viele Unternehmen einen eigenen Cybersicherheitsexperten ein, der auch mit Entwicklern und Programmierern zusammenarbeitet.

Nicht selten hat ein CISO nur wenig Ressourcen in Reserve, um eine umfassende Cyberabwehrstrategie zu planen – geschweige denn umzusetzen. Die Verantwortlichen für IT einerseits und für Sicherheit andererseits haben die Aufgabe, effektive Kommunikationskanäle zu etablieren, um sicherzustellen, dass sie gemeinsame Sicherheitsziele definieren und verfolgen.

Stufe 3: CISO mit erweitertem Aufgabenfeld

Auf dieser Stufe hat ein CISO hinreichend Autonomie, um Abwehrtechnologien unternehmensweit zu bewerten, einzusetzen und zu überwachen. Ohne die Kompetenz, umfassendere Maßnahmen zum Schutz sensibler Bereiche wie der Cloud-Sicherheit zu implementieren und den Zugriff auf alle Unternehmenssysteme zu kontrollieren, kann er seine Aufgaben nicht wahrnehmen. Auch wenn andere C-Level-Führungskräfte Bedenken hinsichtlich der Sicherheitsinitiativen äußern, weil sie etwa die Time-to-Market von Produkten oder Angeboten hinauszögern können, ist es ihre Aufgabe, den CISO zu unterstützen und unternehmenskritische Initiativen zur Cybersicherheit zu fördern.

Auch wenn IT und Sicherheit getrennte Teams bleiben, sollten CIO und CISO eng zusammenarbeiten, um die Ziele von IT-Betrieb und IT-Sicherheit zu harmonisieren. Die ständige Kommunikation ist für die Sicherheit und für einen reibungslosen Geschäftsbetrieb unerlässlich.

Stufe 4: CISO mit strategischen Kompetenzen

In Unternehmen mit einer weiterentwickelten Resilienz ist der CISO bei den strategischen Meetings mit dem Vorstand präsent. Hier berät er unmittelbar zu Cybersicherheitsrisiken und Resilienz. Zusammen mit dem C-Level ermittelt er proaktiv die Risikotoleranz des Unternehmens. Seine Analysen zeigen das sich verändernde Risikoprofil. Zudem entwickelt er die relevanten Strategien und Sicherheitsrichtlinien, um vereinbarte und vertretbare Toleranzen einzuhalten.

Auf dieser Stufe geben CISOs dem Vorstand auch ihr Gutachten über die Vorteile oder Risiken neuer Technologien – wie aktuell künstliche Intelligenz. Cybersicherheit ist nun ein festes Element der strategischen und operativen Planung.

Stufe 5: Sicherheit als Teil der Unternehmens-DNA

Den höchsten Grad haben Organisationen erreicht, wenn sich Beschäftigte unternehmensweit nach den Grundsätzen von „Secure by Design" an Sicherheitsprozesse und -richtlinien halten. Cybersicherheit ist auf dieser Stufe das Fundament aller Unternehmensaktivitäten. Kontinuierliche Tests der Systeme werden erwartet. Alle Abteilungen und Teams sind auf Sicherheitsereignisse und eine Wiederherstellung von Daten, Systemen, Applikationen und Infrastrukturen vorbereitet.

INDIVIDUELLE ENTWICKLUNGSPFADE

Jede Organisation hat ihre eigene technische Infrastruktur, Arbeitsweise und strategische Ausrichtung. Der Entwicklungsstand in Sachen Cybersicherheit lässt sich daher nicht pauschal bestimmen. CISOs mit den nötigen Fähigkeiten können jedoch gemeinsam mit den CIOs die Evolution der Cyberresilienz vorantreiben. Die Kenntnis der eigenen Position im Entwicklungsprozess hilft, Lücken bei Kompetenzen und Rollenverständnis zu identifizieren und zu schließen. ■

KOMMUNIKATIONS-PROBLEME ZWISCHEN CISO UND MANAGEMENT

Das Verankern von Schutz und Resilienz in der Unternehmensorganisation scheitert oft an Missverständnissen und Fehlkommunikationen zwischen den CISOs und der höchsten Management-Ebene. Das belegen die Ergebnisse einer im März 2024 veröffentlichten Studie der FTI Consulting.[3] Rund 800 C-Level-Manager aus neun verschiedenen Ländern und sieben Branchen sahen für ihr Unternehmen den wesentlichen Risikofaktor in bestehenden Kommunikationslücken zwischen CISO und Top-Management.

Ein Mangel an Vertrauen und Unverständnis erzeugen jedoch Schwachstellen. Laut den Autoren der Studie geht jeder dritte Befragte in den Führungsetagen davon aus, dass Cybersicherheitsverantwortliche ihr Top-Management über potenzielle Schwachstellen nur zögerlich informieren. Gleichzeitig meinten 66 Prozent der CISOs, dass die oberste Entscheiderebene Schwierigkeiten habe, ihre Rolle innerhalb des Unternehmens vollständig zu verstehen. 31 Prozent im C-Level haben Probleme, den konkreten Nutzen von Cyberinvestitionen nachzuvollziehen. 98 Prozent der befragten Top-Manager sprachen sich dafür aus, mehr Mittel für Kommunikations- und Präsentationstrainings für CISOs bereitzustellen, wobei fast die Hälfte diesen Bedarf als dringend bezeichnete.

Literatur

[1] Check Point: A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide, 2024. Online verfügbar unter: https://www.checkpoint.com.

[2] Commvault: Cyber Recovery Readiness Report, Juni 2024.

[3] FTI Consulting: CISO Redefined – Navigating C-Suite Perceptions & Expectations. Studie, März 2024.

CHRISTIAN KUBIK
ist Manager Field Advisory Services Team EMEAI bei Commvault.

Cyber Resilience Act stellt Hersteller digitaler Produkte vor Herausforderungen

NEUE SPIELREGELN FÜR OPEN SOURCE

Der Cyber Resilience Act (CRA) der EU ist auf dem Weg, die Sicherheit digitaler Produkte grundlegend zu verändern. Er verpflichtet Anbieter dazu, während des gesamten Lebenszyklus ihrer Lösungen Sicherheitsmaßnahmen zu treffen – inklusive Risikoanalysen, Schwachstellenmanagement und Updates. Die Regulierung betrifft Hardware, Software und „Produkte mit digitalen Elementen" – also fast alles, was heute in Unternehmen zum Einsatz kommt. Doch was bedeutet das für Open-Source-Software und ihre Nutzer? Die Antwort ist kompliziert.

Schon seit die Europäische Kommission den Cyber Resilience Act 2022 in Gang gebracht hat, sorgt er für erhitzte Gemüter zwischen Politik, Wirtschaft und Verbänden. Unternehmen haben nun bis Dezember 2027 eine Übergangsfrist, um sich auf die neuen regulatorischen Anforderungen einzustellen. Ab September 2026 greift sogar schon die Berichtspflicht, etwa bei Vorfällen oder Schwachstellen – es bleibt also nicht viel Zeit. In vielen Punkten herrscht allerdings noch Klärungsbedarf. Das bekomme ich als Vertreter von Stackable in der Expertengruppe der Europäischen Kommission an vorderster Front mit.

Der Cyber Resilience Act der Europäischen Union markiert einen Wendepunkt in der europäischen Digitalgesetzgebung. Ziel ist es, verbindliche Cybersicherheitsstandards für Produkte mit digitalen Elementen zu schaffen – von Software über IoT-Geräte bis hin zu industriellen Steuerungssystemen. Dabei stehen nicht nur klassische Softwarehersteller im Fokus, sondern auch Open-Source-Projekte, Plattformen, Integratoren und Anwenderunternehmen. Die zentrale Herausforderung: Wie lässt sich ein Gesetz, das von klaren Herstellungs- und Vertriebsstrukturen ausgeht, auf ein Ökosystem anwenden, das von Freiwilligen, Dezentralität und kollaborativer Entwicklung geprägt ist?

Der CRA unterteilt Produkte in drei Kategorien: default, important und critical. Alle Produkte müssen grundlegende Anforderungen erfüllen – etwa Schwachstellenmanagement, Sicherheitsupdates, technische Dokumentation und Risikoanalysen. Lösungen der höheren Risikoklassen, important und critical, benötigen zudem eine externe Zertifizierung. Was in der Theorie nach einer sinnvollen Abstufung klingt, wirft in der Praxis eine Reihe von Problemen auf – besonders, weil viele Produkte nicht klar einer Kategorie zugeordnet werden können und es noch an rechtlich eindeutigen Kriterien mangelt, wie ein solches Produkt überhaupt klassifiziert wird.

VERANTWORTLICHKEIT ALS KERNPROBLEM FÜR OPEN SOURCE

Ein zentrales Problem für Open-Source-Projekte ist die Frage der Verantwortlichkeit. Wer als Maintainer eine Bibliothek pflegt, wird möglicherweise als Hersteller eingestuft, wenn dies in einem kommerziellen Kontext geschieht und Geld damit verdient wird – mit allen rechtlichen Pflichten. Diese Verantwortung lässt sich kaum erfüllen, wenn das Projekt auf Freiwilligenarbeit basiert.

Wer ist bei einer Schwachstelle verantwortlich? Der ursprüngliche Autor, der aktuelle Maintainer, der Paketbetreiber – oder am Ende derjenige,

Bild: Tondone | wetzkaz - stock.adobe.com

der das Gesamtpaket integriert? In der Praxis könnte dies dazu führen, dass Entwicklerinnen und Entwickler ihre Projekte nicht mehr veröffentlichen oder pflegen – aus Angst vor regulatorischen Konsequenzen.

Ein weiteres Spannungsfeld ergibt sich aus der CRA-Forderung nach fortlaufendem Support und Updates über den gesamten Produktlebenszyklus. Doch viele Open-Source-Komponenten sind Ein-Personen-Projekte oder werden von kleinen Teams gepflegt. Die Erwartung, langfristig Sicherheitsupdates zu garantieren, steht im Widerspruch zur realen Kapazität vieler Maintainer.

UNKLARE GRENZEN BEI DER MONETARISIERUNG

Viel hängt also davon ab, ob mit einem Projekt Geld verdient wird oder nicht. Aber genau hier gibt es noch zahlreiche offene Fragen. Bin ich Hersteller, wenn ich um Spenden werbe? Oder muss Geld fließen? Gelten meine Lebensunterhaltskosten schon zum „Verdienen" oder nicht? Was, wenn ich Support anbiete für ein Projekt, bei dem ich nicht Maintainer bin? Wie sieht es aus, wenn sich das aber später ändert und man mich zu einem Maintainer macht? Was ist überhaupt ein Maintainer? Ist reiner Quellcode ein Produkt oder wird es das erst durch die Verbreitung von Binaries? Und wie behandeln wir dann interpretierte Sprachen?

Viele dieser Fragen sind bislang offen. Zwar soll die angekündigte EU-Guidance künftig für mehr Orientierung sorgen, doch bis dahin bleibt ein gewisses Maß an Unsicherheit bestehen.

SOFTWARE BILL OF MATERIALS ALS NEUE ANFORDERUNG

Eine der zentralen Anforderungen des CRA ist die Einführung einer Software Bill of Materials (SBOM). Sie soll offenlegen, aus welchen Komponenten ein Produkt besteht. Das ist sinnvoll, und im Open-Source-Bereich zudem leichter umzusetzen als bei proprietärer Software, weil sich alle Informationen einsehen lassen. Dennoch besteht auch hier Unsicherheit durch viele offene Detailfragen. Wird ein SBOM-Format vorgeschrieben? Gibt es bestimmte verpflichtende Elemente? Bis zu welcher Tiefe muss ich eine SBOM liefern und an wen? Letztlich gibt es leider auch keine eindeutigen Standards zur Identifikation von Software.

Unternehmen, die Open Source nutzen – ob als Teil eigener Produkte oder als Infrastruktur – sind ebenfalls in der Pflicht. Sie müssen künftig dokumentieren, welche Komponenten benutzt werden, wie Sicherheitsupdates integriert werden und wie auf Schwachstellen reagiert wird. Die Zeiten, in denen Open Source einfach so verwendet wurde, ohne Governance-Strukturen, sind vorbei. Der CRA macht die Open-Source-Nutzung zu einer Compliance-Frage – mit direktem Einfluss auf Risiko, Haftung und unternehmerische Verantwortung.

Besonders kleine und mittlere Unternehmen stehen damit unter Druck. Sie verfügen oft nicht über eigene Security-Teams. Die EU-Kommission ist gefordert, für diesen Bereich realistische Umsetzungshilfen zu schaffen, etwa durch standardisierte Templates, geförderte Beratung oder zentrale Zertifizierungsstellen. Zudem müssen die Plattformen einbezogen werden: GitHub, GitLab, Maven Central oder PyPI haben eine Schlüsselrolle in der Open-Source-Verbreitung. Sie könnten helfen, SBOMs zu standardisieren, Sicherheitswarnungen zu verbreiten und Verwaltungsinformationen (Stewardship-Informationen) sichtbar zu machen – ohne selbst zu Herstellern zu werden.

HANDLUNGSEMPFEHLUNGEN FÜR UNTERNEHMEN

Damit der CRA sein Ziel nicht verfehlt, braucht es eine differenzierte Umsetzung. Unternehmen, die Open Source nutzen, müssen ihre interne Governance professionalisieren – mit SBOM-Tools, Patch-Strategien und klaren Verantwortlichkeiten. Gleichzeitig sollte die EU gezielt Strukturen fördern, die Open-Source-Projekte bei der Umsetzung des CRA unterstützen – etwa durch Rechtshilfen, Audit-Tools oder Koordinationsstellen. Die Community ist bereit, Verantwortung zu übernehmen – sie braucht dafür aber verlässliche Rahmenbedingungen und Unterstützung.

Unternehmen, die Open Source einsetzen, sollten jetzt aktiv werden. Zunächst gilt es, Transparenz zu schaffen: Welche Open-Source-Komponenten sind im Einsatz? Wer ist intern verantwortlich für deren Integration, Pflege und Aktualisierung? Eine dokumentierte Übersicht, idealerweise unterstützt durch automatisierte Werkzeuge zur SBOM-Erstellung, ist ein erster wichtiger Schritt. Darüber hinaus sollten Prozesse definiert werden, wie auf entdeckte Schwachstellen reagiert wird, etwa mit klaren Zuständigkeiten, Zeitvorgaben und Kommunikationswegen. Für sicherheitskritische Systeme empfiehlt sich ein regelmäßiger Abgleich mit bekannten Sicherheitsdatenbanken wie der CVE-Datenbank oder EUVD sowie gegebenenfalls ein Notfallplan für Patches und Updates.

Auch die Zusammenarbeit mit den Open-Source-Communities sollte aktiv gepflegt werden. Unternehmen, die auf freie Software setzen, sollten sich nicht nur als Nutzer, sondern als Partner begreifen – etwa durch Bug-Reports, Code-Reviews oder gezielte finanzielle Unterstützung. Denn nur ein stabiles, resilientes Open-Source-Ökosystem kann langfristig den regulatorischen Anforderungen standhalten.

Schließlich lohnt es sich, das eigene Compliance-Management auf den Prüfstand zu stellen. Viele Anforderungen des CRA lassen sich mit bestehenden Strukturen aus der IT-Sicherheitszertifizierung oder dem Datenschutzmanagement verknüpfen – vorausgesetzt, sie werden bewusst integriert und nicht als paralleles System aufgebaut. So wird aus der regulatorischen Pflicht ein unternehmerischer Vorteil.

Der Cyber Resilience Act wird die Sicherheitsstrategie der Europäischen Union entscheidend stärken. Unser oberstes Ziel in der Expertengruppe der Europäischen Kommission ist es aktuell, einen für alle Seiten zufriedenstellenden Mittelweg zwischen Effizienz und Bürokratie zu finden. Das Gerüst steht, und in den kommenden Monaten werden wir uns intensiv mit allen offenen Fragen beschäftigen. Das Ziel ist klar: ein Europa, das sicher, wettbewerbsfähig und auf die Zukunft vorbereitet ist. ■

LARS FRANCKE
ist Mitgründer und CTO von Stackable sowie Mitglied der Expertengruppe zum Cyber Resilience Act.

Wie Unternehmen ihre Systeme schützen können

ABWEHRSTRATEGIEN GEGEN ANGRIFFE MIT KI

Mit KI-gestützten Methoden verschaffen sich Angreifer neue Möglichkeiten, Sicherheitsmechanismen gezielt zu umgehen. Unternehmen stehen vor der Aufgabe, ihre Schutzkonzepte kontinuierlich zu überprüfen und flexibel anzupassen. Continuous Threat Exposure Management rückt dabei als praxisnaher Ansatz in den Fokus, um Sicherheitslücken systematisch zu erkennen und Risiken frühzeitig zu mindern.

Mittlerweile hat auch der größte Skeptiker erkannt: An künstlicher Intelligenz (KI) führt kein Weg mehr vorbei. Egal ob es um Chatbots im Kundenservice, Predictive Maintenance in der Industrie, Betrugserkennung im Finanzwesen, Kreditrisikobewertung, Sprachassistenten oder Smarthome-Anwendungen geht – die Liste an KI-Helfern ist schier endlos, und mit den um sich greifenden technologischen Fortschritten und der zunehmenden Verfügbarkeit von Daten erschließen sich immer neue Anwendungsgebiete. Für die Cybersicherheit gilt in diesem Zusammenhang, was auch andere Bereiche beschäftigt: Künstliche Intelligenz ist Fluch und Segen zugleich. Sie hilft, Systeme sicherer zu machen, kommt aber auch vermehrt bei Cyberangriffen zum Einsatz. Es ist höchste Zeit, Verteidigungsstrategien zu entwickeln, die Attacken mit KI etwas entgegensetzen.

KI IM FIRMENEINSATZ

Nach Angaben von Next Move Strategy Consulting wird der Markt für künstliche Intelligenz in den kommenden zehn Jahren deutlich wachsen: Der derzeitige Wert von fast 100 Milliarden US-Dollar könnte sich bis 2030 auf nahezu zwei Billionen US-Dollar verzwanzigfachen. Auch Learn-Bonds erwartet einen kräftigen Zuwachs und prognostiziert, dass der Umsatz mit KI-Software bis 2025 auf über 126 Milliarden US-Dollar steigt, verglichen mit 22,6 Milliarden US-Dollar im Jahr 2020. Zudem wird angenommen, dass künftig jeder fünfte Beschäftigte Teile seiner Arbeit an KI abgeben muss. Eine Analyse von McKinsey kommt zu dem Ergebnis, dass KI-Technologien das Potenzial haben, die globale Wirtschaftsleistung bis 2030 jährlich im Durchschnitt um 1,2 Prozent zu steigern.

Laut ifo Institut setzen derzeit 13,3 Prozent der deutschen Unternehmen KI ein, während 9,2 Prozent den Einsatz planen; weitere 36,7 Prozent diskutieren noch über mögliche Anwendungsfelder. Häufige Einsatzgebiete in Unternehmen sind dabei die Automatisierung von Geschäftsprozessen, die Datenanalyse zur Entscheidungsfindung sowie die Steigerung von Produktqualität und -leistung. Gleichzeitig gibt es auch Bedenken hinsichtlich möglicher negativer Folgen der KI-Welle: Knapp zwei Drittel der Deutschen sorgen sich um den Verlust von Arbeitsplätzen, und insgesamt 45 Prozent stehen laut einer YouGov-Umfrage dem Einsatz von KI skeptisch gegenüber.

Eine weitere Schattenseite der technologischen Entwicklung, die neben vielen positiven Errungenschaften mit der Nutzung von KI einhergehen kann, sind zunehmende und immer gefährlichere Cyberangriffe. Waren bislang oft ein hohes Maß an IT-Know-how, viel Zeit und Aufwand vonnöten, um einen Angriff zu lancieren, können mithilfe von KI heute schon Laien mit wenigen Klicks zum Hacker werden. Unternehmen und Behörden stehen vor der Herausforderung, dieser Entwicklung entschlossen zu begegnen.

DOPPELROLLE DER KI

Künstliche Intelligenz bietet zahlreiche Vorteile für die Cybersicherheit. Dazu zählen verbesserte Bedrohungsanalysen sowie eine präzisere Identifizierung möglicher Angriffsvorläufer, die es erlauben, Bedrohungen frühzeitig zu erkennen. Ebenso trägt KI zu einer optimierten Zugriffskontrolle und sichereren Passwort-Praktiken bei. Unternehmen profitieren außerdem von einer effizienteren Minimierung und Priorisierung von Risiken, was Ressourcen gezielter einsetzbar macht. Hinzu kommt die Fähigkeit zur automatisierten Erkennung von Bedrohungen, die Sicherheitsverantwortliche entlastet. Nicht zuletzt kann der Einsatz von KI die Effizienz und Effektivität der Mitarbeitenden deutlich steigern, indem Routineaufgaben automatisiert und relevante Informationen schneller aufbereitet werden.

Trotz aller Vorteile bringt die künstliche Intelligenz auch erhebliche Herausforderungen mit sich. So bestehen teilweise Schwierigkeiten hinsichtlich der Verlässlichkeit und Genauigkeit von Analyseergebnissen, was Fehleinschätzungen begünstigen kann. Zudem gibt es Bedenken im Hinblick auf Datenschutz und Datensicherheit, besonders wenn große Datenmengen verarbeitet werden. Auch die mangelnde Transparenz vieler KI-Modelle erschwert es, Entscheidungen nachvollziehbar zu machen. Schließlich können verzerrte Trainingsdaten oder fehlerhafte Algorithmen dazu führen, dass Systeme falsche Schlüsse ziehen und damit neue Risiken entstehen.

WIE SETZEN CYBERKRIMINELLE KI EIN?

Cyberkriminelle nutzen künstliche Intelligenz zunehmend für raffinierte Angriffe. Social Engineers setzen KI ein, um präzisere Phishing-Kampagnen zu entwickeln und täuschend echte Deepfakes zu erstellen, die Betroffene gezielt in die Irre führen. Angreifer verlassen sich zudem auf KI-gestützte Techniken zur Passwort-Vorhersage und knacken automatisiert CAPTCHA-Systeme, um sich unbefugten Zugriff auf sensible Daten zu verschaffen. Moderne Hacker agieren inzwischen extrem schnell und entwickeln ständig neue Methoden. Unternehmen haben oft Mühe, Sicherheitskontrollen zu automatisieren oder zeitnah Sicherheitspatches einzuspielen, um Schritt zu halten. Gefragt ist daher ein Programm für das kontinuierliche Management von Bedrohungen, das die gravierendsten Risiken frühzeitig erkennt und priorisiert.

KI bildet insgesamt die Grundlage für immer neue Angriffsvektoren, die zunehmend automatisiert ablaufen und es Hackern ermöglichen, Attacken in bislang unerreichtem Umfang zu skalieren. Die folgenden Angriffsmuster setzen Cyberkriminelle zum Beispiel mit KI um:

- **Phishing und Social Engineering:** KI wird verwendet, um personalisierte und überzeugende Phishing-E-Mails zu erstellen. Diese können Mitarbeitende dazu verleiten, sensible Informationen preiszugeben oder bösartige Links zu öffnen.
- **Adversarial Attacks:** Kriminelle können KI verwenden, um speziell manipulierte Daten zu generieren, die dafür sorgen, dass KI-Systeme wie etwa Bilderkennungs-Tools oder Sicherheitsmechanismen fehlerhafte oder unerwartete Entscheidungen treffen.
- **Automatisierte Angriffe:** KI-gesteuerte Bots können automatisch Schwachstellen in Systemen erkennen, Exploits ausnutzen und Angriffe durchführen – ganz ohne menschliches Eingreifen.
- **Erkennung von Sicherheitslücken:** Mittels KI lassen sich große Datenmengen analysieren und potenzielle Sicherheitslücken in Systemen oder Netzwerken identifizieren, die dann für Angriffe ausgenutzt werden.
- **Verschleierung von Malware:** KI hilft, Malware zu entwickeln, die schwer zu erkennen ist, weil sie ihre Eigenschaften an die Umgebung anpasst oder sich eigenständig verändert, um herkömmliche Sicherheitsmechanismen zu umgehen.

Allerdings können Unternehmen künstliche Intelligenz auch für ihre Zwecke nutzen und Ha-

Bild: our_future | Autism in Focus - stock.adobe.com

cker mit den eigenen Waffen schlagen, denn KI kann zur Verteidigung von Systemen und Daten dienen. Mithilfe von KI-Tools lassen sich viele Angriffe frühzeitig erkennen und automatisch Gegenmaßnahmen ergreifen, um die Auswirkungen zu minimieren. Beispiele sind die bereits erwähnten verbesserten Zugriffskontrollen, Bedrohungsanalysen oder die Priorisierung von Risiken.

GANZHEITLICHER SCHUTZANSATZ NOTWENDIG

Mit einer einzigen Lösung oder Firewall ist es nicht getan: Wer seine Systeme, Daten und Mitarbeiter wirklich nachhaltig vor KI-gestützten Angriffen schützen will, benötigt eine Kombination aus technischen Lösungen, Schulungen und proaktiven Sicherheitsstrategien. So muss einerseits die Belegschaft in speziellen Security-Awareness-Trainings für die Risiken KI-gestützter Angriffe sensibilisiert werden. Mitarbeiter sollten in der Lage sein, verdächtige Aktivitäten zu erkennen und angemessen darauf zu reagieren.

Zudem braucht es klare Sicherheitsrichtlinien und Verfahren, um KI-Technologien sicher einzusetzen und potenzielle Angriffe abzuwehren. Dies umfasst Vorgaben für den Zugriff auf sensible Daten, die Nutzung von KI-Tools und den Umgang mit verdächtigen Aktivitäten. Hinzu kommen die kontinuierliche Überwachung und die Analyse des Netzwerkverkehrs, der Systemaktivitäten und anderer Indikatoren auf potenzielle Angriffe, um ungewöhnliche Vorgänge frühzeitig zu erkennen und zu unterbinden.

Ein weiterer wichtiger Baustein ist der Einsatz technischer Sicherheitsmaßnahmen. Dazu zählen Tools zur Erkennung und Abwehr von Angriffen wie Intrusion-Detection-Systeme (IDS), Intrusion-Prevention-Systeme (IPS), Firewalls, Antiviren-Programme und Endpoint-Sicherheitslösungen. Ebenso entscheidend sind regelmäßige Updates von Software und Betriebssystemen, um Sicherheitslücken zu schließen und mögliche Angriffspunkte zu verringern. Auch Angriffssimulationen und Penetrationstests tragen dazu bei, die Widerstandsfähigkeit eines Unternehmens gegen KI-gestützte Attacken zu prüfen und Schwachstellen aufzudecken. Ein weiterer wesentlicher Aspekt einer ganzheitlichen Sicherheitsstrategie ist die enge Zusammenarbeit mit anderen Unternehmen, Behörden oder Organisationen. Der regelmäßige Austausch von Informationen über neue Bedrohungen, Angriffsmethoden und bewährte Sicherheitspraktiken ermöglicht es, von den Erfahrungen anderer zu profitieren und die eigene Verteidigung kontinuierlich zu verbessern.

CONTINUOUS THREAT EXPOSURE MANAGEMENT

Im Kontext der Abwehr von KI-basierten Cyberangriffen rückt zunehmend der Ansatz des Continuous Threat Exposure Management (CTEM) in den Fokus. Mit diesem Konzept können Organisationen ihre Sicherheitsstrategien an ständig wechselnde Bedrohungen anpassen und schnelle, wirksame Reaktionsmöglichkeiten entwickeln. CTEM unterstützt eine kontinuierliche Überwachung und Bewertung von Risiken und Schwachstellen und ermöglicht es, die Exposition eines Unternehmens gegenüber potenziellen Gefahren laufend neu einzuschätzen, zu steuern und zu minimieren.

Anders als traditionelle Überwachungsansätze, die häufig rein reaktiv arbeiten, setzt CTEM auf proaktive und permanente Analyse, um Bedrohungen frühzeitig zu identifizieren und gezielt Gegenmaßnahmen einzuleiten. Laut einer Prognose von Gartner könnten Unternehmen, die ihre Investitionen in der Cybersecurity auf Grundlage eines CTEM-Programms priorisieren, bis 2026 die Zahl ihrer Sicherheitsvorfälle um mehr als 60 Prozent senken.

Fünf zentrale Maßnahmen tragen zu einem effektiven CTEM bei:

1. **24/7-Überwachung:** Zunächst einmal sollten Organisationen ihre Netzwerke, Systeme, Anwendungen und Daten, kontinuierlich überwachen, denn nur so können sie potenzielle Sicherheitsbedrohungen früh genug erkennen.

2. **Risiken bewerten und priorisieren:** Sicherheitsrisiken lassen sich gezielt angehen, wenn sie nach Bedrohungspotenzial, möglichen Auswirkungen und Eintrittswahrscheinlichkeit bewertet und priorisiert werden. So werden Ressourcen dort eingesetzt, wo sie den größten Schutz bieten.

3. **Abläufe automatisieren:** Moderne Automatisierungslösungen und Analysetechniken wie maschinelles Lernen oder künstliche Intelligenz helfen, große Datenmengen effizient zu verarbeiten und ungewöhnliche Aktivitäten frühzeitig zu identifizieren.

4. **Bedrohungsdaten integrieren:** Daten aus unterschiedlichen Quellen – etwa Sicherheitsinformationen und -ereignissen, Threat-Intelligence-Feeds oder Schwachstellenmanagement – sollten zusammengeführt werden, um ein umfassendes Bild der Sicherheitslage zu erhalten.

5. **Kontinuierlich anpassen:** Sicherheitsmaßnahmen müssen regelmäßig überprüft und angepasst werden, um aktuelle Bedrohungen oder Taktiken abwehren zu können – besonders angesichts der dynamischen Entwicklung von KI-Technologien, die fast täglich neue Angriffsmethoden hervorbringen können.

FAZIT

Künstliche Intelligenz wird künftig eine immer größere Rolle in der Cybersicherheit spielen. Sie hat das Potenzial, IT- und Security-Teams zu unterstützen, Innovationen voranzutreiben und die Informationssicherheit spürbar zu stärken. Gleichzeitig stehen Unternehmen und Behörden vor der Aufgabe, Cyberkriminellen entschlossen entgegenzutreten, die KI für ihre Angriffe nutzen. Letztlich liegt es an uns Menschen, ob KI als „good guy" oder „bad guy" eingesetzt wird. ■

ELMAR TÖRÖK
ist Strategic Consultant Microsoft Cloud bei der SITS Deutschland GmbH.
E-Mail: elmar.toeroek@sits.com
Weitere Informationen: sits.com

Schnittstellen als Einfallstor in die interne IT?

WIE BEDROHUNGS-MODELLIERUNG DIE SICHERE IMPLEMENTIERUNG VON SCHNITTSTELLEN FÖRDERT

Bei einem Penetrationstest eines Onlineshops zeigte sich ein alarmierendes Bild: Das System bot nicht nur direkte Angriffsflächen, sondern ermöglichte über unzureichend gesicherte Schnittstellen auch den Zugriff auf interne Enterprise-Resource-Planning-(ERP)- und Business-Intelligence-(BI)-Systeme. Threat Modeling kann solche Schwachstellen frühzeitig identifizieren und absichern.

Bild: ImageFlow | Maryna • stock.adobe.com

Oftmals sind Webanwendungen nur ein Nebengeschäft oder dienen einem Marketingzweck, sei es der Onlineshop als Ergänzung zum stationären Handel oder die Webseite als digitale Visitenkarte. In der Praxis werden solche Systeme daher häufig als Projekt betrachtet, das nach dem Go-live abgeschlossen ist. Die zur Verfügung stehenden finanziellen und personellen Ressourcen werden anschließend weitestgehend zurückgefahren. Selten gibt es einen Pentest oder einen Wartungsvertrag, der alle Sicherheitsaspekte adäquat abdeckt. So geht von der einst mühevoll aufgebauten Webanwendung schnell ein hohes Sicherheitsrisiko aus.

Besonders kritisch wird es, wenn solche Systeme über Schnittstellen mit internen Anwendungen verbunden sind. Was beim isolierten Website-Baukasten eines Massenhosters für manche Betreiber vertretbar wirkt, wird beispielsweise bei einem Onlineshop schnell zum Potenzial für Reputationsschäden und Datenschutzverletzungen:

- personenbezogene Daten von Kunden,
- sensitive Unternehmensinformationen wie Umsätze oder Kostenstruktur,
- Schnittstellen zur Übertragung von Bestellungen in das ERP-System.

HERAUSFORDERUNGEN BEI DER SCHNITTSTELLENENTWICKLUNG

Es liegt in der Natur der Sache, dass bei der Implementierung von Schnittstellen zwei unterschiedliche Domänen auf einen gemeinsamen Nenner gebracht werden müssen. In der Idealvorstellung sind die beteiligten Personen mit beiden Domänen vertraut und wissen schon in der Konzeptionsphase, worauf es zu achten gilt und welche Besonderheiten die Systeme haben. In der Praxis häufiger anzutreffen ist jedoch einseitiges Domänenwissen: Während die Onlineshop-Agentur bestens mit dem Shopsystem vertraut ist, kennt der ERP-Berater jeden Winkel seines ERP-Systems. Sind dann noch unterschiedliche Infrastrukturbetreiber wie die interne IT für die demilitarisierte Zone (DMZ) und der Hoster für die Webanwendung beteiligt, steigen Kommunikations-Overhead, Komplexität und Fehleranfälligkeit weiter an.

Die Entwicklung von Schnittstellen wird dadurch häufig zur Kompromisslösung: Man beschäftigt sich genauso viel (oder wenig) mit dem anderen System, wie es für die Lösung der konkreten Aufgabe notwendig ist. Das kann zu zahlreichen Problemen und Angriffsvektoren führen, unter anderem:

- falsch konfigurierte Zugriffsberechtigungen,
- Systemausfälle aufgrund zu hoher Schnittstellenlast,
- unnötig offene Ports in die DMZ,
- Cross-Site-Scripting oder andere Injections aufgrund von Unterschieden bei der Datenvalidierung und -bereinigung,
- Datenlecks durch fälschlicherweise offene Endpunkte.

Häufig liegen die Ursachen hierfür nicht in mangelnden technischen Fähigkeiten, sondern in fehlendem Systemverständnis, Missverständnissen bei der Kommunikation oder unklaren Zuständigkeiten.

BEDROHUNGEN SYSTEMATISCH IDENTIFIZIEREN

Wann immer es um Risiken geht, lautet die Standardantwort: Risikomanagement nach dem Risk-Management-Lifecycle (Risikoidentifizierung, Risikobewertung, Risikobehandlung und Risikokontrolle). Für den gezielten Umgang mit Bedrohungen existiert jedoch eine spezifischere Methodik: das Threat Modeling.

Dabei handelt es sich um einen strukturierten Ansatz, um Bedrohungen zu identifizieren, zu verstehen und zu behandeln. Die „Open Web Application Security Project (OWASP)"-Foundation definiert mit dem „Four Questions Framework" einen strukturierten Ansatz für den Aufbau eines Bedrohungsmodells:

- Umfang und Kontext definieren: „Woran arbeiten wir?"
- Bedrohungen identifizieren: „Was kann schiefgehen?"
- Maßnahmen festlegen: „Was werden wir dagegen tun?"
- Maßnahmen bewerten: „Haben wir gute Arbeit geleistet?"

Bedrohungen entstehen besonders beim Datenaustausch – einschließlich Metadaten wie HTTP-Request-Informationen. Daher bilden Datenflussdiagramme eine gute Basis für den Aufbau eines Threat Models. In einem oberflächlichen Diagramm lassen sich grundlegend die beteiligten Prozesse, Entitäten und Datenspeicher ablesen (siehe Abbildung 1).

Vertrauensstufen (Trust Levels) definieren die Berechtigungen von Entitäten und Prozessen. Ein Onlineshop läuft beispielsweise als www-data-Systembenutzer, während das ERP-System einen

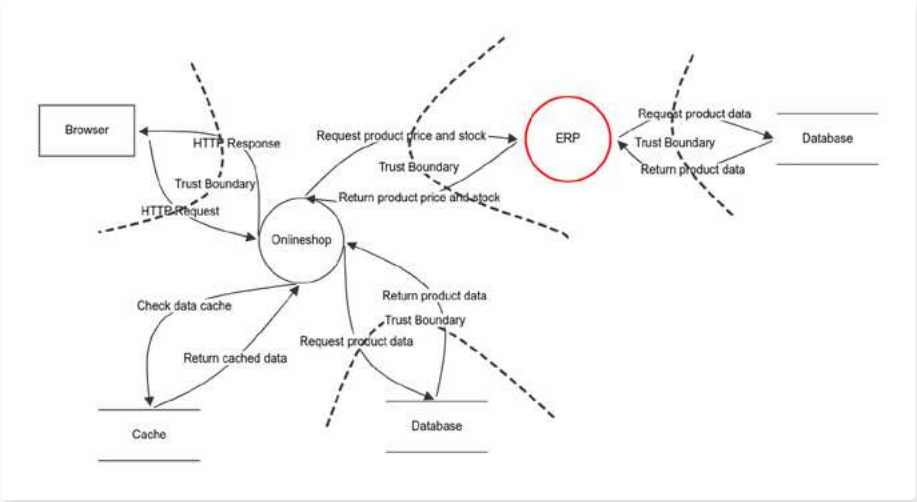


Abbildung 1: Darstellung eines beispielhaften und einfach gehaltenen Threat Models einer Schnittstelle zwischen Onlineshop und ERP aus Threat Dragon (https://owasp.org/www-project-threat-dragon/). (Bild: Dev Specialists GmbH)

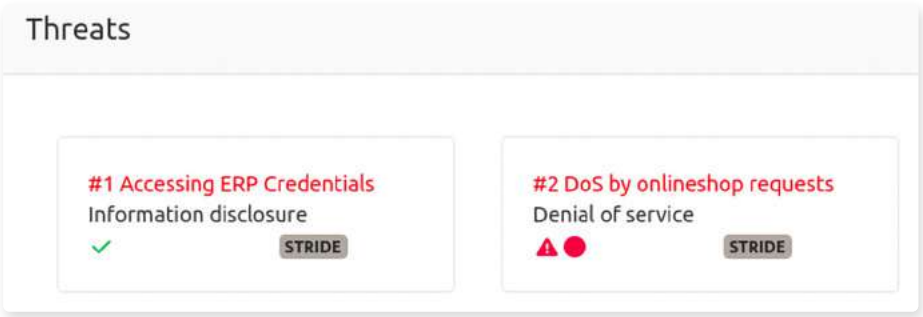


Abbildung 2: Darstellung von beispielhaften Risiken am ERP-Prozess aus Threat Dragon. (Bild: Dev Specialists GmbH)

speziellen Schnittstellenbenutzer benötigt. Ändern sich die Trust Levels, wird dies über Vertrauensgrenzen (Trust Boundaries) kenntlich gemacht, die dadurch kritische Datenflüsse kennzeichnen.

Auf Basis von Klassifikationsmodellen wie STRIDE oder LINDDUN lassen sich nun spezifische Bedrohungen für Entitäten, Prozesse und Datenspeicher definieren (siehe Abbildung 2). In detaillierteren Modellen können auch komplexere Architekturen wie Microservices abgebildet werden.

PRAKTISCHER NUTZEN VON THREAT MODELS

Ein Threat Model vereint Infrastruktur, Architektur und Datenflüsse und ermöglicht die systematische Klassifikation von Bedrohungen. Als Anbieter einer Schnittstelle, die von Dritten genutzt und implementiert wird, lassen sich Risiken sowohl in einem allgemeinen als auch in einem spezifischen Kontext – beispielsweise endpunktbezogen – modellieren und Vorgaben zur Mitigation ableiten.

Eine typische Bedrohung ergibt sich aus dem Umgang mit den Zugangsdaten für Schnittstellen. Gerade in Onlineshops und ähnlichen Anwendungen sind diese unverschlüsselt in Konfigurationsdateien, in der Datenbank oder leider auch hartkodiert im Quelltext zu finden. Klare Vorgaben zur Risikominderung, die bereits im Threat-Modeling-Prozess definiert werden, können hier Abhilfe schaffen.

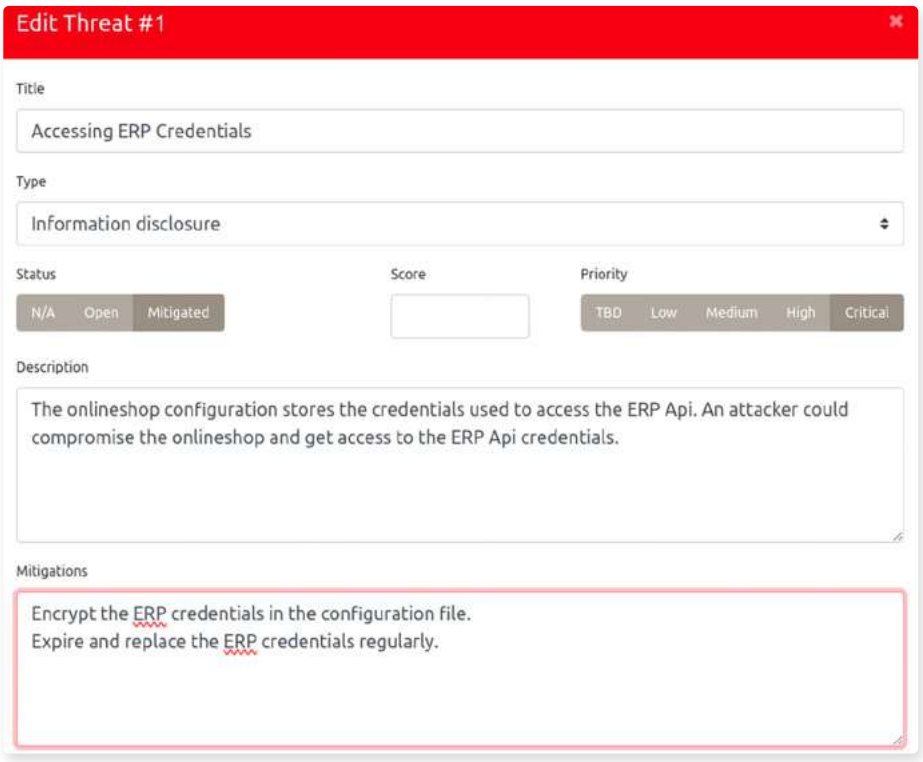


Abbildung 3: Bearbeitungsfenster eines beispielhaften Risikos in Threat Dragon. (Bild: Dev Specialists GmbH)

Anstatt nur auf Anbietervorgaben zu setzen, können Implementierer Bedrohungen auch eigenverantwortlich adressieren. Das Threat Model hilft hier bei der Schaffung von Awareness für die Besonderheiten des Systems, als Fahrplan zur Schnittstellenabsicherung und zur Dokumentation der Mitigation.

Grundsätzlich ist jedoch zu beachten, dass die Menge an Bedrohungen, die durch den Implementierer mitigiert werden müssen, minimal zu halten ist. Threat Models dürfen nicht zum Instrument werden, die eigene Verantwortung an Dritte abzuwälzen. Eine Delegation an den Entwickler darf nur bei Bedrohungen erfolgen, bei denen der Anbieter keine andere Mitigationsmöglichkeit hat.

Auch mit einem umfassenden Bedrohungsmodell bleiben externe Sicherheitstests unverzichtbar. Die implementierten Schutzmaßnahmen müssen überprüft werden, und die unabhängige Perspektive kann neue Bedrohungen aufdecken, die das Modell weiter verbessern.

FAZIT: MEHR ALS EIN PAPIERTIGER

Threat Models erscheinen zunächst als zusätzlicher bürokratischer Aufwand. Richtig eingesetzt entwickeln sie sich jedoch zu wirksamen Werkzeugen für bessere Anwendungssicherheit. Besonders für externe Entwickler bieten sie erhebliche Vorteile: Sie schaffen Systemverständnis, liefern Handlungsempfehlungen und definieren klare Anforderungen. So verhindern sie, dass Schnittstellen zum Einfallstor in die interne IT werden. ■

DOMINIK STRAUSS
ist CEO und Senior Solutions Architect bei der Dev Specialists GmbH.

Mehr Risikobewusstsein notwendig

WARUM KRANKENHÄUSER BEI CYBERVERSICHERUNGEN UNTERVERSORGT SIND

Bild: Eshana | redflower - stock.adobe.com

Cyberangriffe bedrohen zunehmend den Klinikbetrieb in Deutschland. Doch viele Krankenhäuser sind noch immer nicht ausreichend versichert – oft aus Kostengründen oder wegen zu hoher Anforderungen der Versicherer. Entscheidend für besseren Schutz sind ein realistischer Blick auf die eigene Risikolage und ein enger Dialog mit Anbietern.

Cyberangriffe haben sich zu einer ernsthaften Bedrohung für Krankenhäuser entwickelt. Zwischen 2020 und 2024 stieg die Zahl erfolgreicher Attacken um 74 Prozent, wie eine aktuelle Auswertung des Hasso-Plattner-Instituts zeigt.[1] Die Vorfälle reichen von klassischen Ransomware-Attacken bis hin zu Erpressungsversuchen ohne Datenverschlüsselung, berichtet das Fachportal Krankenhaus-IT.[2]

Trotz dieser alarmierenden Entwicklung verfügen längst nicht alle Krankenhäuser über einen angemessenen Versicherungsschutz gegen Cyberrisiken. Dafür gibt es verschiedene Ursachen: Einige Kliniken werden von Versicherern als zu risikobehaftet eingestuft, andere bewerten die angebotenen Prämien als zu hoch oder haben sich mit dem Thema bisher nicht intensiv auseinandergesetzt.

UNTERSCHIEDLICHE REIFEGRADE BEI DEN EINRICHTUNGEN

Insgesamt ist das Bewusstsein für Cyberrisiken in den vergangenen Jahren gestiegen. Krankenhäuser investieren vermehrt in IT- und OT-Sicherheitsmaßnahmen. Gerade kleinere Einrichtungen weisen jedoch oft erhebliche Defizite beim Schutz ihrer IT-Infrastruktur auf. Notwendige Investitionen in Technik, Personal und Prozesse bleiben hier häufig aus.

Der Druck auf Krankenhäuser nimmt zu – nicht nur wegen steigender Risiken, sondern auch durch zunehmende gesetzliche Vorgaben zur Umsetzung wirksamer Sicherheitsmaßnahmen. Die EU-Richtlinie „Network and Information Security" (NIS-2) hätte in Deutschland bis Oktober 2024 umgesetzt sein müssen. Dies ist bislang jedoch nicht erfolgt. Experten erwarten, dass das NIS-2-Umsetzungsgesetz frühestens im Herbst 2025 in Kraft tritt.

Krankenhäuser, die unter die NIS-2-Richtlinie fallen, sind dann verpflichtet, umfassende Cybersicherheitsmaßnahmen umzusetzen, einschließlich der Einführung eines effektiven Risikomanagements. Unter die Richtlinie fallen Krankenhäuser, die als kritische Infrastrukturen oder wichtig für die öffentliche Gesundheit eingestuft werden. Betroffen sind vor allem große Krankenhäuser mit umfassenden Versorgungs-

Welche Herausforderungen müssen bei einem Cyberangriff bewältigt werden?

Die sechs Hauptherausforderungen bei Cyberangriffen im Gesundheitssektor erfordern einen ganzheitlichen Ansatz: Von der Patientenversorgung über IT-Wiederherstellung bis hin zum Reputationsmanagement müssen Einrichtungen auf verschiedenen Ebenen gleichzeitig reagieren. (Bild: Relyens)

aufgaben. Je nach nationaler Umsetzung können auch mittelgroße und kleinere Kliniken einbezogen werden, wenn sie in Bereichen tätig sind, die als systemrelevant gelten.

KOMPLEXE RISIKOSITUATION IN KLINIKEN

Krankenhäuser stehen vor besonderen Herausforderungen in der IT-Sicherheit. Sie verarbeiten hochsensible Gesundheitsdaten, die für Kriminelle besonders interessant und deutlich wertvoller sind als einfache personenbezogene Informationen. Gleichzeitig gilt ihre IT-Infrastruktur als überaus angreifbar. Neben klassischen Geräten wie PCs, Servern und Druckern sind auch zahlreiche medizinische Systeme im Einsatz, die häufig mit veralteter Software betrieben werden und dadurch zusätzliche Schwachstellen aufweisen.

Erschwerend kommt der Mangel an personellen und finanziellen Ressourcen hinzu: Viele Einrichtungen verfügen nicht über ausreichend Fachkräfte, um ihre IT-Systeme umfassend zu betreuen, Sicherheitsüberprüfungen durchzuführen oder Mitarbeiter regelmäßig zu schulen. Ein weiteres Risiko stellen externe Dienstleister dar – sie werden zunehmend zum Einfallstor für Angriffe.

MEDIZINTECHNIK ALS BESONDERE HERAUSFORDERUNG

Während klassische IT-Produkte häufig durch marktübliche Sicherheitslösungen geschützt werden können, stellen vernetzte Medizingeräte und Betriebstechnik die Kliniken vor größere Herausforderungen. So kann es etwa vorkommen, dass ein Medizingerät ein proprietäres Betriebssystem nutzt und der Hersteller keine Installation von Virenschutzsoftware zulässt. Für Versicherer ist in solchen Fällen entscheidend, ob und wie sich das Krankenhaus mit den besonderen Risiken dieser Geräte auseinandergesetzt hat – ein wichtiger Indikator für das Sicherheitsbewusstsein der Einrichtung.

Aus Sicht eines Versicherers ist das Thema Cybersicherheit im Krankenhaus herausfordernd: Viele Kliniken können nicht transparent darlegen, wie gut ihre Cybersicherheit tatsächlich ist. Für Versicherer ist es daher sehr schwierig, das Gefahrenpotenzial realistisch einzuschätzen, zumal die traditionelle Kalkulation auf Basis historischer Schadendaten hier nicht funktioniert.

Daher ist die Cyberversicherung nicht vergleichbar mit anderen Versicherungssparten. Neben der unklaren Risikosituation und der zunehmenden Anzahl von Schäden kommt noch ein sogenanntes Kumulrisiko hinzu: Bei einem Hackerangriff können mehrere Krankenhäuser in verschiedenen Städten und verschiedener Trägerschaft betroffen sein, etwa wenn Kriminelle mehrere Krankenhäuser gleichzeitig angreifen oder dieselbe Software-Schwachstelle ausnutzen. Viele Versicherer machen daher um das Thema Cyberversicherung einen großen Bogen. Aufgrund der schwierigen Voraussetzungen bieten in Deutschland daher nur wenige Anbieter Versicherungen gegen Cyberangriffe für Krankenhäuser an.

WEGE ZU BESSERER ABSICHERUNG

Damit Krankenhäuser versichert werden können, braucht es bessere Risikoanalysen, verbindliche Sicherheitsstandards und aktive Präventionsmaßnahmen. Nur dann können Versicherer auch bezahlbare Policen mit sinnvollem Schutz anbieten. Die Verzahnung von Versicherung und Risikomanagement ist im Bereich Cybersicherheit entscheidend.

Cyberversicherer stellen daher klare Anforderungen an Kliniken. Wer beispielsweise bei Anbietern wie Relyens eine Police abschließen möchte, muss bestimmte Mindeststandards in der IT-Sicherheit erfüllen. Voraussetzung ist eine grundlegende Absicherung der Systeme – etwa durch Virenschutz, Firewalls, regelmäßige Datensicherungen, ein konsequentes Update-Management sowie Zwei-Faktor-Authentifizierung. Auch Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter gehören zum Standardprogramm. In einem gemeinsamen Risikodialog zwischen dem Versicherer und dem Interessenten wird dann das IT-Security-Level festgestellt, um ein Gefühl für die Sensibilität des Hauses und die Herausforderungen zu bekommen.

GEMEINSAME ENTWICKLUNG VON SICHERHEITSKONZEPTEN

Versicherer erwarten von Krankenhäusern keine perfekten Lösungen oder eine vollständig modernisierte IT-Infrastruktur. Vielmehr geht es darum, Schwachstellen zu erkennen und gezielt anzugehen. Im Rahmen der Risikobewertung geben Versicherer den Krankenhäusern Hinweise, an welchen Stellen Verbesserungen möglich sind.

Die Kernaufgabe besteht darin, die IT-Systeme so abzusichern, dass der Klinikbetrieb –besonders die Patientenversorgung – auch im Krisenfall stabil aufrechterhalten werden kann oder im Krisenplan Alternativen geschaffen wurden. Voraussetzung dafür ist ein realistisches Verständnis der eigenen Risikolage sowie ein strategischer Plan, der Maßnahmen für den Ernstfall umfasst.

Ein auf Krankenhäuser spezialisierter Versicherer kann umfassende Risikomanagementmaßnahmen anbieten, die darauf abzielen, das Risiko einer Cyberattacke einzudämmen beziehungsweise die Auswirkungen eines entstandenen Schadens einzugrenzen. Grundsätzlich gibt es sechs Bereiche, die innerhalb des Cyberrisikomanagements eine Rolle spielen und für die konkrete Maßnahmen entwickelt werden können. Beispielsweise hilft eine Präsenzschulung von Führungskräften dabei, über die NIS-2-Richtlinie aufzuklären und sie damit in die Lage zu versetzen, die richtigen Entscheidungen zu treffen.

Das Thema Cybersicherheit – einschließlich Cyberversicherungen – ist im deutschen Gesundheitswesen angekommen, die praktische Umsetzung jedoch noch nicht flächendeckend ausgereift. Viele Einrichtungen befinden sich weiterhin im Entwicklungsprozess. Versicherer fordern dabei klare Fortschritte, um einen wirksamen Versicherungsschutz anbieten zu können. ■

Literatur

[1] *Engelmann Software GmbH: Alarmsignal Cybersicherheit: Wie verwundbar ist das Gesundheitswesen? Cyberangriffe auf Krankenhäuser nehmen weiter zu. Online verfügbar unter: https://engelmann.com/de/sicherheit/cyberangriffe-krankenhaeuser/*

[2] *Krankenhaus-IT: Cyberangriffe auf Krankenhäuser: Strategische Neuausrichtung der IT-Landschaft und Resilienz als kritische Komponenten. In: Krankenhaus-IT Journal Online, 2025. Online verfügbar unter: www.krankenhaus-it.de/item.4068/cyberangriffe-auf-krankenhaeuser-strategische-neuausrichtung-der-it-landschaft-und-resilienz-als-kritische-komponenten.html*

DIRK BEDNAREK
ist Leiter der deutschen Niederlassung von Relyens. (Bild: Relyens)

Interview mit Professor Christof Paar, Direktor am Max-Planck-Institut für Sicherheit und Privatsphäre

POST-QUANTEN-KRYPTOGRAFIE, KI UND DATENSCHUTZ: WOHIN STEUERT DIE IT-SICHERHEIT?

Die IT-Sicherheit steht vor einem tiefgreifenden Wandel: Quantencomputer bedrohen bestehende Verschlüsselungen, künstliche Intelligenz verändert Angriffs- wie Abwehrmechanismen, und Datenschutz wird zur geopolitischen Frage. Einer, der diese Entwicklungen seit Jahrzehnten mitgestaltet, ist Prof. Christof Paar. Als Gründungsdirektor des Max-Planck-Instituts für Sicherheit und Privatsphäre in Bochum forscht er an den Schnittstellen von Technik, Gesellschaft und Mensch. Im Gespräch mit unserem Fachautor Prof. Norbert Pohlmann erklärt er, warum Kryptografie längst überall ist, wo die größten Herausforderungen liegen und warum IT-Sicherheit endlich benutzbar werden muss.

Bild: Leopard - stock.adobe.com

Prof. Norbert Pohlmann: Herr Professor Paar, Ihr Weg in die IT-Sicherheitsforschung ist eher ungewöhnlich – vom Fernmeldemechaniker zum Max-Planck-Direktor. Wie kam es dazu?

Prof. Christof Paar: Das stimmt, mein Weg war etwas untypisch. Nach meinem Realschulabschluss habe ich eine Handwerkslehre als Fernmeldemechaniker gemacht. Danach kamen Fachabitur, Studium der Nachrichtentechnik und schließlich eine Promotion in Codierungstheorie. Schon damals hat mich die Verbindung von Technik, Mathematik und Praxis fasziniert. Als dann der Internet-Boom begann, wurde Kryptografie plötzlich extrem relevant. Das war mein Glück – ich konnte zur richtigen Zeit in ein Feld einsteigen, das enorm an Bedeutung gewonnen hat.

Kryptografie: Von der Nische zum Herzstück

Pohlmann: Sie haben sich früh mit angewandter Kryptografie beschäftigt, lange bevor sie im Alltag eine Rolle spielte. Wie hat sich das Feld seither verändert?

Paar: Dramatisch. In den 90er-Jahren war Kryptografie eher eine mathematische Nische. Dann kam der Internet-Boom, und plötzlich wurde Datenschutz in Webbrowsern, Smartcards und dem aufkommenden Internet der Dinge relevant.

Ich hatte das Glück, genau in dieser Zeit mit dem Thema Krypto-Engineering ein damals kaum besetztes Feld aufzubauen. Heute ist Kryptografie in jedem Smartphone, in jeder Banking-App, in jedem Auto. Aber die Komplexität ist enorm gewachsen. Viele Herausforderungen, die es damals gab, sind übrigens auch heute noch da.

Pohlmann: Sie haben selbst die CHES-Konferenz gegründet, die diese Entwicklung mitgeprägt hat. Was war damals die größte Herausforderung, diese Community ins Leben zu rufen?

Paar: Damals, 1999, war das noch ein ziemliches Experiment. Mein Kollege Çetin Koç und ich dachten, vielleicht kommen 30 oder 40 Leute. Am Ende waren es 160. Das war ein riesiger Erfolg – auch, weil Leute wie Adi Shamir dabei waren, der auf der Konferenz spektakuläre Forschungsergebnisse vorgestellt hat. Die größte Herausforderung war sicher, die Leute davon zu überzeugen, dass Kryptografie nicht nur Mathematik ist, sondern auch eine Ingenieursdisziplin. Es ging darum, die praktische Umsetzung sicherer Systeme in den Fokus zu rücken. Das war damals neu.

Pohlmann: Ein gutes Beispiel für die praktische Umsetzung sicherer Systeme sind die elliptischen Kurven, die Sie früh bearbeitet haben. Warum sind die so wichtig geworden?

Paar: Elliptische Kurven sind heute praktisch überall. In WhatsApp, in Webbrowsern, bei Bitcoin – überall, wo digitale Signaturen eingesetzt werden. Der große Vorteil ist, dass sie bei gleicher Sicherheit viel kleinere Schlüssel benötigen als etwa RSA. Das spart Speicherplatz und macht die Verfahren schneller. Das war schon früh klar, auch wenn es damals nur wenige Leute gemacht haben.

Wir werden alle sterben …!?

Pohlmann: Stehen wir Ihrer Ansicht nach eher am Rand des digitalen Untergangs oder sehen Sie Fortschritte bei der Abwehr?

Paar: Da gibt es zwei Sichtweisen. Die eine Seite sagt: Alles Katastrophe, Cyberangriffe, Ransomware, Zero-Day-Exploits – wir sind verloren. Die andere Seite meint: Kryptografie ist so stark wie nie, viele Verfahren sind unbrechbar. Wie so oft liegt die Wahrheit irgendwo dazwischen. Ja, wir haben ernsthafte Bedrohungen. Ransomware ist ein gutes Beispiel. Aber wir lernen auch, immer besser damit umzugehen.

Pohlmann: Und das bedeutet?

Paar: IT-Sicherheit ist kein Zustand, den man irgendwann erreicht und dann abhaken kann. Sie ist ein Dauerzustand. Ich vergleiche das oft mit Einbruchschutz. Man kann die Risiken minimieren, aber nie ganz eliminieren.

PROFESSOR CHRISTOF PAAR
ist ein deutscher Kryptograf. Er ist Direktor am Max-Planck-Institut für Sicherheit und Privatsphäre in Bochum und „Wissenschaftliches Mitglied" der Max-Planck-Gesellschaft.

NORBERT POHLMANN
ist Professor für Cyber-Sicherheit 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.

Pohlmann: Was bedeutet das für Unternehmen?

Paar: Unternehmen müssen IT-Sicherheit strukturell denken – über alle Ebenen hinweg. Es geht nicht nur um technische Maßnahmen, sondern auch um Organisation, Prozesse und Schulungen.

Wichtig ist vor allem: Niemand sollte erwarten, Angriffe komplett verhindern zu können. Entscheidend ist, wie schnell man reagieren kann und wie realistisch die eigene Risikoeinschätzung ist.

Pohlmann: Sie vergleichen Cybersicherheit mit Einbruchschutz im Alltag. Heißt das, wir sollten in der IT-Sicherheit auch stärker über akzeptierte Restrisiken sprechen?

Paar: Ja, absolut. Wie bei Fahrraddiebstahl oder Wohnungseinbrüchen geht es auch in der IT-Sicherheit darum, Risiken zu kalkulieren. Niemand kauft das teuerste Schloss, wenn der Wert des Fahrrads das nicht rechtfertigt. In der IT-Sicherheit müssen wir genauso abwägen, welche Risiken wir tragen können und welche wir absichern sollten.

Quantencomputer: Der Countdown läuft

Pohlmann: Welche Technologien stehen dabei besonders im Fokus?

Paar: Ganz klar die Post-Quanten-Kryptografie. Quantencomputer werden in der Lage sein, heute gängige asymmetrische Verfahren wie RSA oder ECC zu brechen.

Pohlmann: Und das dauert aber noch Jahre, oder?

Paar: Ja, vermutlich zehn bis fünfzehn Jahre. Aber trotzdem müssen wir jetzt anfangen umzurüsten. Denn es gibt Daten, die heute verschlüsselt werden und die auch in 20 Jahren noch geheim bleiben müssen. Geheimdienste speichern heute schon große Mengen verschlüsselter Daten, um sie später zu knacken.

Pohlmann: Viele Organisationen könnten Post-Quanten-Kryptografie als unnötig teuer empfinden. Haben Sie Verständnis für diese Haltung – oder ist das Risiko zu groß?

Paar: Das ist nachvollziehbar. Für den normalen Alltagsnutzer ist oft nicht einsichtig, warum das nötig sein soll, wenn der Quantencomputer erst in Jahren kommt. Aber bei langlebigen Systemen wie Autos oder kritischen Infrastrukturen müssen wir früh anfangen. Sonst haben wir später ein Problem.

Es liegt nicht (immer) am User

Pohlmann: Der Mensch gilt in der IT-Sicherheit oft als Schwachstelle. Muss man diese Sichtweise überdenken?

Paar: Unbedingt. Es bringt nichts, die Menschen „optimieren" zu wollen, wenn die Systeme nicht benutzbar sind. Wir müssen Sicherheit so ge-

stalten, dass sie sich an den Menschen anpasst – nicht umgekehrt.

Pohlmann: Sie kritisieren fingierte Phishing-Tests als möglicherweise kontraproduktiv. Woran liegt das Ihrer Meinung nach?

Paar: Solche Tests können Misstrauen säen. Die Leute fühlen sich ständig überwacht und getestet. Das schafft kein gutes Arbeitsklima. Außerdem gibt es Forschung, die zeigt, dass solche Maßnahmen langfristig keinen positiven Effekt haben – sondern eher negative.

Pohlmann: Sie haben gesagt, man solle aufhören, den Menschen zu ändern, sondern Systeme benutzbarer machen. Haben Sie ein Beispiel, wo das bislang besonders schlecht gelingt?

Paar: E-Mails sind da ein gutes Beispiel. Ich bekomme jede Woche E-Mails, bei denen ich nicht weiß: Soll ich klicken oder nicht? Selbst ich als Fachmann bin oft überfordert. Das zeigt, dass wir Systeme entwickeln müssen, die solche Entscheidungen abnehmen, statt immer mehr Schulungen zu machen.

Datenschutz und andere Zumutungen

Pohlmann: Wenn wir vom Menschen weg und auf die regulatorische Ebene schauen: Wie steht Europa beim Thema Datenschutz da?

Paar: Sehr gut. Die Datenschutzgrundverordnung (DSGVO) ist weltweit ein Maßstab. Auch in den USA wird das Thema inzwischen ernster genommen, weil das Vertrauen in große Plattformen bröckelt. Allerdings ist die praktische Umsetzung oft noch eine Herausforderung.

Pohlmann: Die großen Plattformen verdienen weiterhin Milliarden mit unseren Daten. Können wir dem etwas entgegensetzen?

Paar: Ich halte wenig davon, nur auf Regulierung zu setzen. Besser wäre es, echte Alternativen zu schaffen – europäische Suchmaschinen, Cloud-Dienste oder KI-Modelle mit eingebautem Datenschutz.

Pohlmann: Viele Menschen lesen oder verstehen auch die langen AGBs nicht. Glauben Sie, dass wir andere Mechanismen brauchen, um Datenschutz verständlich zu kommunizieren?

Paar: Auf jeden Fall. Niemand liest zehn Seiten AGB. Das ist nicht benutzerfreundlich und bringt auch keinen effektiven Datenschutz. Wir brauchen neue Interaktionsmodelle zwischen Nutzer, Technik und Regulierung, die verständlicher und kürzer sind.

Pohlmann: Sie sagen, der bessere Weg seien europäische Alternativen statt bloßer Regulierung. Wo sehen Sie momentan die größten Chancen, solche Dienste in Europa erfolgreich aufzubauen?

Paar: Ich denke, es gibt durchaus Chancen, gerade bei Diensten, die auf Vertrauen setzen – wie sichere Kalender- oder Kommunikationsdienste. Apple zeigt ja, dass sich Datenschutz auch verkaufen lässt, weil sie sagen: Wir verdienen unser Geld mit Hardware, nicht mit deinen Daten. In Europa müssten wir solche Modelle stärker entwickeln.

Yin und Yang

Pohlmann: Welche Rolle spielt künstliche Intelligenz (KI) in der IT-Sicherheit?

Paar: Eine sehr große. KI wird inzwischen fast überall in der IT-Sicherheitsforschung eingesetzt, auch bei uns im Exzellenzcluster. Sie hilft zum Beispiel dabei, Schwachstellen zu finden, Angriffe zu erkennen oder große Datenmengen zu analysieren.

Pohlmann: Ist das eine Gefahr für die Privatsphäre?

Paar: Ja, absolut. KI kann sehr detaillierte Profile erstellen, die oft weit über das hinausgehen, was ein Mensch freiwillig preisgeben würde. Das wird besonders gefährlich, wenn schwache Datenschutzgesetze gelten. Deshalb brauchen wir Privacy-by-Design auch im KI-Kontext – und Systeme, die erklärbar bleiben.

Pohlmann: Wo sehen Sie aktuell das größte Risiko für Angriffe durch künstliche Intelligenz?

Paar: Spear-Phishing ist ein gutes Beispiel. KI kann sehr gezielt E-Mails erstellen, die persönlich wirken und auf frühere Kommunikation Bezug nehmen. Das macht solche Angriffe extrem gefährlich, weil sie schwer zu erkennen sind.

Pohlmann: Gleichzeitig setzen viele Sicherheitsforscher auf KI zur Verteidigung. Gibt es Bereiche, wo das aus Ihrer Sicht schon heute einen echten Unterschied macht?

Paar: Definitiv. Zum Beispiel beim Aufspüren von Schwachstellen in Software oder beim Analysieren großer Datenströme auf Angriffe. Da kann KI schon sehr hilfreich sein. Aber es ist ein Wettrüsten: Die Angreifer nutzen KI halt genauso.

Fully Homomorphic Encryption

Pohlmann: Zum Schluss noch: Was sind für Sie persönlich die spannendsten Fragen in der IT-Sicherheitsforschung?

Paar: Zwei Dinge faszinieren mich besonders. Erstens die Weiterentwicklung kryptografischer Verfahren – etwa Fully Homomorphic Encryption, mit der man auf verschlüsselten Daten arbeiten kann. Das ist technisch anspruchsvoll, könnte aber den Datenschutz revolutionieren.

Zweitens der Faktor Mensch: Wie schaffen wir es, Sicherheit so zu gestalten, dass sie sich wirklich in den Alltag integriert? Wenn uns das gelingt, können wir viele Angriffe verhindern, bevor sie überhaupt entstehen.

Pohlmann: Was wäre aus Ihrer Sicht der wichtigste Anwendungsfall für Fully Homomorphic Encryption?

Paar: Ein gutes Beispiel wäre das Arbeiten mit verschlüsselten Daten in der Cloud. Heute muss man Daten oft entschlüsseln, um sie zu verarbeiten. Fully Homomorphic Encryption würde es ermöglichen, Daten verschlüsselt zu lassen und trotzdem Berechnungen durchzuführen. Das könnte viele Datenschutzprobleme lösen. Aber es ist noch eine große technische Herausforderung, das effizient genug zu machen.

Pohlmann: Herr Professor Paar, vielen Dank für das Gespräch. ■

Mehr Stimmen und Geschichten aus der Branche gibt es in der Podcast-Reihe „Köpfe der IT-Sicherheit" unter ***https://it-sicherheit.de/markplatz-format/koepfe-der-it-sicherheit/***

Von der Norm zur Wirkung (1):
Wie Unternehmen mit ISO 9001 Output, Steuerung und Resilienz stärken

QUALITÄT ALS BASIS

Die ISO 9001 gilt oft als bürokratisches Pflichtprogramm – dabei steckt darin das Potenzial für echte Führungswirksamkeit. Richtig umgesetzt, wird die Norm zum architektonischen Rahmen, um Ziele, Risiken und Verantwortung systematisch zu vernetzen. Sie schafft die Grundlage für digitale Regelkreise, die Qualität, Resilienz und Output gleichermaßen fördern. Dieser Beitrag zeigt, wie Unternehmen mit der SECaaS.IT-Methode ISO 9001 als strategisches Steuerungsinstrument nutzen können. Damit beginnt unsere Serie „Regulierung wirksam gestalten".

Regulatorischer Druck, steigende Kundenerwartungen und immer kürzere Innovationszyklen zwingen Unternehmen dazu, ihre Strukturen und Prozesse laufend zu hinterfragen. Viele reagieren mit Einzelmaßnahmen: neue Tools, neue Dokumente, externe Audits. Doch oft führt diese Fragmentierung nicht zu Klarheit – sondern zu mehr Komplexität.

Unsere Überzeugung: Qualität ist nicht das Ziel, sondern der Weg. Und ISO 9001 ist nicht die Lösung, sondern der Rahmen, in dem echte Lösungen operationalisiert werden können – mit Wirkung im Tagesgeschäft und auf strategischer Ebene.[1]

Mit der von den Autoren entwickelten SECaaS.IT-Methode wird aus einem normkonformen Qualitätsmanagement ein aktiver Steuerungsansatz: digitale Self-Assessments, KPI-basierte Performance-Steuerung und automatisierte Review-Prozesse machen Organisationen nicht nur auditfähig – sondern entscheidungsfähig. So entsteht eine neue Führungslogik: schlank genug für schnelle Entscheidungen, robust genug für regulatorische Anforderungen – und stark genug für Wachstum.

MESSBARE VERBESSERUNGEN DURCH STRUKTURIERTES QUALITÄTSMANAGEMENT

Studien wie der EFQM Global Excellence Index[2] oder Erhebungen des Fraunhofer IAO[3] belegen: Organisationen mit strukturierten, kennzahlenbasierten Managementsystemen reagieren schneller auf Veränderungen, verbessern ihre Krisenresilienz – und verkürzen ihre Innovationszyklen messbar. Der Schlüssel liegt dabei nicht allein in der Norm, sondern in der Art der Umsetzung: Digitale Regelkreise, klare Rollenverantwortung und automatisierte Steuerungspunkte machen aus Qualitätsmanagement ein Führungsinstrument.

Mit der SECaaS.IT-Methode zeigen sich in der Praxis folgende Effekte:

- 25 Prozent mehr Output in Kernprozessen bei gleichbleibender Teamgröße,
- 40 Prozent weniger Rückfragen durch klare Prozessverantwortung,
- 20 Prozent schnellere Markteinführung durch integrierte Compliance,
- 60 Prozent weniger manuelle Aufwände durch Audit-Trail-Automatisierung.

Eine Metaanalyse von Martínez-Costa & Martínez-Lorente (2007) weist für systematisch umgesetzte ISO-Qualitätsstrukturen eine durchschnittliche Produktivitätssteigerung von 15 bis 25 Prozent aus – unabhängig von Branche oder Unternehmensgröße[4,5]. Fazit: Wer ISO 9001 entlang strukturierter Umsetzungslogik einführt, schafft die prozessuale Basis, um auch Informationssicherheit, Risikomanagement und Nachhaltigkeit integriert, wirksam und ohne Mehraufwand zu steuern.

DIE ARCHITEKTUR DER ISO 9001 VERSTEHEN

ISO 9001 ist kein bürokratischer Rahmen, sondern ein architektonisches Steuerungsmodell. Richtig interpretiert, liefert sie das verbindende Fundament für integrierte Managementsysteme, die operative Exzellenz, strategische Klarheit und organisationale Resilienz miteinander verbinden.

Seit der Revision 2015 folgt die ISO 9001 der sogenannten Harmonized Structure (HS) – früher „High Level Structure".[7] Dieses Rahmenwerk wird auch in ISO 27001 (Informationssicherheit), ISO 14001 (Umweltmanagement) oder ISO 45001 (Arbeitsschutz) verwendet. Damit lassen sich verschiedene Managementsysteme modular zusammenführen, ohne Methodik oder Tools mehrfach erfinden zu müssen. Die Harmonized Structure wird dadurch zum „Systemträger" für integrierte Steuerung – nicht nur für Qualität, sondern auch für Sicherheit, Nachhaltigkeit, interne Kontrollsysteme (IKS) oder Umwelt-, Sozial- und Governance-Aspekte (ESG).

Sie umfasst sieben Kernbereiche (vgl. Tabelle 1) und fordert explizit, Qualitätsziele mit Chancen und Risiken zu verknüpfen. Das bedeutet: Steuerung basiert nicht nur auf Zielkennzahlen, sondern auch auf Risikowahrnehmung und -bewertung – ein Prinzip, das sich auch auf Informationssicherheit, Nachhaltigkeit oder ESG übertragen lässt. So entsteht ein skalierbares Risikoreporting mit Frühwarncharakter – zentral für resilientere Entscheidungen und agile Ressourcensteuerung.

Die Umsetzung erfolgt typischerweise in vier Schritten:

1. **Identifikation:** Prozessverantwortliche benennen potenzielle Abweichungen, zum Beispiel Lieferverzug, Kompetenzlücken, Dateninkonsistenzen.
2. **Bewertung:** Eintrittswahrscheinlichkeit × Auswirkung ergibt Risikoprioritäten

Bild: Sora von OpenAI

HS Kapitel	Zweck	Leitfrage
1. Kontext der Organisation (Scope)	Analyse externer/interner Einflussfaktoren sowie Stakeholder-Erwartungen. Ergebnis: messbarer Rahmen für Ziele und Risiken	Was beeinflusst unsere Zielerreichung maßgeblich?
2. Führung	Die oberste Leitung übernimmt Verantwortung, stellt Ressourcen bereit und verankert Qualität in der Strategie.	Wie demonstriert das Top-Management sein Commitment?
3. Planung	Chancen und Risiken werden identifiziert, priorisiert und mit Maßnahmen verknüpft.[8]	Welche KPIs und Risiken steuern unsere Maßnahmen?
4. Unterstützung	Kompetenzen, Wissen, Tools und Daten bilden das Rückgrat der Umsetzung. Excel-Silos werden durch digitale Workflows ersetzt.	Haben Teams die Voraussetzungen für Qualität?
5. Betrieb	Prozesslenkung auf operativer Ebene – eindeutig, messbar, wiederholbar	Sind Abläufe stabil, sichtbar und steuerbar?
6. Bewertung der Leistung	KPIs, Audits und Reviews machen Fortschritt objektiv sichtbar – Voraussetzung für faktenbasierte Entscheidungen.	Welche Informationen ermöglichen aktive Steuerung?
7. Verbesserung	Lernen durch Abweichungen. Der PDCA-Zyklus sorgt für kontinuierliche Entwicklung statt punktueller Reaktion.[9]	Wie fließt Erfahrung in Steuerung und Zukunftsgestaltung ein?

Tabelle 1: Übersicht der Kapitel der Harmonized Structure (HS) der ISO 9001 mit ihrem jeweiligen Zweck und den zentralen Leitfragen, die Unternehmen bei der Umsetzung eines integrierten Managementsystems unterstützen

Norm/Richtlinie	Relevanz für Qualität und Führung
ISO 9001:2015	Strukturrahmen für wirksames Qualitätsmanagement
ISO 9004:2018	Orientierung für nachhaltigen Unternehmenserfolg und Reifegradentwicklung
ISO 19011:2018	Leitfaden für Audits von Managementsystemen
ISO 31000:2018	Grundlage für risikobasierte Steuerung und Entscheidungsfindung
EU NIS 2 (2022/2555)	Anforderungen an Cyberresilienz, besonders für kritische Infrastrukturen
IDW PS 982/IDW PS 951	Standards für Prüfung von internen Kontrollsystemen (IKS)

Tabelle 2: Relevante Regulatorik und Standards

3. **Maßnahmenableitung:** Vorbeugung oder Korrektur, inklusive Fälligkeiten und Verantwortlichkeiten

4. **Review:** Dashboards zeigen Trends und Restrisiken, Management-Reviews bewerten die Wirksamkeit.

Damit verbunden ist ein modernes Verständnis von Dokumentation: Die Norm versteht dokumentierte Information nicht mehr als Pflicht, sondern als lebendiges Wissenssystem. Verfügbarkeit, Integrität und Aktualität stehen im Vordergrund – unterstützt durch digitale Werkzeuge. Statt statischer Dokumente entstehen auditfähige, steuerbare Informationsflüsse mit Versionierung, Freigabeworkflows und automatisierten Prozessschnittstellen. In Kombination mit modernen Tools wie Office 365, Jira oder Power BI entsteht ein „Systemgedächtnis", das Prozesse lenkbar und transparent macht.

Die SECaaS.IT-Methode nutzt diesen Rahmen gezielt, um digitale Steuerungsarchitekturen zu etablieren: mit rollenbasierter Umsetzung, automatisierten Reviews, KPI-Logik und Heatmaps zur Risiko- und Reifegradbewertung. Das Ergebnis: Aus einem ISO-Rahmenwerk wird ein lebendiges, datengetriebenes Steuerungssystem – schlank, belastbar und zukunftsorientiert. Der Effekt entsteht nicht durch die Norm selbst, sondern durch die Art ihrer konsequent digitalen Übersetzung.[10]

METHODISCHE UMSETZUNG UND NUTZEN

Der größte Mehrwert entsteht, wenn Unternehmen die ISO 9001 nicht als Zertifizierungsprojekt, sondern als Regelkreis für Leistungsfähigkeit und Führungsarbeit verstehen. Das gelingt besonders dann, wenn die Umsetzung nicht mit Dokumentation beginnt – sondern mit digital gestützter Wirkungsanalyse. Genau hier setzt die SECaaS.IT-Methode an – mit klaren Rollen, messbaren Effekten und minimalem Dokumentationsaufwand.

Anstelle langwieriger Audits nutzt die SECaaS.IT-Methode ein digitales Self-Assessment, das sich an ISO 9004 orientiert – dem internationalen Leitfaden für nachhaltigen Unternehmenserfolg. Ein strukturierter Fragenkatalog analysiert etwa 30 Qualitätsdomänen von „Initial" bis „Optimierend". KI-Logik erkennt dabei Widersprüche, etwa hohe Prozessreife ohne

Phase	Umsetzung mit SECaaS.IT-Methode
Plan	Ziele, KPIs, Risiken aus Strategie und Stakeholder-Analyse ableiten
Do	Prozesse digitalisiert und rollenbasiert umsetzen – inklusive Aufgabenpaketen und Eskalation
Check	KPI-Dashboards, interne Audits, Heatmaps und Trendanalysen nutzen
Act	Automatisierte Lessons-Learned-Prozesse, Maßnahmen-Tracking, Review-Feedback

Tabelle 3: Umsetzung des PDCA-Zyklus

Kennzahlen, und schlägt automatisch Maßnahmen vor – inklusive Nutzen, Aufwand, Rolle und Deadline. Diese Vorgehensweise erlaubt:

- **einen niedrigschwelligen Einstieg,** ohne Prüfungscharakter,
- **klare Priorisierung** nach ROI-Schwellen und
- **objektive Reifegraddarstellung** als Radar-Diagramm (siehe Beispiel Abbildung 1).

Die Methode basiert auf sieben Prinzipien, die Auditfähigkeit und Steuerung verbinden:

1. **Normkonformität als Struktur – nicht als Ziel:** Normen wie ISO 9001 bilden das Rahmenwerk, der Fokus liegt auf operativer Wirksamkeit.
2. **Prozessorientierung statt Dokumentation:** Statt statischer Handbücher setzen erfolgreiche Implementierungen auf lebendige, digitale Prozesse mit Rollen, KPIs und Schnittstellen.
3. **Reifegrad-Assessment als Einstieg:** Ein digitales Self-Assessment liefert in 30 Minuten eine fundierte Ausgangslage. Integrierte KI priorisiert Maßnahmen nach Wirkung, nicht Aufwand.
4. **Automatisierung und Workflow-Logik:** Freigaben, Eskalationen, Nachweise werden alles systemgestützt abgebildet. Genutzt werden bestehende Tools (O365, ERP, Jira) via Low-Code/No-Code-Logik.

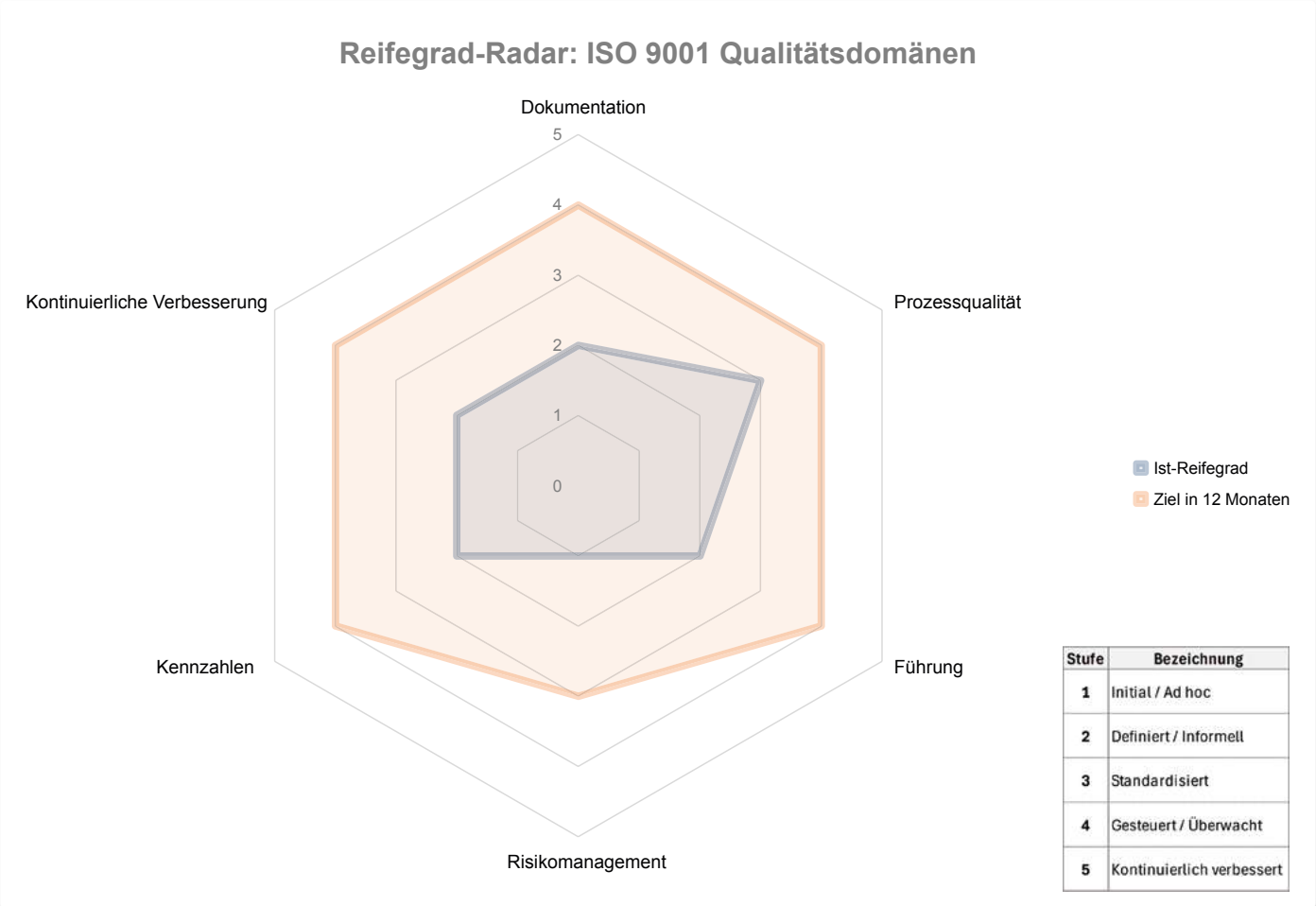


Abbildung 1: Das Chart zeigt den Ist-Reifegrad, eine zweite Linie den Zielwert in zwölf Monaten. Fortschritte aktualisieren sich, sobald Teilaufgaben erledigt sind – ein Motivationsbooster für Teams und ein belastbares Steuerungsinstrument für das Management. (Bild:SECaaS.IT)

5. **KPI-basierte Steuerung mit Frühwarnindikatoren:** Kennzahlen wie On-Time Delivery (OTD), Nacharbeitsquote oder Durchlaufzeit liefern Führungskräften Echtzeit-Einblicke – visualisiert in Heatmaps, Dashboards und Trendanalysen.

6. **Rollenorientierung und Akzeptanz:** Anforderungen werden in bestehende Rollen integriert, mit Micro-Trainings, Aufgabenpaketen und Checklisten unterstützt.

7. **Compliance by Design – Performance by Intention:** Managementsysteme sind so gestaltet, dass sie automatisch auditfähig sind und gleichzeitig Performance, Output und Skalierung ermöglichen.

Diese Prinzipien spiegeln sich in einem praxisbewährten Umsetzungsprozess, der Organisationen schrittweise zu Output, Steuerungssicherheit und Auditfähigkeit führt (siehe Tabelle 4). Dieser Aufbau verbindet strategische Analyse mit operativer Steuerung. Unternehmen können damit binnen Wochen in die wirksame Umsetzung starten.

Schritt	Methode/Tool	Digitale Umsetzung	Nutzen
1. Kontextanalyse	SWOT, Stakeholder-Mapping, PESTEL	Whiteboards, Trendanalyse, KI-Unterstützung	gemeinsames Lagebild & strategische Klarheit
2. Prozesslandkarte	SIPOC, BPMN, RACI	Low-Code-Prozessmodellierung	Transparenz, Verantwortlichkeiten, Schnittstellen
3. Risikobewertung	Heatmaps, Scoring, Balanced Scorecard	Daten-Connectoren aus ERP, CRM et cetera	risikoorientierte Planung und KPI-Steuerung
4. Workflow-Logik	Freigaben, Reminder, Eskalationen	Automatisierung via Prozess-Engines	Reduktion manueller Aufwände, schnelle Reaktion
5. Reviews und PDCA	Audits, Dashboards, Natural-Language-Reports	Management-Reports, Heatmaps	kontinuierliche Verbesserung, Frühwarnfunktion

Tabelle 4: Umsetzungsprozess

Die SECaaS.IT-Methode hat in verschiedenen Projekten zu messbaren Verbesserungen geführt – und das ohne proprietäre Software oder zusätzliche Ressourcen im laufenden Betrieb. In realen Projekten aus Fertigung, Dienstleistung und Gesundheitswesen wurden unter anderem eine um 30 Prozent reduzierte Auditvorbereitungszeit, eine um 25 Prozent verkürzte Durchlaufzeit von Freigabeprozessen durch Automatisierung sowie eine um 15 Prozent gesteigerte Liefertreue durch kennzahlenbasierte Frühwarnsysteme erzielt.

Ebenso konnte die Umsetzungsgeschwindigkeit von Maßnahmen um 40 Prozent steigen, während sich die manuellen Aufwände bei Audits und Qualitätsmanagement-Prozessen um 60 Prozent verringerten. Auch die Prozessoutputrate, etwa gemessen an Aufträgen je Ressource, erhöhte sich um 25 Prozent durch eine Architektur, die Rollen und Kennzahlen eng miteinander verknüpft. Diese Ergebnisse stammen aus 27 Projekten im Zeitraum von 2020 bis 2024 und wurden auf Basis von Zeiterfassungen, Review-Zyklen und ERP-Logs dokumentiert.

Zur Steuerung und Visualisierung der Fortschritte setzt die Methode auf digitale Werkzeuge: Ein interaktives Reifegrad-Radar zeigt den Entwicklungsstand im Vergleich von Ist- und Zielwerten, während eine Heatmap die wichtigsten Risiken priorisiert. Maßnahmenpakete sind dabei stets mit Aufgaben- und Eskalationslogiken verknüpft. So erhalten Führungskräfte auf einen Blick Antworten auf zentrale Fragen wie: Wo stehen wir? Was blockiert uns? Und welche Maßnahmen erzielen tatsächlich Wirkung? Diese Form der Transparenz ersetzt klassische Status-Meetings oder umfangreiche Präsentationen und schafft eine steuerbare Echtzeit-Systematik.

ROLLEN IM FOKUS

Ein wirkungsvolles Managementsystem lebt nicht allein von Regeln und Prozessen, sondern entsteht durch klar definiertes, rollenbasiertes Handeln – über alle Ebenen hinweg. Die SECaaS.IT-Methode setzt genau hier an: Sie sorgt dafür, dass jeder Beteiligte versteht, was seine Aufgabe im System ist, ganz gleich, ob in der Geschäftsführung, im Fachbereich oder im operativen Bereich.

Für die Geschäftsführung bedeutet das, dass die ISO 9001 weniger als Sammlung technischer Vorgaben, sondern vielmehr als Instrument für Unternehmensführung verstanden wird. Ziel ist es, die Steuerungsfähigkeit des Unternehmens zu stärken, ohne sich dabei in operativen Details zu verlieren. Ein Beispiel für eine Umsetzung ist die SECaaS.IT-Methode, die diesen Ansatz nutzt, um die Norm als strategische Steuerungsplattform einzusetzen. Frühwarnindikatoren sollen dabei helfen, Risiken frühzeitig zu erkennen und Entscheidungen auf fundierter Basis zu treffen – mit dem Ziel, nicht nur die Audit-Bereitschaft sicherzustellen, sondern auch die Führungsfähigkeit zu verbessern.

Unterstützt wird dies durch verschiedene Mechanismen: So lassen sich Kennzahlen aus dem Managementsystem direkt mit strategischen Unternehmenszielen wie Umsatzwachstum, Liefertreue oder Kundenbindung verknüpfen. Rollenbasierte Nachweise zeigen zudem, wer welche Entscheidungen getroffen hat, welche Risiken bestehen und welche Maßnahmen umgesetzt wurden, was Rechts- und Revisionssicherheit erhöht. Frühwarnsysteme wie KPI-Trendlinien, Maßnahmenstaus oder Rest-Risiko-Indikatoren ermöglichen zudem eine vorausschauende Ressourcenplanung, anstatt erst im Krisenfall zu reagieren.

Studien belegen, dass Organisationen mit solchen integrierten Frühwarnsystemen im Durchschnitt 28 Prozent schneller auf externe Veränderungen reagieren.

Auch für Fachverantwortliche wie Qualitätsmanager, Sicherheitsbeauftragte oder Verantwortliche für das Interne Kontrollsystem (IKS) schafft die ISO 9001 eine gemeinsame Sprache für Systemverantwortung über alle Fachdisziplinen hinweg. Die SECaaS.IT-Methode macht diese Verantwortung steuerbar, indem sie konsistente

Schnittstellen etabliert, gemeinsame Risikoregister nutzt und einheitliche Reviews sowie abgestimmte Eskalationslogiken vorsieht, um den Abstimmungsaufwand zu minimieren.

Fachverantwortliche können Maßnahmen und Kontrollen anhand von Kennzahlen, Fristen und ihrer tatsächlichen Wirksamkeit nachverfolgen, ohne dabei auf manuell geführte Excel-Listen angewiesen zu sein. Zudem lassen sich Erkenntnisse aus Audits oder Vorfällen domänenübergreifend teilen, zum Beispiel zwischen Qualitätsmanagement und Informationssicherheit. In der Praxis ergeben sich daraus konkrete Vorteile wie eine Reduktion des Vorbereitungsaufwands bei Audits um bis zu 50 Prozent, eine klarere Priorisierung bei knappen Ressourcen sowie eine schnellere Identifikation von „blinden Flecken" durch Signale aus Heatmaps.

In vielen Unternehmen gilt Qualitätsmanagement als zusätzliche Belastung mit neuen Formularen, unklaren Prozessen und Formalismen. Ein effektiver Ansatz setzt dagegen auf Rollenintegration statt auf zusätzliche Pflichten.

Mitarbeiter erhalten kontextbezogene Aufgaben mit Zielbeschreibung, Checklisten und Schulungseinheiten, die mit Prozessen verknüpft sind und nicht losgelöst davon existieren. Prozesskennzahlen wie Nacharbeitsquote, Durchlaufzeit oder Freigabeverzögerung werden live sichtbar gemacht, sodass jeder Einfluss nehmen kann. Micro-Trainings sind direkt mit Aufgaben verknüpft, beispielsweise beim Erfassen einer Abweichung oder bei neuen Prozessvarianten.

Die Wirkung ist messbar: Die Einarbeitung erfolgt bis zu 30 Prozent schneller durch kontextspezifische Aufgabenpakete. Rückfragen bei Abläufen reduzieren sich um etwa 40 Prozent durch klare Rollenzuordnung und Steuerung. Zudem steigt die Prozessqualität, weil Verantwortung konkret wird und Feedback unmittelbar erfolgt.

PRAXISBEISPIEL

Ein Managementsystem kann nur dann seine volle Wirkung entfalten, wenn es konsequent in die Strukturen, Prozesse und Führungslogik eines Unternehmens eingebettet wird. Der folgende Praxisfall zeigt, wie ein mittelständisches Dienstleistungsunternehmen sein bestehendes ISO-9001-System in ein digital gestütztes Steuerungsinstrument transformiert hat – ohne dabei die operativen Bereiche zusätzlich zu belasten oder teure Spezialsoftware anzuschaffen. Die zentrale Leitfrage lautete dabei: Wie wird aus einem bloß zertifizierten Qualitätsmanagementsystem ein Frühwarnsystem, das spürbaren Mehrwert erzeugt?

Die Ausgangssituation war typisch für viele zertifizierte Unternehmen: Prozessbeschreibungen lagerten in Netzlaufwerken, Auditdokumente verstaubten in E-Mail-Postfächern und Prüfprotokolle existierten als unübersichtliche Excel-Tabellen. Die jährliche Nachweissammlung verschlang rund 120 Arbeitsstunden ohne erkennbaren Mehrwert für die Unternehmenssteuerung. Ein Stau von 38 offenen Korrekturmaßnahmen – teilweise doppelt erfasst oder erledigt, aber nicht dokumentiert – zeugte von mangelnder Systematik. Die Geschäftsführung tappte bei Risiko- und Reifegradentwicklungen weitgehend im Dunkeln.

Der Transformationsprozess begann mit einem digitalen Reifegrad-Assessment. Prozessverantwortliche beantworteten in jeweils etwa 25 Minuten einen strukturierten Online-Fragebogen zu 30 Qualitätsdomänen wie Führung, Lieferantensteuerung und Maßnahmenverfolgung. Das automatisch generierte Reifegrad-Radar offenbarte deutliche Schwachstellen, besonders in den Bereichen „Maßnahmenverfolgung" (Stufe 2) und „Risikobasierung" (Stufe 1).

Auf Basis dieser Ergebnisse generierte das System priorisierte Maßnahmenpakete mit konkreten Zielbeschreibungen, klaren Verantwortlichkeiten und definierten Fristen. Jedes Paket enthielt automatische Erinnerungsfunktionen und verknüpfte die Maßnahmen mit relevanten Prozessen und Risiken. So erzeugte etwa das Maßnahmenpaket „Risikobasierung" einen Workflow, der alle Kernprozesse mit einem Risikoregister verband und bei Fertigstellung die Risiko-Heatmap ohne manuellen Eingriff aktualisierte.

Das Herzstück des neuen Systems bildete ein zentrales Dashboard, das verschiedene Steuerungsgrößen zusammenführte: Der Reifegrad-Fortschritt visualisierte die Entwicklung im Zeitverlauf, während offene und überfällige Maßnahmen als Eskalationspunkte für Führungsgespräche dienten. Die durchschnittliche Maßnahmen-Durchlaufzeit machte Prozessreife und Blockaden sichtbar, und eine Risiko-Heatmap half bei der Identifikation besonders gefährdeter Bereiche. Diese visuelle Darstellung nach Risikowert ermöglichte fundierte Budget- und Coaching-Entscheidungen.

Ein guter Schritt war die Integration der Reviews in bestehende Führungsformate statt der Schaffung zusätzlicher Termine. In monatlichen Prozess-Standups präsentierten Verantwortliche aktuelle Dashboards anstelle von PowerPoint-Folien. Das Quartals-Management-Review verglich den aktuellen Reifegrad mit dem Vorquartal und betrachtete Risikoentwicklung sowie Maßnahmenstatus. Besonders effizient: Das System generierte automatisch revisionssichere Protokolle aus dem Dashboard – ohne zusätzlichen Dokumentationsaufwand.

Nach neun Monaten zeigten sich deutliche Verbesserungen: Der Auditvorbereitungsaufwand sank von 120 auf 45 Stunden pro Jahr (−62 Prozent), die durchschnittliche Durchlaufzeit für Korrekturmaßnahmen verkürzte sich von 47 auf 18 Tage (−62 Prozent), und die Zahl offener Maßnahmen reduzierte sich von 38 auf 7, wobei keine mehr überfällig war (−82 Prozent). Die Abdeckung durch das Risikoregister stieg von 35 Prozent auf 100 Prozent der Prozesse, und das System generierte erstmals mehr als zwölf Frühwarnungen pro Quartal.

Diese Verbesserungen wirkten sich direkt auf das Kerngeschäft aus: Die Liefertreue verbesserte sich durch frühzeitige Eskalation von Engpässen, Produkte kamen schneller auf den Markt dank fokussierter Ressourcensteuerung, und in der Linie entwickelte sich eine stärkere Rollenverantwortung mit weniger Rückfragen und mehr Eigenverantwortung.

Zwei Visualisierungselemente spielten eine zentrale Rolle in der Steuerung: Das Reifegrad-Radar diente als strategisches Steuerungstool in Reviews, während die Risiko-Heatmap die Priorisierungsentscheidungen unterstützte. Beide Darstellungen fungierten nicht nur als Berichtsinstrumente, sondern als echte Führungswerkzeuge für Planung, Dialog und Budgetierung.

FAZIT

ISO 9001 ist weit mehr als ein Werkzeug für Audits. Richtig eingesetzt, wird sie zur Grundlage für wirksame Führung, Resilienz und Wachstum. Wie Organisationen diese Prinzipien umsetzen, hängt von ihren individuellen Gegebenheiten ab. Die SECaaS.IT-Methode steht

exemplarisch dafür, wie sich ISO-Strukturen in digitale Steuerungsprozesse übertragen lassen. Ihre fünf zentralen Prinzipien sind:

1. **Struktur statt Bürokratie:** Normen als Rahmen für praktische Wirksamkeit.
2. **Führung durch Frühwarnung:** Risiken erkennen, bevor sie wirken.
3. **Rollen statt Zentralismus:** Verantwortung klar verankern.
4. **Kennzahlen statt Bauchgefühl:** Steuerung durch objektive Daten.
5. **Performance by Design:** Systeme schaffen, die Leistung ermöglichen.

Im nächsten Teil der Serie zeigen wir, wie Informationssicherheit als Führungsaufgabe umgesetzt werden kann. ■

Literatur

[1] *ISO (2015): ISO 9001:2015 – Qualitätsmanagementsysteme – Anforderungen. Genf: International Organization for Standardization, Kapitel 5 und 6.*

[2] *EFQM. (2023). EFQM Global Excellence Index 2023. Brüssel: European Foundation for Quality Management.*

[3] *Fraunhofer IAO. (2021). Managementsysteme im Wandel – Resilienz und Innovation durch integrierte Managementsysteme. Stuttgart: Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO.*

[4] *Martínez-Costa, M. & Martínez-Lorente, A. R. (2007): A triple analysis of ISO 9000 effects on company performance. International Journal of Productivity and Performance Management*

[5] *Sousa & Voss (2002): Quality management re-visited: A reflective review and agenda for future research. Journal of Operations Management*

[6] *ISO (2018): ISO 9004:2018 – Qualitätsmanagement – Qualität einer Organisation – Anleitung zum Erreichen nachhaltigen Erfolgs. Genf: International Organization for Standardization.*

[7] *ISO/IEC (2015): ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, Annex SL. Genf: International Organization for Standardization.*

[8] *ISO (2015/2018): ISO 9001:2015, Abschnitt 6.1 sowie ISO 31000:2018 – Risikomanagement – Leitlinien. Genf: International Organization for Standardization.*

[9] *ISO (2018): ISO 19011:2018 – Leitfaden für Audits von Managementsystemen. Genf: International Organization for Standardization sowie PDCA-Zyklus nach Juran*

[10] *ISO (2018): ISO 9004:2018 – Qualitätsmanagement – Qualität einer Organisation – Anleitung zum Erreichen nachhaltigen Erfolgs. Genf: International Organization for Standardization, insbesondere zur Reifegradentwicklung und lernenden Organisationen.*

Regulierung wirksam gestalten: Wie Organisationen durch Struktur, KI und Systeme souverän agieren

Regulatorische Anforderungen nehmen stetig zu. Neue EU-Verordnungen, branchenspezifische Standards und umfangreiche Berichtspflichten treffen auf globalisierte Lieferketten und digitalisierte Geschäftsmodelle. Unternehmen stehen dabei vor der Herausforderung, einerseits flexibel zu bleiben und andererseits jederzeit nachweisbar regelkonform zu handeln. Entscheidend ist nicht mehr die Frage, ob Managementsysteme nötig sind, sondern wie sie so gestaltet werden können, dass sie wirksam, schlank und zugleich belastbar sind.

Hier setzt diese fünfteilige Artikelreihe an. Sie beleuchtet, wie Organisationen:

- ***Qualität als Grundlage für stabile Prozesse etablieren,***
- ***Informationssicherheit strategisch verankern,***
- ***Risiken strukturiert steuern,***
- ***Governance-Anforderungen aus Bereichen wie Internem Kontrollsystem (IKS), ESG oder DORA integrieren, und***
- ***Lieferkettenrisiken umfassend managen.***

Jeder Beitrag entwickelt praxisnahe Lösungsansätze und zeigt, wie diese in Rollen, Abläufen und Kennzahlen verankert werden können. Die Serie richtet sich an Führungskräfte ebenso wie an Fachverantwortliche, die regulatorische Anforderungen nicht allein als Pflicht, sondern als Chance zur Verbesserung von Steuerung, Transparenz und Leistungsfähigkeit begreifen möchten.

MICHAEL THEUMERT,
Co-Founder der SECaaS.IT, gestaltet sichere und menschenzentrierte Digitalisierung mit technischer Tiefe, Haltung und Herz. Er schafft Zukunftsräume, in denen Sicherheit und innere Klarheit in Resonanz treten – für wirksamen und nachhaltigen Wandel.

JÜRGEN KREUZ,
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.

TOBIAS KRAUS, M. A.,
ist Head of Compliance & IT Assurance bei der BFMT-Gruppe. Die BFMT-Gruppe ist ein unabhängiges Beratungsunternehmen mit den Schwerpunkten Steuerberatung, Wirtschaftsprüfung und Unternehmensberatung.

Nattapat - stock.adobe.com

10 % Rabatt für <kes>+ Abonnenten

ISO 27001 Lead Auditor Kurs - PECB zertifiziert

Wie auditierst du ein ISMS nach ISO 27001? Erhalte praxisnahes Wissen und sichere dir die PECB-Zertifizierung.

25.-28.08.2025 | Frankfurt/M. + Onlineprüfung
Referent: Alexander Jaber

Schwerpunkte:

- ✓ Konzepte und Prinzipien eines ISMS nach ISO/IEC 27001
- ✓ Interpretation der Normanforderungen aus Auditorensicht
- ✓ Bewertung der ISMS-Konformität und Durchführung von Audits gemäß ISO 19011 und ISO/IEC 17021-1
- ✓ Steuerung von Audit-Programmen, Leitung von Audit-Teams und professionelle Dokumentation von Audits

Jetzt anmelden: **www.datakontext.com/it-sicherheit**

Schluss mit Vendor Lock-in

DATA ACT VERPFLICHTET CLOUD-ANBIETER ZUM EINFACHEN ANBIETERWECHSEL

Der Data Act der Europäischen Union bringt tiefgreifende Änderungen für Cloud-Anbieter mit sich. Die Verordnung verpflichtet Unternehmen, die Software-as-a-Service, Plattformen oder Infrastruktur anbieten, technische und vertragliche Hürden für einen Anbieterwechsel abzubauen. Für Kunden bedeutet das mehr Flexibilität und weniger Abhängigkeit von einzelnen Anbietern.

Der Data Act gilt für alle Anbieter von Cloud-Diensten, die unter den Begriff des „Datenverarbeitungsdienstes“ fallen. Darunter versteht man digitale Dienste, die einen konfigurierbaren, skalierbaren Pool an Rechenressourcen auf Abruf (On Demand) bereitstellen (Artikel 2 Nummer 8 Data Act). Das betrifft alle Anbieter, die Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) oder Infrastructure-as-a-Service (IaaS) anbieten. Dabei spielt es keine Rolle, ob der Anbieter seinen Sitz in der Europäischen Union hat – entscheidend ist, ob der Dienst in der EU angeboten wird.

Ab September 2025 werden folgende konkrete Pflichten für Cloud-Anbieter verbindlich:

- Kunden müssen ihre Daten einfach und kostenlos zu anderen Anbietern oder in die eigene IT-Infrastruktur übertragen können.
- Die maximale Kündigungsfrist darf zwei Monate nicht überschreiten. Automatische Vertragsverlängerungen ohne aktive Zustimmung werden untersagt.
- Bis Januar 2027 dürfen Anbieter nur die tatsächlichen Kosten für den Wechselprozess berechnen. Danach sind Wechselgebühren vollständig verboten.
- Die Datenübertragung muss in gängigen, maschinenlesbaren Formaten möglich sein. Offene Schnittstellen sollen den Wechsel technisch erleichtern.

TRANSPARENZ UND FUNKTIONSÄQUIVALENZ

Anbieter müssen ihre Kunden vor und während des Wechsels umfassend informieren. Dazu gehören Angaben zum Ablauf, zu Datenformaten, technischen Einschränkungen und verfügbaren Schnittstellen. Nach dem Wechsel sollen die wichtigsten Funktionen und Prozesse weiterhin nutzbar sein. Über mögliche Einschränkungen, etwa wenn bestimmte Automatisierungen nicht übernommen werden können, müssen Anbieter transparent informieren.

Individuell angepasste Lösungen oder Testversionen sind teilweise von den Wechselregeln ausgenommen.

Dennoch müssen Anbieter auch hier alle notwendigen Informationen bereitstellen, um einen Wechsel zu ermöglichen, ohne dass Betriebsgeheimnisse offengelegt werden müssen.

DATENLIZENZVERTRÄGE NACH DEM DATA ACT

Die Verordnung regelt auch, wie Daten zwischen verschiedenen Parteien genutzt werden dürfen. Datenlizenzverträge müssen fair und transparent sein, besonders wenn Daten an Dritte weitergegeben werden. Klauseln, die kleine Unternehmen benachteiligen, sind unzulässig. Die Verträge müssen klar festlegen, für welche Zwecke die Daten genutzt werden dürfen.

Die Datenweitergabe kann abgelehnt werden, wenn dadurch Geschäftsgeheimnisse gefährdet werden. Für die Weitergabe an Dritte dürfen grundsätzlich angemessene Kosten verlangt werden – bei kleinen Unternehmen jedoch nur die tatsächlichen Bereitstellungskosten.

UMSETZUNGSZEITPLAN UND SANKTIONEN

Ab dem 12. September 2025 gelten die Vorschriften unmittelbar und verbindlich. Verstöße können mit Bußgeldern von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes geahndet werden.

Die EU-Kommission wird bis zum Stichtag freiwillige Standardvertragsklauseln zur Verfügung stellen. Diese bieten Orientierung, sind aber nicht zwingend zu verwenden. Eigenentwickelte Klauseln müssen jedoch dieselben Vorgaben erfüllen.

PRAKTISCHE UMSETZUNG FÜR UNTERNEHMEN

Für eine fristgerechte Umsetzung sollten Cloud-Anbieter folgende Schritte einleiten:

1. **Bestandsaufnahme:** Analyse der bestehenden SaaS- und Cloud-Verträge auf kritische Klauseln (zum Beispiel lange Kündigungsfristen, Wechselhindernisse) und Prüfung der aktuellen Datenexport- und Schnittstellenmöglichkeiten auf Konformität mit Data-Act-Standards.

2. **Rechtliche Anpassungen:** Überarbeitung der Vertragsmuster unter Einbezug der Data-Act-Vorgaben, besonders von Kündigungsfristen, Exit-Kosten und Transparenzpflichten. Entwicklung von Standard-Exit-Klauseln oder Übernahme der EU-Musterklauseln, sobald sie verfügbar sind.

3. **Technische Maßnahmen:** Sicherstellung der Datenportabilität in offenen, maschinenlesbaren Formaten (gegebenenfalls Implementierung oder Anpassung von Schnittstellen) und Dokumentation der Datenformate sowie Bereitstellung technischer Whitepapers oder API-Dokumentationen. Entwicklung oder Anpassung von Tools zur Migration beziehungsweise Exportfunktionalitäten für Kunden.

4. **Monitoring und Compliance:** Laufende Überwachung der Einhaltung der Data-Act-Vorgaben in Verträgen und technischen Abläufen. Vorbereitung auf externe Audits oder Zertifizierungen zur Einhaltung von Interoperabilitäts-Standards. Dokumentation aller Wechselprozesse und Kostenschätzungen zur Transparenz gegenüber Kunden.

5. **Frühzeitiger Start:** Rechtzeitige Planung und Umsetzung vor dem Geltungsbeginn. Aufbau eines Projektplans mit klaren Verantwortlichkeiten und Meilensteinen.

FAZIT

Der Data Act sorgt dafür, dass Kunden nicht mehr an einen Anbieter gebunden sind. Bis spätestens 12. September 2025 müssen Anbieter alle vertraglichen und technischen Voraussetzungen schaffen, um einen einfachen und fairen Anbieterwechsel zu ermöglichen. Wer frühzeitig handelt, kann sich durch Transparenz und Nutzerfreundlichkeit einen Wettbewerbsvorteil sichern. ■

BERNHARD HARLE
ist seit 2022 Rechtsanwalt der Technologiekanzlei Schürmann Rosenthal Dreyer Rechtsanwälte und spezialisiert auf das Datenschutzrecht und IT-Recht.

JAN O. BAIER
ist Rechtsanwalt und Fachanwalt für Urheber- und Medienrecht. Seit 2011 ist er Associated Partner der Technologiekanzlei Schürmann Rosenthal Dreyer Rechtsanwälte. Er ist spezialisiert auf das Medien-, IT-, und Datenschutzrecht sowie den gewerblichen Rechtsschutz.

www.srd-rechtsanwaelte.de

Studie zeigt: Deutsche Apps setzen verstärkt auf Werbe- und Tracking-Dienste

SMARTPHONE-APPS KONTAKTIEREN IM SCHNITT 25 SERVER UND DURCHQUEREN SECHS NETZWERKE

Bild: iff(is)

Jede Berührung des Smartphone-Displays setzt weltweit Dutzende Server in Bewegung. Eine aktuelle Untersuchung der 65 beliebtesten Apps in Deutschland offenbart die komplexen digitalen Infrastrukturen hinter alltäglichen Anwendungen. Während US-Konzerne auf eigene Netzwerke setzen, nutzen deutsche Anbieter deutlich mehr externe Dienste – mit Folgen für Datenschutz und digitale Souveränität.

In Deutschland besitzen etwa 69 Millionen Menschen ein Smartphone.[1] Das Institut für Internet-Sicherheit – if(is) hat nun analysiert, welche digitalen Infrastrukturen die beliebtesten Apps tatsächlich nutzen. Das Ergebnis: Hinter dem vermeintlich einfachen „läuft in der Cloud" verbirgt sich ein komplexes globales Netzwerk.

Für die Untersuchung wählten die Forscher 65 Apps aus den Top-50-Rankings des Google Play Stores und des iOS App Stores in Deutschland aus. Diese wurden in drei Gruppen eingeteilt: „Alle Apps" (65 Apps), „Top 20 Apps" (die meistgenutzten Anwendungen) und „Deutsche Apps" (14 Anwendungen mit Firmensitz in Deutschland). Um vergleichbare Ergebnisse zu gewährleisten, wurden alle 65 Apps vorab in funktionale Gruppen wie E-Mail, Messenger, Social Media oder Shopping eingeteilt. Innerhalb jeder Gruppe erfolgte die Nutzung nach definierten Ablaufszenarien, zum Beispiel Liken von Beiträgen in Social-Media-Apps oder das Senden und Empfangen von E-Mails in der gleichen Anzahl. Jede App wurde dabei fünf Minuten lang genutzt. Wenn möglich, wurde für jede App ein neues Nutzerkonto angelegt.

AUFZEICHNUNG UND ANALYSE DES TRAFFICS

Um den Smartphone-Traffic mitzuschneiden und zu analysieren, wurde ein neues Motorola Moto G24 mit Android 14 verwendet. Um sowohl App-spezifischen als auch den gesamten Netzwerkverkehr zu erfassen, kamen zwei Verfahren zum Einsatz:

- **On-Device-Erfassung mit PCAPdroid:** Die Android-App „PCAPdroid" zeichnet den Netzwerkverkehr einzelner Anwendungen gezielt auf. So lassen sich App-Sessions isoliert betrachten, ohne dass System- oder Hintergrundprozesse den Mitschnitt verfälschen. PCAPdroid speichert die Traffic-Daten im PCAP-Format, das später in Analyse-Tools wie Wireshark importiert werden kann.
- **Port-Mirroring im WLAN:** Zusätzlich wurde der gesamte Smartphone-Traffic, inklusive dem Android Hintergrund-Traffic, mittels Port-Mirroring an einem PC mitgeschnitten. Das Setup bestand aus **Smartphone – Access Point – Switch – Router – PC.** Der Access Point übernahm allein die WLAN-Funktion, während der Switch den Verkehr zum PC spiegelte. Auf dem PC lief Wireshark mit Filterregeln, um anhand der statisch eingestellten MAC-Adresse des Smartphones dessen Datenpakete zu ermitteln. Andere Geräte, die Traffic im Netzwerk erzeugen, wurden so zuverlässig ausgeklammert.

Um eine belastbare Datengrundlage zu gewährleisten, verzichteten die Forscher bewusst auf virtuelle Emulatoren oder Root-Berechtigungen. Zahlreiche Apps erkennen solche Umgebungen und passen ihr Netzwerkverhalten entsprechend an [3]. Zur Einordnung der erfassten IP-Adressen sowie zur Bestimmung von Hosting-Anbietern, Peering-Beziehungen und der geografischen Verteilung nutzten sie außerdem öffentlich zugängliche Datenquellen, darunter ipinfo.io, PeeringDB, GeoIP-Datenbanken sowie die weitverbreitete Hosts-Liste von Steven Black auf GitHub.

APPS VERBINDEN SICH WELTWEIT

Die Analyse des Smartphone-Datenverkehrs verdeutlicht das Ausmaß der digitalen Infrastruktur, die hinter den meistgenutzten Apps steckt. Bei den 65 untersuchten Anwendungen stellten die Forschenden fest, dass insgesamt über 1.600 Server mit unterschiedlichen IP-Adressen kontaktiert wurden. Im Durchschnitt nimmt jede App Verbindung zu rund 25 einzelnen Servern auf, und die IP-Pakete durchlaufen dabei etwa 6,35 eigenständige Netzwerke (Autonome Systeme, ASNs). Mehr als drei Viertel dieser Netzwerke und Server befinden sich in US-amerikanischer Hand.

Besonders stark vertreten sind die Rechenzentren von drei Unternehmen: Amazon, Google und Akamai. Bei diesen Anbietern wurden die meisten eindeutigen IP-Adressen registriert. In rund 90 Prozent aller Top-Apps sind sie präsent. Fast jede der 65 Anwendungen greift somit auf mindestens einen dieser drei globalen Infrastruktur-Riesen zurück.

Auch die DNS-Aktivität ist ein wichtiger Faktor. Im Durchschnitt fragt jede App 65 Domains ab, wobei etwa 13 Aufrufe pro Anwendung auf Werbe- oder Tracking-Server entfallen. Diese machen insgesamt 23 Prozent aller DNS-Anfragen aus und verdeutlichen, wie häufig Drittanbieter-Komponenten in den Datenstrom eingreifen.

Das dabei übertragene Datenvolumen ist beachtlich. Die gesamten Uploads aller Apps summieren sich auf circa 115,6 MB, während die Downloads mit rund 2,84 GB deutlich darüber liegen. Pro App entspricht das etwa 1,78 MB Upload und 43,7 MB Download. Jede Interaktion zieht somit eine nennenswerte Datenmenge nach sich.

Obwohl moderne Plattformen längst IPv6 anbieten, bleibt IPv4 mit einem Anteil von 96 Prozent das technisch dominierende Protokoll. Gleichzeitig wird rund 93 Prozent des Traffics verschlüsselt.

Die Ergebnisse der Analyse machen deutlich, dass bereits wenige Minuten Smartphone-Nutzung ein komplexes, weltumspannendes Netz aus Diensten und Verbindungen durch den Datenaustausch in Bewegung setzen.

US-DOMINANZ IN DER DIGITALEN INFRASTRUKTUR

Diese globalen Datenströme spiegeln sich auch in der Netzwerkanalyse wider: Welche Akteure die digitale Infrastruktur dominieren, verdeutlichen

die Abbildungen 1a und 1b. Sie veranschaulichen die zehn führenden autonomen Systeme, die von den 65 meistgenutzten Smartphone-Apps in Deutschland kontaktiert werden, gemessen an der Anzahl der Konversationen. Eine Konversation bedeutet dabei einen zusammenhängenden Datenaustausch zwischen Smartphone und entferntem Server, wie ihn Wireshark anhand von IP-Flows und Port-Kombinationen aufzeichnet.

Von allen aufgezeichneten Sessions entfallen 60 Prozent auf drei US-Tech-Giganten: Google mit 30 Prozent, Amazon mit 16 Prozent und Facebook mit 14 Prozent. Weitere große Content-Delivery-Netzwerke und Cloud-Provider wie Akamai, Fastly und Cloudflare erreichen jeweils Werte bis zu 14 Prozent. Insgesamt liegen mindestens 75 Prozent aller Top-ASNs in US-amerikanischer Hand, was die starke Konzentration des App-Traffics bei wenigen Anbietern unterstreicht.

Die Konzentration auf wenige Provider führt zu einer starken Abhängigkeit. Unternehmen haben oft nur begrenzten Einfluss darauf, über welche Netzknoten ihre Daten geleitet werden. Damit sind sie unmittelbar von Preisänderungen oder technischen Umstellungen der großen Anbieter betroffen.

DEUTSCHE APPS STEUERN GRÖSSERE INFRASTRUKTUREN AN

Neben der dominanten Rolle weniger US-Anbieter fällt auf, dass deutsche Apps oft deutlich komplexere Netzwerkstrukturen nutzen. Abbildung 2 zeigt, wie viele autonome Systeme die unterschiedlichen App-Gruppen durchschnittlich einbinden:

- **Alle Apps:** 6,35 autonome Systeme (Netzwerke)
- **Top 20 Apps:** 5,6 autonome Systeme (Netzwerke)
- **Deutsche Apps:** 11,35 autonome Systeme (Netzwerke)

Deutsche Anwendungen steuern fast doppelt so viele Netzwerke an wie die international dominierenden Top-20-Apps und liegen damit auch deutlich über dem Gesamtdurchschnitt.

Internationale Großanbieter betreiben häufig eigene, hochintegrierte Netzwerke und Content-Delivery-Strukturen. Durch den Betrieb eigener Rechenzentren und optimierter Peering-Vereinbarungen können sie ihren Datenverkehr gebündelt über vergleichsweise wenige autonome Systeme abwickeln. Das erklärt, warum Apps wie WhatsApp oder YouTube mit etwa fünf bis sechs autonomen Systemen pro App auskommen.

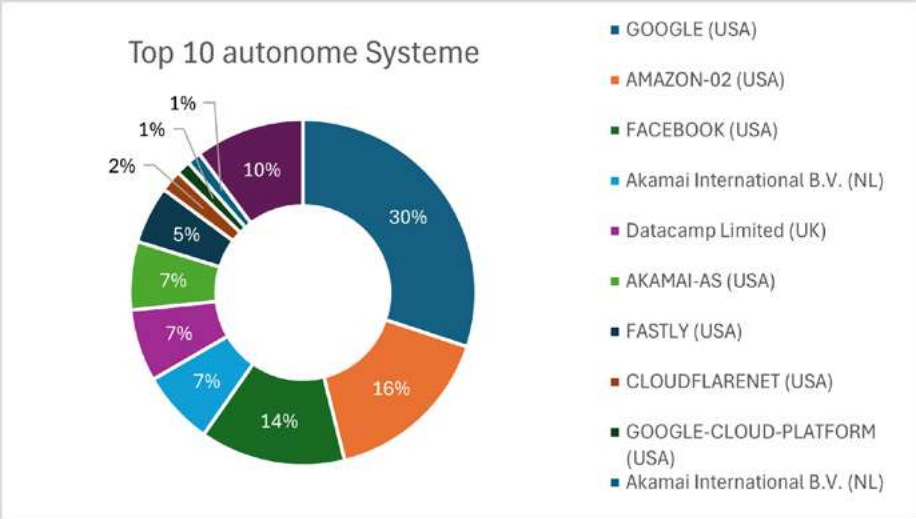


Abbildung 1a: Verteilung der autonomen Systeme bei der Unterstützung aller Apps (Bild: if(is))

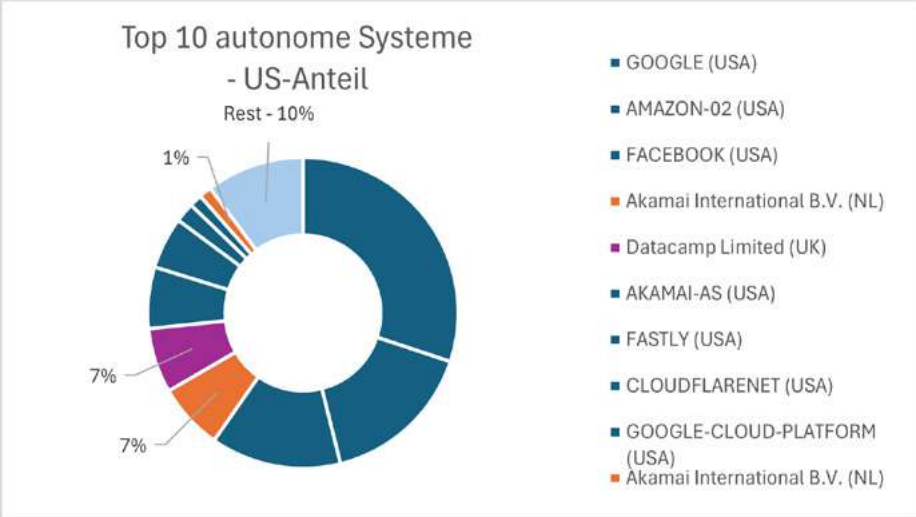


Abbildung 1b: US-Anteil aus Abbildung 1a in dunkelblau (Bild: if(is))

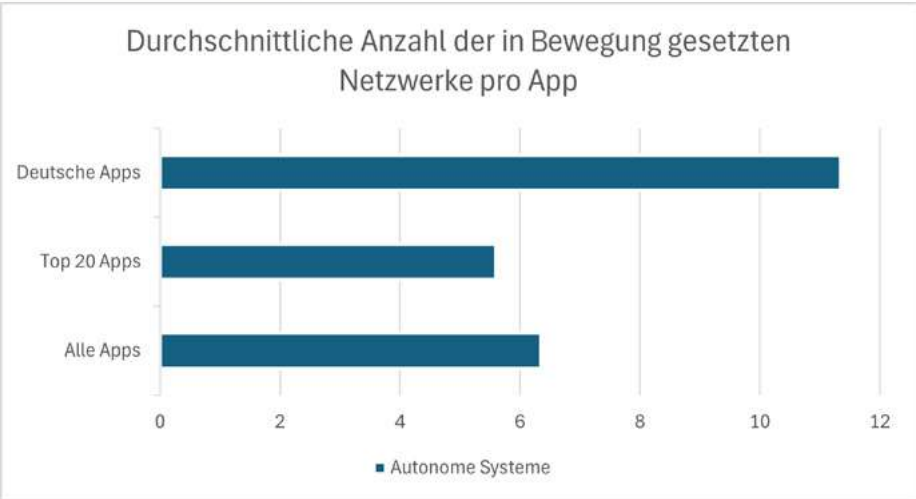


Abbildung 2: Durchschnittliche Anzahl eindeutiger Netzwerke (ASNs) mit denen eine App kommuniziert (Bild: if(is))

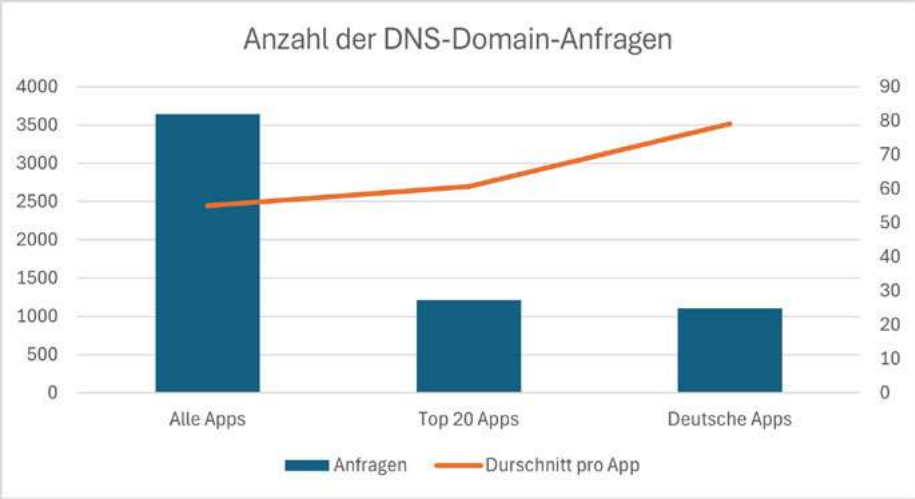


Abbildung 3: Gesamt- und durchschnittliche Anzahl an DNS-Domain-Anfragen (Bild: if(is))

Deutsche Apps hingegen nutzen seltener eine monolithische Infrastruktur. Stattdessen greifen sie auf eine Vielzahl spezialisierter externer Dienste zurück, etwa regionale Dienstleister, Analytics-Plattformen sowie Content-Delivery-Networks. Jede zusätzliche Integration spiegelt sich als weiteres autonomes System in unserer Messung wider.

Eine hohe Zahl an autonomen Systemen pro App steht einerseits für Vielfalt und Skalierbarkeit, bedeutet jedoch auch wachsende Komplexität und weniger transparente Abhängigkeiten in der Infrastruktur. Der Einsatz europäischer oder eigener Infrastrukturen könnte dabei helfen, die Abhängigkeit von US-Hyperscalern zu reduzieren und die digitale Souveränität zu stärken.

MEHR DNS-ANFRAGEN PRO APP-KATEGORIE

Neben der Vielzahl autonomer Systeme fällt bei deutschen Apps auch die DNS-Aktivität ins Auge. Hier zeigt sich ebenfalls ein deutlich komplexeres Muster. Abbildung 3 vergleicht die Gesamtzahl der DNS-Domain-Anfragen (Balken, linke Achse) und den Durchschnitt pro App (Linie, rechte Achse) für drei App-Gruppen:

- **Alle Apps:** etwa 3.600 Anfragen insgesamt, ca. 55 Anfragen pro App (65 Apps)
- **Top-20-Apps:** etwa 1.200 Anfragen insgesamt, ca. 60 Anfragen pro App (20 Apps)
- **Deutsche Apps:** etwa 1.100 Anfragen insgesamt, ca. 80 Anfragen pro App (14 Apps)

Im Durchschnitt generieren deutsche Anwendungen rund 80 DNS-Anfragen, was etwa ein Drittel mehr ist als bei den US-dominierten Top-20-Apps (60) und deutlich mehr als der Durchschnitt aller Apps (55). Dieser erhöhte DNS-Traffic deutet erneut auf eine fragmentierte Infrastruktur hin. Anstatt zentrale, eigene Nameserver zu nutzen, greifen deutsche Apps offenbar häufiger auf eine Vielzahl externer Domains und Dienste zu.

TRACKING BEI DEUTSCHEN APPS

Ein weiterer auffälliger Unterschied zeigt sich bei der Nutzung von Werbe- und Tracking-Diensten. Hier klafft die größte Lücke zwischen deutschen Apps und internationalen Anbietern. Abbildung 4 zeigt den Anteil an Werbung und Tracking der aufgerufenen Domains (Balken, linke Achse) sowie die durchschnittliche Anzahl an unterschiedlich aufgerufenen Werbe- und Tracking-Domains pro App (Linie, rechte Achse):

- **Alle Apps:** etwa 23 Prozent Werbung und Tracking, durchschnittlich circa 13 unterschiedliche Domains pro App
- **Top-20-Apps:** etwa 15 Prozent Werbung und Tracking, durchschnittlich circa neun unterschiedliche Domains pro App
- **Deutsche Apps:** etwa 41 Prozent Werbung und Tracking, durchschnittlich circa 33 unterschiedliche Domains pro App

In diesem Kontext sind mit „Werbe- und Tracking-Domains " jene Hostnamen gemeint, die typischerweise für nicht unmittelbar funktionsrelevante Dienste wie Werbung und Tracking genutzt werden. Die Quelle dieser Domains ist die weitverbreitete Open-Source-Liste „Hosts" von Steven Black.

Deutsche Anwendungen rufen deutlich mehr Werbe- und Tracking-Domains auf als US-dominierte Top-Apps und der Gesamtdurchschnitt. Das heißt jedoch nicht zwangsläufig, dass die internationalen Anbieter weniger Nutzerdaten erheben. Vielmehr setzen sie unter anderem häufiger auf serverseitiges Tracking, bei dem die Requests im Backend stattfinden und nicht über öffentlich sichtbare DNS-Abfragen laufen. Dank optimierter Infrastrukturen und moderner Integrationsmethoden können die großen Anbieter Analysen und Profiling betreiben, ohne jeden einzelnen Endpunkt im Client direkt sichtbar zu machen.

Die höhere Dichte an Werbung und Tracking bei deutschen Apps resultiert vor allem aus der Integration zahlreicher externer Drittanbieter-

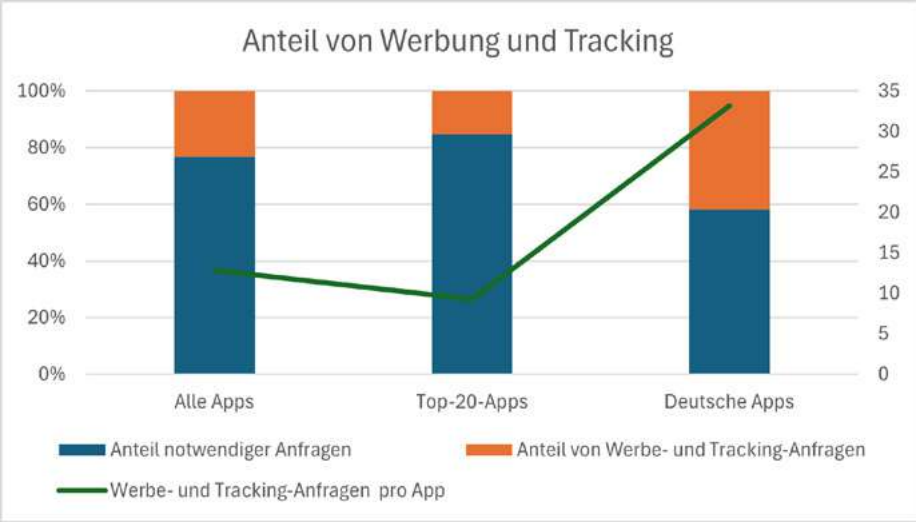


Abbildung 4: Verhältnis von Werbung und Tracking zu notwendigen DNS-Anfragen (Bild: if(is))

DIGITALE INFRASTRUKTUREN UND DIGITALE SOUVERÄNITÄT

Digitale Infrastrukturen bilden das Rückgrat unserer vernetzten Welt. Sie reichen von Glasfaserkabeln und Rechenzentren bis hin zu Content-Delivery-Netzwerken und Cloud-Plattformen großer Anbieter wie Microsoft, Google oder Amazon. Zentral ist dabei das Zusammenspiel aus Client-Server-Architektur und DNS-basierten Diensten. Smartphones lösen Hostnamen auf, initiieren API-Aufrufe an Server-Endpunkte und nutzen verteilte Dienste.

Digitale Souveränität

Digitale Souveränität bezeichnet die Fähigkeit, diese Infrastruktur sowie die übertragenen und gespeicherten Daten selbstbestimmt zu kontrollieren. Dabei sind vor allem folgende Aspekte entscheidend:

- *Geografische Verteilung: Die physische Lage von Rechenzentren hat Einfluss auf Latenz, Ausfallsicherheit und Compliance. Eine ausgewogene Mischung aus nationalen, europäischen und internationalen Standorten verringert das Risiko lokaler Störungen oder die Auswirkungen geopolitischer Spannungen.*
- *Anbieterdiversität: Die Abhängigkeiten von wenigen Hyperscalern reduziert die Handlungsspielräume und kann mit Preiserhöhungen und Leistungsänderungen einhergehen. Die Nutzung mehrerer regional verteilter Provider stärkt die Unabhängigkeit und steigert die betriebliche Resilienz.*

Entscheidend ist nicht nur die Leistungsfähigkeit einzelner Komponenten, sondern vor allem ihre Zusammensetzung und Steuerbarkeit als Gesamtsystem. Eine souveräne digitale Landschaft erfordert Vielfalt, regionale Präsenz und transparente Datenflüsse als Grundvoraussetzungen für stabile IT-Dienste.

Smartphones als Endpunkt

Smartphones fungieren heute als Endpunkte in komplexen digitalen Infrastrukturen. Nach aktuellen Zahlen der Bitkom nutzen bereits 83 Prozent aller Deutschen ein Smartphone.[1] Mit einem gemeinsamen globalen Marktanteil von rund 99 Prozent sind die dominierenden Betriebssysteme Android mit circa 72 Prozent und iOS mit 27 Prozent [2].

Smartphones und digitale Infrastrukturen wie moderne Cloud-Rechenzentren bilden eine untrennbare Symbiose. Die Portabilität und ständige Vernetzung der Smartphones ermöglichen dynamisch skalierbare Dienste, schnelle Updates und Innovationen. Dadurch rücken digitale Anwendungen direkt in unseren Alltag. Gleichzeitig vergrößert diese enge Kopplung jedoch auch Abhängigkeiten und technische Ausfallrisiken.

Zudem wirft permanentes Tracking Fragen zu Datenschutz und ökologischer Nachhaltigkeit auf.

Autonome Systeme

Das Internet besteht aus miteinander verbundenen Netzwerken, den sogenannten autonomen Systemen (AS oder ASN). Jedes autonome System ist einem Unternehmen als Betreiber zugeordnet, und alle autonomen Systeme bilden gemeinsam das Internet. Alle IP-Adressen sind den autonomen Systemen zugeordnet. Die Zuordnung eines ASN zu einem Land bezieht sich auf den Betreiber und dessen Policies, nicht zwangsläufig auf den physischen Standort der Server oder Rechenzentren. So kann ein ASN den USA zugeordnet sein, aber dennoch deutsche IP-Adressen besitzen, was verdeutlicht, wie komplex nationale Zuordnungen im globalen Datenverkehr sind.[4]

Dienste, die jeweils eigene Aufrufe erzeugen. Dadurch wird die Infrastruktur fragmentierter und die Infrastrukturen der Drittanbieter sind leichter identifizierbar. Es zeigt sich, dass die technische Umsetzung (clientseitig vs. serverseitig) die Messbarkeit deutlich beeinflusst, jedoch nicht zwangsläufig das tatsächliche Ausmaß der Datenerfassung.

DIE 15 GRÖSSTEN NETZWERKE NACH ANZAHL IHRER IP-ADRESSEN

Neben DNS-Abfragen und autonomen Systemen lohnt auch ein Blick auf die IP-Adressen selbst. Sie zeigen, welche Anbieter hinter der Infrastruktur der Apps stehen und wie viele eindeutige IP-Adressen von den 65 untersuchten Smartphone-Apps jeweils pro Netzwerk (ASN) kontaktiert werden. Mit 338 einzelnen IPs führt Amazon.com das Feld an, gefolgt von Google LLC (237 IPs) und Akamai Technologies (142 IPs). Microsoft belegt mit 74 IP-Adressen den vierten Platz, dicht gefolgt von Cloudflare (62) und Google Cloud (61). Unter den Top 15 finden sich außerdem klassische Hyperscaler wie Amazon AES (48 IPs), welches Amazons IP-Raum erweitert sowie spezialisierte CDN- und Hosting-Anbieter, wie Fastly (27) und CDN77 (24). Mit OVHcloud (30), IONOS SE (20 IPs) und Hetzner Online (17 IPs) sind auch deutsche beziehungsweise europäische Provider vertreten.

Die Anzahl unterschiedlicher IP-Adressen pro Netzwerk spiegelt das Ausmaß und die Breite der Netzwerkinfrastruktur wider, über die App-Daten geroutet werden. Große Cloud- und CDN-Anbieter unterhalten global verteilte Serverfarmen mit Hunderten von IP-Adressen, um geringe Latenzen, hohe Ausfallsicherheit und Lastverteilung sicherzustellen.

Gleichzeitig lässt sich aus der Verteilung ablesen, welche Anbieter für die beliebtesten Apps in Deutschland unverzichtbar sind. Hyperscaler dominieren nicht nur die Konversationsstatistik, sondern stellen auch die umfangreichsten Adressräume bereit. Die Präsenz europäischer Provider unter den Top 15 zeigt, dass regionale Provider zwar vorhanden sind, jedoch in IP-Kapazität und geografischer Abdeckung hinter den Big-Tech zurückbleiben. Die Daten machen deutlich, dass Smartphone-Apps eng mit wenigen globalen Infrastrukturgebern verbunden sind. Deshalb ist es wichtig, diese Verbindungen bei Architektur- und Betriebsentscheidungen zu berücksichtigen.

WELCHE APPS VERBRAUCHEN AM MEISTEN DATEN?

Doch nicht nur, wohin Daten fließen, ist entscheidend – sondern auch, wie viele Daten einzelne Apps verursachen. Dabei zeigen sich deutliche Unterschiede zwischen den einzelnen App-Kategorien:

- **Grocery-Apps** senden im Schnitt 1,0 MB und empfangen etwa 14,2 MB, ein Verhältnis von rund 1 zu 14. Dies spiegelt den hohen Download-Anteil wider, da Produktbilder, Preise und Angebote kontinuierlich nachgeladen werden.
- **Mail-Apps** zeigen ein differenziertes Bild. Im Gesamtdurchschnitt werden 2,5 MB gesendet und 40,3 MB empfangen (1 zu 16). Entfernt man allerdings GMX und Web.de, sinkt

das Verhältnis auf rund 1,8 MB gesendet zu 3,7 MB empfangen (1 zu 2). Outlook und Gmail folgen diesem schlankeren Profil. GMX und Web.de binden über ihre Kernfunktionen hinaus Cloud-Speicher, News-Feeds und weitere Zusatzdienste ein, was das Datenvolumen deutlich erhöht. Outlook und Gmail beschränken sich hingegen weitgehend auf den reinen E-Mail-Verkehr, weshalb ihr Traffic-Profil deutlich schlanker ausfällt.

- **Messenger-Apps** senden im Schnitt 5,0 MB und empfangen 23,6 MB (1 zu 4,8). Hier dominieren Medien- und Dateitransfers innerhalb Chats.
- **Shopping-Apps** weisen mit 2,9 MB zu 34,5 MB (1 zu 12) ein ähnliches Muster wie Grocery auf, allerdings auf einem höheren Datenvolumen insgesamt, da detaillierte Produktansichten und personalisierte Empfehlungen übertragen werden.
- **Social-Apps** schließlich liegen mit 1,0 MB an gesendeten und 31,8 MB an empfangenen Daten (1 zu 32) an der Spitze des Down-/Up-Verhältnisses, bedingt durch kontinuierliches Laden von Feeds, Bildern und Videos.

In allen Kategorien überwiegt deutlich der Download-Anteil. Die Mail-Apps ohne GMX und Web.de bilden eine Ausnahme, die zeigt, dass das Datenprofil stark von integrierten Zusatzdiensten abhängt. Insgesamt verdeutlichen diese Werte, welche App-Typen besonders viele Daten verbrauchen und wo die Hauptlast im mobilen Datenverkehr liegt.

IPV4- VERSUS IPV6-ANTEIL IM APP-TRAFFIC

Abbildung 5 veranschaulicht den prozentualen Anteil von IPv4- und IPv6-Verbindungen aller untersuchten Smartphone-Apps. Von sämtlichen aufgezeichneten Verbindungen entfallen rund 96 Prozent auf IPv4-Adressen, während nur etwa 4 Prozent der Verbindungen über IPv6 laufen.

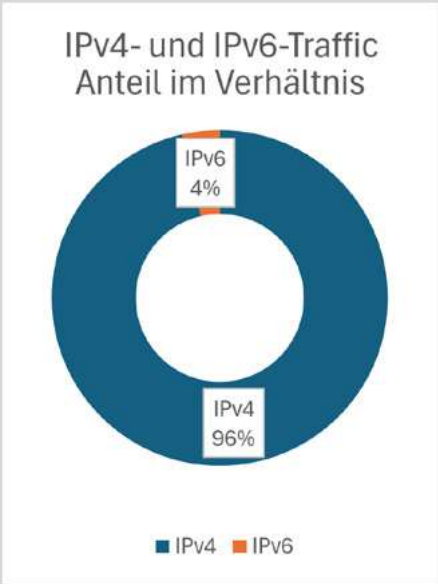


Abbildung 5: Vergleich des Anteils von IPv4- und IPv6-Traffic (Bild: if(is))

Interessanterweise bleibt IPv6 damit selbst bei den beliebtesten Apps weiterhin eine Randerscheinung. Obwohl zahlreiche Provider und Apps IPv6 unterstützen, dominieren in der Praxis nach wie vor IPv4-Adressen. Dies lässt sich vor allem auf drei Faktoren zurückführen. Zum einen sind viele etablierte Anwendungen und Backend-Dienste nach wie vor auf IPv4 ausgelegt, um maximale Kompatibilität und einen reibungslosen Betrieb zu gewährleisten. Einige Netzbetreiber und Content-Delivery-Network-(CDN)-Anbieter schrecken vor einer kompletten Abschaltung ihrer IPv4-Umgebungen zurück, da sie unerwartete Störungen befürchten. Um die flächendeckende Nutzung auszubauen, ist man außerdem auf die Umstellung von Diensten von Drittanbietern auf IPv6 angewiesen.

Die Messwerte basieren auf der kombinierten Auswertung des gesamten Smartphone-Traffics, inklusive Android-Hintergrundaktivitäten, die nicht in allen Endgeräte-Logging-Tools sichtbar sind. Dadurch ergibt sich ein vollständigeres Bild des tatsächlichen Protokolleinsatzes im mobilen Alltag.

Bei der Verschlüsselung der Datenübertragung zeigt sich ein erfreulich hohes Niveau. Etwa 93 Prozent des gesamten Datenverkehrs der analysierten Apps werden über gesicherte Protokolle übertragen, nur etwa 7 Prozent bleiben unverschlüsselt.

Dieses Ergebnis zeigt, dass App-Anbieter und Plattformbetreiber dem Schutz von Nutzerdaten heute eine hohe Priorität einräumen.

FAZIT

Smartphones sind Endpunkte einer globalen digitalen Infrastruktur. Die Untersuchung zeigt, dass deutsche Apps im Durchschnitt mehr Server und Domains ansteuern als ihre internationalen Konkurrenten – ein Hinweis auf komplexe und fragmentierte Backend-Strukturen. Um die Symbiose von Smartphone und digitalen Infrastrukturen effizienter, unabhängiger und ressourcenschonender zu gestalten, ist Transparenz über diese Datenflüsse unerlässlich. ■

FERHAN KESICI
studiert den Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Analyse der Nutzung der digitalen Infrastruktur durch Smartphone-Apps".

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.

Literatur

[1] *Statista. „Smartphone-Nutzung in Deutschland." Online verfügbar unter: https://de.statista.com/themen/6137/smartphone-nutzung-in-deutschland (Zugriff am 8. Juli 2025).*

[2] *StatCounter. „Mobile Operating System Market Share Worldwide." Online verfügbar unter: https://gs.statcounter.com/os-market-share/mobile/worldwide/ (Zugriff am 8. Juli 2025).*

[3] *OWASP. „MAS Testing Guide – Tampering and Reverse Engineering: Why You Need It." Online verfügbar unter: https://mas.owasp.org/MASTG/0x04c-Tampering-and-Reverse-Engineering/#why-you-need-it (Zugriff am 8. Juli 2025).*

[4] *Cloudflare. „What is an Autonomous System?" Online verfügbar unter: https://www.cloudflare.com/de-de/learning/network-layer/what-is-an-autonomous-system/ (Zugriff am 8. Juli 2025).*

VORSCHAU Ausgabe 5|25 OKTOBER/ NOVEMBER

SCHWERPUNKT: it-sa – Produkte, Services und Lösungen

Die it-sa Expo&Congress in Nürnberg hat sich zum größten europäischen Branchenevent für Cybersicherheit entwickelt. Mit einem Besucherrekord von über 25.000 Fachbesuchern und 897 Ausstellern zeigte die it-sa 2024 eindrucksvoll, wie relevant das Thema Cybersicherheit für Wirtschaft, Staat und Gesellschaft ist.

Im kommenden Heft widmen wir uns diesem zentralen Marktplatz für IT-Security-Lösungen. In unserem Schwerpunkt werden die wichtigsten Entwicklungen, Produkte und Trends von der Messe beleuchtet– von neuen Security-Plattformen über KI-gestützte Angriffserkennung bis hin zu Managed Services und Lösungen für kritische Infrastrukturen.

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

Das Heft erscheint am 1. Oktober 2025.

IT-SICHERHEIT
Management und Technik

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

Chefredaktion:
Sebastian Frank (S.F.)
(verantwortlich für den redaktionellen Teil)
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 (verantwortlich für den Anzeigenteil)
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 31

Vertrieb/Herstellung:
Torid Kehmeier
Tel.: +49 2234 98949-78
Torid.kehmeier@datakontext.com

Hersteller:
DATAKONTEXT GmbH
Augustinusstr. 11A, 50226 Frechen

Kontakt und Informationen zum Thema Produktsicherheitsverordnung:
Per Telefon: +49 2234 98949-99
Per Mail: dieter.schulz@datakontext.com
www.datakontext.com/produktsicherheitsverordnung

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.

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.

Titelbild: ImageFlow - stock.adobe.com

Fotos: Firmenbilder; Bitdefender; if(is); ChatGPT Image; (Aksaka, Andrey Popov, Autism in Focus, Ceylon Frames, Eshana, ImageFlow, Leopard, Li, Maryna, mattegg, Naru, our_future, Pixelpulse Creative, Pixel Studio, redflower, Tondone, wetzkaz, WrightStudio) - stock.adobe.com

31. Jahrgang 2025 · ISSN: 1868-5757

Awareness, die wirkt!

Wecken Sie die Superhelden in Ihrem Unternehmen

Das E-Learning für nachhaltige Awareness in der IT-Sicherheit.

Inhalte

- Social Engineering
- Phishing
- Malware
- CEO-Fraud
- Deep Fakes

Jetzt testen:
www.itsicherheit-online.com/elearning

DATAKONTEXT