HZ219245 · ISSN 1868-5757 · www.itsicherheit-online.com Oktober/November 5/2025

IT-SICHERHEIT

Management und Technik

Gut gerüstet für NIS-2

Mit einem ISMS zur gelebten Sicherheitskultur

INKLUSIVE SPECIAL
it-sa 2025

- **KI-Sicherheit:** Sind universelle Plattformen die Lösung?
- **Resilienz:** Wie Unternehmen ihre Handlungsfähigkeit sichern können
- **Marktüberblick:** Relevante Produkte und Dienstleistungen

Wenn Angreifer den Vertrag testen
Rechtliche Vorsorge als Teil der Cyberabwehr

Agenten-Wildwuchs
Klare Regeln für digitale Kollegen

Mobile Unabhängigkeit
Wege jenseits von iOS und Android

DATAKONTEXT

IT-SICHERHEIT
Management und Technik

<kes>
Die Zeitschrift für
Informations-Sicherheit

Yulia - stock.adobe.com

Wir sind IT-Sicherheit!

Besuchen Sie uns auf der it-sa 2025.

Halle 7 **Stand 106**

Liebe Leserinnen, liebe Leser,

die it-sa in Nürnberg gilt seit Jahren als Leitmesse für IT-Sicherheit – und sie macht einmal mehr deutlich: Cybersecurity ist längst kein Nischenthema mehr, sondern eine der zentralen Fragen für Wettbewerbsfähigkeit, Innovation und Gesellschaft. Künstliche Intelligenz, Resilienz und geopolitische Unsicherheiten fordern Unternehmen und Behörden gleichermaßen heraus. Im Schwerpunkt dieser Ausgabe greifen wir unter anderem diese Themen auf: Wie lassen sich KI-Anwendungen durch universelle Plattformen absichern (Seite 14)? Welche Rolle können Chief Resilience Officers künftig für die Handlungsfähigkeit unter Krisenbedingungen spielen (Seite 12)? Ergänzend zeigen wir, wie unkontrollierter Agenten-Wildwuchs durch Schatten-KI entsteht, und warum Unternehmen ihre digitalen Helfer mit festen Regeln verwalten sollten – vom Onboarding bis zum Offboarding (Seite 60).

Darüber hinaus richten wir in dieser Ausgabe den Blick nach vorn: Ein Ausblick bis 2030 beschreibt neun Handlungsfelder der Cybersicherheit – von Zero Trust über digitale Souveränität bis zum strategischen Talentmanagement. Im Artikel von Deloitte wird gezeigt, warum Security zur Führungsaufgabe wird und wie sich Technologie mit Organisationsentwicklung zu einem Zukunftsbild verbindet, das nicht erst in ferner Zukunft, sondern schon heute Vorbereitung verlangt (Seite 30).

Wie verwundbar Unternehmen aktuell sind, verdeutlicht der Beitrag zur OT-Cyberresilienz: Produktionsbetriebe benötigen Notfallpläne, um auch bei IT-Totalausfällen arbeitsfähig zu bleiben. Das Playbook für den Ernstfall (Seite 32) zeigt, wie Vorbereitungszeit, klare Rollen und strukturierte Fallbacks über Erfolg oder Stillstand entscheiden – und warum die Produktion immer enger mit IT-Fragen verknüpft ist.

Ein weiterer Autor behandelt die Blackout-Resilienz von Rechenzentren: Solar, Biogas, Batteriespeicher und KI-gestütztes Lastmanagement werden zu einem Standortfaktor – nicht nur für Betreiber, sondern auch für die digitale Infrastruktur ganzer Volkswirtschaften (Seite 36). Gerade hier zeigt sich, dass Resilienz nicht allein technisch ist, sondern auch politische und wirtschaftliche Dimensionen hat.

Schließlich geht es um Abhängigkeiten: Ab 2027 gilt eine verpflichtende *Software Bill of Materials* (SBOM) für Lieferketten (Seite 68), während bei mobilen Endgeräten Alternativen jenseits von Google und Apple gefragt sind (Seite 54). Beide Themen berühren die Frage, wie Unternehmen ihre digitale Souveränität sichern können und wie Europa seine Handlungsspielräume in Krisen- und Technologiekonflikten wahren kann.

Die it-sa setzt die Themen, diese Ausgabe nimmt sie auf: Sicherheit ist mehr als Technik. Sie umfasst Governance, Strategie und Resilienz. Sie verlangt, Menschen einzubinden, Prozesse anzupassen und Strukturen so zu gestalten, dass Krisen nicht zur Katastrophe werden.

Viel Freude bei der Lektüre,
Ihr Sebastian Frank

www.itsicherheit-online.com/
newsletter

LEIPZIGER MESSE

protekt
25.–26.11.2025
leipzig

ihre leitkonferenz

jetzt online ticket buchen!

wissen vernetzen.
KRITIS schützen.

www.protekt.de

INHALT

38 GUT VORBEREITET AUF DEN DIGITALEN ERNSTFALL
WIE SICH MIT EINEM ISMS SICHERHEITSKULTUR IM UNTERNEHMEN ETABLIEREN LÄSST

TREND MICRO SPONSERT **MCLAREN**

Der Cybersicherheitsanbieter Trend Micro wird offizieller Partner des McLaren Formel-1-Teams für den Rest der Saison 2025 und darüber hinaus. Die Partnerschaft baut auf der bestehenden Zusammenarbeit im Elektro-Rennsport auf, wie McLaren Racing mitteilte. „Ihr Fachwissen war bei der Unterstützung des Teams im Elektro-Rennsport von unschätzbarem Wert", erklärt Matt Dennington, Co-Chief Commercial Officer bei McLaren Racing. Die Zusammenarbeit verbinde zwei Unternehmen, deren Kerngeschäft Innovation sei und die sich der Sicherheit in dynamischen Umgebungen verschrieben hätten.

Im Rahmen der Partnerschaft sind während der gesamten Formel-1-Saison Aktivitäten mit Kunden und Partnern geplant, bei denen diese das McLaren-Team kennenlernen und sich zu sicherheitsrelevanten Themen austauschen können. McLaren Racing wurde 1963 gegründet und hat seither 21 Formel-1-Weltmeisterschaften sowie 200 Grands Prix gewonnen. ■

MATERNA VIRTUAL SOLUTION MIT NEUER GESCHÄFTSFÜHRUNG

Materna Virtual Solution hat Daniel Zimmermann zum Geschäftsführer berufen. Der 43-Jährige leitet das Unternehmen seit dem 1. September gemeinsam mit Volkan Gümüs. Zuvor war Zimmermann Geschäftsführer bei rola Security Solutions mit rund 350 Mitarbeitenden. Frühere Stationen seiner Laufbahn waren eine Unternehmensberatung, die Deutsche Telekom und T-Systems, bevor er 2018 zu rola wechselte.

Das Münchener Unternehmen entwickelt Lösungen für sicheres mobiles Arbeiten, darunter die Container-App SecurePIM und die Office-Suite SecurePIM WorkSPACE. Sämtliche Produkte entstehen nach eigenen Angaben in Deutschland und sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprüft. Materna Virtual Solution gehört zur Materna-Gruppe. ■

NOVASTOR UND **CRAYON** KOOPERIEREN BEI BACKUP-SERVICES

Der Hamburger Backup-Hersteller NovaStor und der Channel-Spezialist Crayon haben eine Partnerschaft angekündigt. Die Zusammenarbeit soll Systemhäuser, Managed Service Provider (MSPs), Hoster und Rechenzentren beim Aufbau von Managed Backup Services unterstützen. Die Partner setzen nach eigenen Angaben auf deutsche Software als Wettbewerbsvorteil gegenüber nicht europäischen Anbietern. Mit der in Hamburg entwickelten Backup-Software NovaStor DataCenter 10 wollen sie eine Grundlage für differenzierende Managed Services schaffen.

„Systemhäuser und MSPs stehen vor der Aufgabe, neue Services zu entwickeln und gleichzeitig den steigenden Anforderungen ihrer Kunden an Sicherheit gerecht zu werden", erklärt Axel Gillert, Director Channel Sales bei Crayon. Besonders wichtig sei dabei, die digitale Souveränität von IT-Infrastrukturen zu stärken. Stefan Utzinger, Geschäftsführer der NovaStor GmbH, betont die Vorteile der deutschen Entwicklung: „Mit NovaStor DataCenter bieten wir eine in Deutschland entwickelte Software, die Sicherheit, Compliance und direkte Nähe zum Hersteller verbindet." ■

VDE WARNT VOR CHIP-ABHÄNGIGKEIT

Der VDE warnt vor einer wachsenden europäischen Abhängigkeit in der Mikroelektronik und fordert entschlossenes Handeln. In seinem neuen Positionspapier „Hidden Electronics IV" kritisiert der Verband, dass Europa trotz massiver Investitionen in den USA und Asien den Anschluss zu verlieren droht. „In der Mikroelektronik sind wir viel zu abhängig von anderen Regionen der Welt", erklärt Prof. Christoph Kutter, Direktor des Fraunhofer-Instituts für Elektronische Mikrosysteme und Festkörper-Technologien (EMFT) sowie stellvertretender VDE-Präsident.

Das auf dem VDE-Jahresempfang in Brüssel vorgestellte Papier sieht gravierende Defizite beim Chipdesign: Die wichtigsten Designwerkzeuge stammen fast ausschließlich aus den USA. Europa müsse daher eine eigene Electronic-Design-Automation-(EDA)-Kompetenz aufbauen und Open-Source-Ansätze wie RISC-V fördern. Vollständige Autarkie sei kein realistisches Ziel, jedoch die Verringerung kritischer Abhängigkeiten durch strategische Partnerschaften mit Japan, Taiwan oder Singapur. „Ohne koordiniertes Vorgehen wird Europa in der Mikroelektronik dauerhaft in die zweite Reihe abrutschen", betont Dr. Ronald Schnabel von der VDE/VDI Gesellschaft Mikroelektronik. ■

ARCSERVE MIT NEUEM VERTRIEBSLEITER FÜR EMEA

Der Datenresilienz-Anbieter Arcserve hat Danilo Labovic zum Vice President of Sales für die Region Europa, Naher Osten und Afrika (EMEA) ernannt. Labovic verfügt über rund 25 Jahre Erfahrung im internationalen Vertriebsmanagement und war zuvor in Führungspositionen bei CA Technologies, Palo Alto Networks, Verisign und Symantec tätig. ■

SEPPMAIL DEUTSCHLAND FEIERT ZEHNJÄHRIGES BESTEHEN

Der E-Mail-Verschlüsselungsanbieter SEPPmail Deutschland begeht im August sein zehnjähriges Firmenjubiläum. Das Münchener Unternehmen bietet seit 2015 Lösungen für E-Mail-Verschlüsselung und sicheren Nachrichtenaustausch.

SEPPmail ist ein Spezialist für sichere E-Mail-Kommunikation in verschiedenen Branchen. Das Unternehmen entwickelt Technologien für E-Mail-Verschlüsselung, digitale Signatur und sicheren Nachrichtenaustausch, die sich nach Herstellerangaben nahtlos in bestehende IT-Infrastrukturen integrieren lassen.

„Unsere Vision ist heute so aktuell wie bei der Gründung: Wir wollen digitale Kommunikation so sicher wie nötig und gleichzeitig so einfach wie möglich machen", erklärt Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH. Das inhabergeführte Unternehmen mit Sitz in der Schweiz und Deutschland vermarktet seine Technologie weltweit. Die Lösungen verschlüsseln elektronische Nachrichten und versehen diese optional mit digitaler Signatur. SEPPmail betont die Benutzerfreundlichkeit seiner Produkte und wirbt damit, dass keine zusätzlichen Schulungen erforderlich seien. ■

PROCILON ÜBERNIMMT ÖSTERREICHISCHEN IDENTITÄTSPRÜFUNGS-SPEZIALISTEN

Der Düsseldorfer IT-Sicherheitsanbieter Procilon hat den österreichischen Spezialisten POS Solutions übernommen. Das Unternehmen will damit nach eigenen Angaben seine Position im Bereich digitaler Identitätsprüfung stärken. Die Transaktion ist die erste im Rahmen einer Buy-and-Build-Strategie, die von der Beteiligungsgesellschaft Main Capital Partners unterstützt wird.

POS Solutions mit Sitz in Braunau am Inn entwickelt Lösungen für digitales Onboarding, Online-Identifikation und elektronische Signaturen. Das 2009 gegründete Unternehmen beschäftigt rund 16 Mitarbeiter und betreut nach eigenen Angaben über 150 Kunden, darunter Banken, Versicherungen und Telekommunikationsanbieter in der DACH-Region. Die Lösungen entsprechen den internationalen eIDAS-Vorschriften.

Procilon entwickelt Sicherheitssoftware und digitale Vertrauenslösungen für Behörden und Betreiber kritischer Infrastrukturen. Das Unternehmen mit rund 100 Beschäftigten an drei Standorten ist hauptsächlich in Deutschland und in der Schweiz aktiv. ■

DIGICERT BETEILIGT SICH AN NIST-INITIATIVE ZU DEVSECOPS

DigiCert nimmt an einem Projekt des National Cybersecurity Center of Excellence (NCCoE) des US-amerikanischen National Institute of Standards and Technology (NIST) teil. Das Vorhaben zielt darauf ab, sichere DevSecOps-Praktiken in der Software-Entwicklung zu stärken. Der Digital-Trust-Anbieter schließt sich 13 weiteren Technologieunternehmen an, darunter Google, Microsoft, IBM, Palo Alto Networks, CyberArk, Dell Technologies und GitLab. Gemeinsam wollen die Partner integrierte Lösungen zur Verbesserung der Software-Lieferketten-Sicherheit entwickeln.

Hintergrund sind zunehmende Angriffe auf Software-Lieferketten, die nach Einschätzung der Beteiligten vertrauenswürdige Absicherungsmethoden für Entwicklungsumgebungen erforderlich machen. Das von der US-Regierung geförderte Projekt soll eine unabhängige Bewertung ermöglichen, wie sich verschiedene Technologien integrieren und die Software-Integrität verbessern lassen. „Sichere Softwareentwicklungsprozesse basieren häufig auf fragmentierten Tools, die sich über den gesamten Software-Lebenszyklus hinweg nicht gut integrieren oder skalieren lassen", erklärt Tim Hollebeek, Vice President of Industry Standards bei DigiCert. Das Projekt solle Wege aufzeigen, wie sich vertrauenswürdige Technologien zu einem zusammenhängenden, risikobasierten DevSecOps-Ansatz koordinieren lassen. Das NCCoE will praxisnahe Implementierungen entwickeln, die über theoretische Konzepte hinausgehen und Security- sowie Compliance-Ziele mit aktuellen Werkzeugen erreichen. ■

UMBRELLA SECURITY OPERATIONS KOOPERIERT MIT SILVERFORT

Der IT-Sicherheitsdienstleister Umbrella Security Operations hat eine Partnerschaft mit dem Identity-Security-Anbieter Silverfort angekündigt. Die Zusammenarbeit zielt nach Angaben der Unternehmen darauf ab, Identitätssicherheit über verschiedene Umgebungen und Ressourcen hinweg zu gewährleisten.

Silverfort kritisiert fragmentierte Sicherheitsansätze: „Das Hauptproblem vieler Unternehmen ist, dass sie Sicherheit zu kurz fassen. Ganzheitliche Konzepte fehlen, stattdessen setzen sie allenfalls vereinzelt Lösungen ein", erklärt Dr. Shahriar Daneshjoo, VP Sales EMEA Central bei Silverfort.

Die Identity Security Platform des Anbieters soll über die Runtime-Access-Protection-(RAP)-Technologie alle Authentifizierungen in Active Directory zentral überwachen. Sebastian Rohr, Managing Director von Umbrella Security Operations, betont die praktischen Vorteile: „Alleine mit der in wenigen Stunden umgesetzten Analyse können wir unseren Bestandskunden die Augen öffnen und bisher unentdeckte Risiken aufzeigen."

Das Konzept umfasst nach Herstellerangaben nicht nur menschliche Nutzer, sondern auch privilegierte Anwender, nicht menschliche Identitäten (NHIs) und KI-Agenten. Die Plattform soll Sicherheitsmaßnahmen über On-Premises-, Hybrid-, Cloud- und Multi-Cloud-Umgebungen konsolidieren und Legacy-Systeme bis hin zu modernen SaaS-Anwendungen abdecken. ■

Anzeige

noris network

Ihr Premium IT-Dienstleister für
zukunftssichere Cloud-Lösungen

- **Maximale Sicherheit und Vertrauen:** Hochsichere, zertifizierte Rechenzentren in Deutschland
- **Flexibilität nach Maß:** Private, Public oder Hybrid Cloud – individuell anpassbar und hochverfügbar
- **Passgenaue Lösungen:** Vielfältige Cloud-Services für Ihre individuellen Anforderungen
- **Regelkonform und zuverlässig:** Expertenwissen für Governance, Compliance und Datenschutz
- **Transparente Kosten:** Keine versteckten Gebühren

it sa
7.-9.10.2025
Messe Nürnberg
Halle 7 / 7-212

Jetzt informieren

BOX INTEGRIERT MISTRAL AI

Box hat eine Partnerschaft mit Mistral AI angekündigt und integriert den Dialogassistenten Le Chat über den Box MCP Server in seine Intelligent-Content-Management-Plattform. Nutzer können damit Dateien in Box durchsuchen, zusammenfassen, analysieren und für die Erstellung neuer Inhalte verwenden, ohne die gewohnte Arbeitsoberfläche zu verlassen. Die Integration ermöglicht kommunikative Interaktion mit Box-Dateien in mehreren Sprachen, darunter Deutsch, Englisch, Französisch und Spanisch. Nutzer können Informationen aus großen Dokumentbibliotheken extrahieren und innerhalb der Mistral-Workflows mit Box-Inhalten arbeiten, während die Sicherheits- und Governance-Berechtigungen von Box erhalten bleiben.

„KI liefert den höchsten ROI für Unternehmen, wenn diese an ihre Bedürfnisse angepasst und durch die einzigartigen Geschäftsinhalte und Daten der Unternehmen angereichert wird", erklärt Ben Kus, Chief Technology Officer bei Box. Software-Entwickler können ihre Coding-Workflows beschleunigen, da Le Chat kontextbezogene Code-Schnipsel anzeigen kann. Die Integration setzt auf hardwarebasierte Sicherheit und Datensparsamkeit. ■

EUDI-WALLET-KERN FÜR DIGITALE IDENTITÄTEN

Die Bundesdruckerei-Gruppe realisiert im Auftrag der Bundesagentur für Sprunginnovationen (SPRIND) das Hintergrundsystem für die Ausstellung der Person Identification Data (PID), die als digitale Kernidentität der EUDI-Wallet dient. Das Projekt wird aus Mitteln des Bundesministeriums für Digitales und Staatsmodernisierung finanziert.

Das System erstellt aus den im Chip des Personalausweises hinterlegten personenbezogenen Daten eine PID, die als interoperable und rechtssichere digitale Kernidentität in die EUDI-Wallet auf das Smartphone übertragen wird. Der PID-Provider-Dienst nutzt die bereits notifizierte Online-Ausweisfunktion und Hardware-Sicherheitsmodule für die Verarbeitung hochschützenswerter Daten. „Mit dem produktiven PID-Provider-Dienst setzt die Bundesdruckerei als Expertin für digitale Identitäten und sichere Infrastrukturen eine Kernkomponente für das deutsche EUDI-Wallet-Ökosystem um", sagt Dr. Daniel Fett, Product Owner Wallet Infrastructure bei SPRIND. Benutzer können künftig ihre wichtigsten Identitätsdaten wie Name, Nationalität und Geburtsdatum grenzüberschreitend in den 27 EU-Staaten für verschiedenste Zwecke verwenden. Die Entwicklungsergebnisse werden als Open Source bereitgestellt. ■

EXPRESS-KURSE FÜR IT-SICHERHEITS-FACHKRÄFTE

Die internationale Cybersecurity-Organisation ISC2 hat 14 neue Online-Express-Kurse vorgestellt. Die ein- bis zweistündigen On-Demand-Angebote decken Themen wie Cloud-Sicherheit, Governance, Risk and Compliance (GRC), Datenschutz sowie Sicherheitsbewusstsein ab.

Laut einer aktuellen ISC2-Studie sind vor allem Cloud-Sicherheit und Risikomanagement besonders gefragte Kompetenzen. Die Kurse sollen Fachkräfte bei der Weiterbildung in diesen Bereichen unterstützen. Das Themenspektrum reicht von Sicherheitsbildung (SETA) über Container- und Virtualisierungstechnologien bis zu Standards für kritische Infrastrukturen und OT-Umgebungen.

Die Kurse sind für ISC2-Mitglieder vergünstigt über „My Courses" und für Nichtmitglieder über die Website des Verbands verfügbar. Teilnehmer können je nach Umfang 0,5 bis 1,0 CPE-Credits erwerben. ISC2 zählt nach eigenen Angaben weltweit über 265.000 zertifizierte Mitglieder. ■

PAM-PLATTFORM ERHÄLT KI-FUNKTIONEN

Keeper Security hat mit KeeperAI eine Erweiterung seiner PAM-Plattform vorgestellt. Die agentenbasierte Lösung soll privilegierte Sitzungen in Echtzeit überwachen, Bedrohungen klassifizieren und bei verdächtigem Verhalten automatisch reagieren. Nach Herstellerangaben analysiert KeeperAI Sitzungsmetadaten, Tastenanschlagprotokolle und Befehlsausführungen, um ungewöhnliche Aktivitäten zu erkennen. Befehle werden in Risikostufen eingeteilt, riskante Sitzungen können automatisch beendet oder überwacht werden.

Die Lösung unterstützt die Anbindung an Large-Language-Model-Dienste wie AWS Bedrock, Anthropic, Google Gemini und OpenAI. Anpassbare Richtlinien sollen eine individuelle Risikoklassifizierung ermöglichen. Derzeit ist KeeperAI für SSH-Sitzungen verfügbar, eine Erweiterung auf weitere Protokolle wie RDP oder Datenbanken ist angekündigt. ■

„HALL OF FAME" FÜR E-MAIL-SICHERHEIT VERÖFFENTLICHT

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemeinsam mit eco und Bitkom rund 150 Unternehmen ausgezeichnet, die moderne E-Mail-Sicherheitsmaßnahmen umgesetzt haben. Grundlage sind die Technischen Richtlinien TR-03108 für sicheren Transport und TR-03182 für E-Mail-Authentifizierung. Erstere sorgt für die Verschlüsselung während der Übertragung, letztere für die Erkennung gefälschter Absenderadressen.

Parallel startet das BSI eine Awareness-Kampagne für Verbraucher. Ein neuer E-Mail-Checker soll anzeigen, ob der jeweilige Anbieter die Kriterien erfüllt. Zudem stellt ein „Wegweiser Kompakt" acht Tipps für mehr Sicherheit im digitalen Alltag bereit. Weitere Informationen finden sich unter www.einfachabsichern.de ■

ABO-MODELL FÜR BACKUP-SPEICHER GESTARTET

Object First führt in Europa ein nutzungsbasiertes Abonnementmodell für seine Backup-Speicherlösung Ootbi ein. Kunden können nun zwischen einem CapEx-Modell und einem flexiblen Verbrauchsmodell ohne Vorabinvestitionen wählen. Das bereits im April in den USA eingeführte Modell ist jetzt auch in Großbritannien und in der EU verfügbar.

Das Schweizer Unternehmen bietet Backup-Speicherkapazitäten von 17 Terabyte bis 7 Petabyte mit monatlicher Abrechnung und einjährigem Abonnement an. Updates, Hardware-Aktualisierungen und Support sind im Preis enthalten. „Unternehmen wollen bei ihren Mitarbeitern mehr Kapazitäten für anspruchsvolle Aufgaben schaffen und eine integrierte, gut verwaltete Infrastruktur mit optimierter Auslastung aufbauen", erklärt Luis Fernandes, Senior Research Manager bei IDC.

Object First verzeichnete im zweiten Quartal 2025 in der EMEA-Region 961 Prozent mehr Buchungen als im Vorjahr. Das Unternehmen erweitert zudem sein Partnerprogramm um das Verbrauchsmodell und bietet ein Not-for-Resale-Programm für Partner an. Die unveränderliche Speicherlösung richtet sich speziell an Veeam-Nutzer und soll vor Ransomware schützen. ■

RMM-PLATTFORM UM ENDPOINT-RESILIENCE ERWEITERT

Absolute Security hat die Lösung Absolute Resilience für Managed Service Provider (MSPs) in die Remote-Monitoring-und-Management-(RMM)-Plattform ConnectWise integriert. Die Anwendung ist im ConnectWise Marketplace verfügbar und soll MSPs erweiterte Kontrolle über Endgeräte von Kunden ermöglichen.

Die Integration erlaubt die Überwachung zentraler Geräteeigenschaften und die Wiederherstellung kritischer Sicherheitsanwendungen. Bei Vorfällen können PCs per Fernzugriff in einen regelkonformen Zustand zurückgesetzt werden. Weitere Funktionen sind die Sperrung kompromittierter Endpunkte, sichere Datenlöschung mit Audit-Nachweis, die Durchsetzung von Verschlüsselung sowie Geofencing-Regeln für mobile Systeme. MSPs erhalten damit zusätzliche Transparenz über Gerätestandorte und den Zustand installierter Sicherheitsanwendungen.

Nach Unternehmensangaben arbeitet Absolute Security mit mehr als 28 PC-Herstellern zusammen. Die Technologie ist bereits auf BIOS-Ebene in rund 600 Millionen Endgeräten verankert und wird durch Lizenzierung freigeschaltet. Weltweit setzen Tausende Organisationen die Software ein, insgesamt für etwa 16 Millionen PCs. ■

ROUTER-SERIE UM IPS-FUNKTIONEN ERWEITERT

QNAP Systems hat die Routermodelle QHora-301W, QHora-322 und QHora-321 ab Firmware-Version 2.6.0 mit Intrusion-Prevention-System-(IPS)-Funktionen ausgestattet. Die signaturbasierte Erkennung und Blockierung von Bedrohungen erfolgt in Echtzeit, die Nutzung ist derzeit ohne zusätzliche Lizenzgebühren möglich.

Die IPS-Funktion greift auf automatisch aktualisierte Bedrohungsdatenbanken zu und wird über den QuWAN-SD-WAN-Dienst aktiviert. Neben IPS bieten die Router weitere Sicherheitsfunktionen, darunter L3/L7-Firewall mit Deep Packet Inspection, GeoIP-Blockierung und Webfilter. Über die SD-WAN-Lösung lassen sich zudem routenbasierte IPsec-VPN-Verbindungen mit Drittanbietergeräten herstellen. ■

ENDPOINT-SCHUTZ IN XDR-/MDR-PLATTFORM INTEGRIERT

Sophos hat den hauseigenen Endpoint-Schutz in die Extended-Detection-and-Response-(XDR)- und Managed-Detection-and-Response-(MDR)-Plattformen Taegis integriert. Die Integration folgt auf die Übernahme von Secureworks im Februar 2025 und soll den Betrieb vereinfachen.

Sophos Endpoint ist künftig in allen Taegis-Abonnements enthalten, ohne dass separate Lizenzen erforderlich sind. Funktionen wie Ransomware-Schutz (CryptoGuard) und Adaptive Attack Protection lassen sich direkt in der Konsole nutzen. Nach Unternehmensangaben bleibt Taegis eine offene Plattform: Kunden können weiterhin alternative Endpoint-Lösungen einsetzen oder zusätzliche Anbieter wie CrowdStrike und Microsoft Defender einbinden. Auch eine reine „Detection-only"-Sensor-Option steht zur Verfügung. ■

NEUE SCHLÜSSELÜBERPRÜFUNG FÜR E-MAILS

Der verschlüsselte E-Mail- und Kalenderdienst Tuta hat eine Funktion zur Schlüsselüberprüfung eingeführt. Ziel ist es, sogenannte Monster-in-the-Middle-(MITM)-Angriffe zu erschweren und die Ende-zu-Ende-Sicherheit zu erhöhen.

Nutzer können öffentliche Schlüssel ihrer Kontakte entweder über einen QR-Code mit der Tuta-App oder durch Abgleich eines Verifikationscodes in den Einstellungen prüfen. Nach erfolgreicher Überprüfung stellt der Dienst sicher, dass Nachrichten ausschließlich mit dem bestätigten Schlüssel verschlüsselt werden. Für alle übrigen Fälle greift das Trust-on-First-Use-(TOFU)-Verfahren; bei unerwarteten Schlüsseländerungen erfolgt eine Warnung. Tuta hatte bereits im März 2024 Post-Quanten-Verschlüsselung eingeführt. Das Unternehmen setzt dafür auf ein hybrides Verfahren mit quantenresistenten und klassischen Algorithmen. ■

SELF-SERVICE-TOOL ERHÄLT CLOUD-PASSWORT-RESET

Specops Software hat das Passwort-Tool uReset für Cloud-Infrastrukturen erweitert. Die Self-Service-Funktion ermöglicht es Anwendern, Passwörter eigenständig in Cloud-Umgebungen zurückzusetzen. Das Angebot richtet sich vor allem an Unternehmen, die Microsoft Entra ID einsetzen. Unterstützt werden mehr als 20 Identity-Provider, darunter Microsoft Authenticator, Okta, Duo Security und Yubikey. Sicherheitsfunktionen umfassen Geoblocking, Schutz vor MFA-Fatigue und den Abgleich mit einer Datenbank kompromittierter Passwörter.

Im Unterschied zu den integrierten Entra-ID-Optionen bietet uReset nach Herstellerangaben flexible MFA-Einbindung mit Drittanbietern sowie dynamisches Feedback an Endnutzer. Unterstützt werden lokales Active Directory, hybride Umgebungen und natives Entra ID. Passwörter lassen sich über Windows-Anmelde- und Sperrbildschirme oder aus dem Browser heraus zurücksetzen. Specops Software gehört seit 2022 zu Outpost24 und wurde 2001 gegründet. ■

Messevorschau

IT-SA 2025

Europas größte IT-Sicherheitsmesse wächst um über zwölf Prozent und führt KI-gestützte Live-Übersetzungen ein.

Anfang Oktober startet die it-sa Expo&Congress und baut ihre Position als Europas größte IT-Sicherheitsmesse weiter aus. Laut NürnbergMesse findet die Veranstaltung vom 7. bis 9. Oktober 2025 erstmals in fünf Messehallen statt. Die neu hinzugekommene Halle 8 sei bereits vollständig ausgebucht, teilt Exhibition Director Thimo Holst mit. Dadurch wächst die Ausstellungsfläche gegenüber dem Vorjahr um mehr als zwölf Prozent und bietet über 950 Ausstellern Platz.

„Die it-sa Expo&Congress ist für uns jedes Jahr ein zentraler Treffpunkt der IT-Sicherheitsbranche", erklärt Holst. Die Erweiterung verdeutliche die hohe Nachfrage und die zunehmende Bedeutung von IT-Sicherheitsthemen im internationalen Kontext.

ÜBER 400 SESSIONS MIT KI-GESTÜTZTER ÜBERSETZUNG

Das Forenprogramm der Messe umfasst laut Veranstalter über 400 Beiträge in sechs offenen Foren direkt in den Messehallen. Die Themenpalette reiche von technologischen Trends wie KI, Cloud-Sicherheit, Zero Trust und OT-Security über strategische Aspekte wie Cyberresilienz und digitale Souveränität bis hin zu Management-Themen wie Awareness, Datenschutz und Governance (www.itsa365.de/de-de/actions-events/events/foren-itsa-expo).

Eine wesentliche Neuerung stelle die KI-gestützte Live-Übersetzung dar: Laut Nürnberg-Messe werden erstmals sämtliche Beiträge live zwischen Deutsch und Englisch übersetzt, um das Programm für ein internationales Publikum zugänglich zu machen. Alle Sessions sind frei zugänglich und werden im Anschluss auf der Digitalplattform it-sa 365 bereitgestellt.

Das Programm deckt zudem verschiedene Branchenschwerpunkte ab, darunter kritische Infrastrukturen, Gesundheitswesen, Industrie und öffentlicher Sektor. Zusätzlich gibt es Community-Formate wie Women4Cyber und UP25@it-sa für junge Unternehmen.

CONGRESS STARTET BEREITS AM MONTAG

Parallel zur Messe läuft vom 6. bis 9. Oktober der Congress@it-sa im Congress Center NCC Ost. Das Programm startet also bereits am Montag vor der Messe und ermöglicht einen Rahmen für vertieften fachlichen Austausch mit Branchenverbänden, Industrieorganisationen und Anbietern von IT-Sicherheitslösungen (www.itsa365.de/de-de/actions-events/events/congress-it-sa).

Zu den konkreten Sessions gehört unter anderem die IT-Jahrestagung der IT-Sicherheitsbeauftragten in Ländern und Kommunen am 7. Oktober von 9:00 bis 13:00 Uhr im Saal Tokio. Laut Programm haben der Bund als IT-Planungsrat-Vorsitz, die Arbeitsgruppe Informationssicherheit des IT-Planungsrates unter Vorsitz von Rheinland-Pfalz, die Bundesakademie für öffentliche Verwaltung, der Deutsche Landkreistag, das BSI, die FITKO und das Landesamt für Sicherheit in der Informationstechnik Bayern die Themen zusammengetragen.

Weiterhin wird es einen Workshop zum Thema „Realität trifft Hoffnung: Einsatzpotenziale von KI in der Cyberabwehr" geben. Laut Bitkom werden am 7. Oktober von 9:30 bis 10:30 Uhr im Raum Riga praxiserprobte Ansätze entlang des NIST-Frameworks vorgestellt, etwa im Bereich Endpunktschutz, SIEM und SOC. Auch neue Entwicklungen wie generative und spezialisierte KI-Agents sollen eingeordnet werden.

◀ *Eingangsbereich der Messe 2024: Auch im vergangenen Jahr kamen Tausende Fachbesucher zur it-sa und sorgten für volle Vortragsräume und lebendigen Austausch. (Bild: NürnbergMesse/Frank Boxler)*

▼ *Auf der it-sa gibt es zahlreiche Einblicke in aktuelle Sicherheitsthemen – hier im vergangenen Jahr auf der Bühne: Claudia Plattner, Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik (BSI). (Bild: NürnbergMesse/Frank Boxler)*

KEYNOTE ZU GEOPOLITISCHEN TECHNOLOGIE-ASPEKTEN

Als besonderen Höhepunkt kündigt die NürnbergMesse die Special Keynote von Dr. Jean-Marc Rickli am 9. Oktober 2025 von 12:00 bis 13:00 Uhr an. Der Leiter der Abteilung „Global Risk and Resilience" am Geneva Centre for Security Policy (GCSP) spricht über „Sicherheit und geopolitische Auswirkungen neuer Technologien".

Rickli beschäftigt sich laut eigenen Angaben mit aufkommenden Risiken im Zusammenhang mit neuen Technologien, insbesondere künstliche Intelligenz (KI), Neurotechnologien und synthetische Biologie. Sein Fachgebiet ist Kriegsführung mit regionalen Schwerpunkten auf Europa und dem Nahen Osten. Vor seiner Tätigkeit am GCSP war er Professor am King's College London und an der Khalifa University in Abu Dhabi.

In seiner Keynote wird Rickli, wie er vorab in einem Interview erläuterte, seine These vorstellen, dass KI bereits heute bewaffnete Konflikte prägt und künftig zu grundlegenden geopolitischen Machtverschiebungen führen wird. KI werde bereits in großem Umfang zur Datenauswertung und Zielidentifikation eingesetzt, erklärt der Experte mit Blick auf die Konflikte in Gaza und in der Ukraine. Für die Zukunft prognostiziert er den Einsatz autonomer Malware, die „selbstständig Ziele identifiziert, nach Sicherheitslücken sucht und geeignete Maßnahmen entwickelt und ausführt, um den Gegner anzugreifen." Besonders problematisch sei die Entwicklung zur kognitiven Kriegsführung durch maßgeschneiderte Desinformation. Geopolitisch warnt Rickli vor Europas Abhängigkeit von US-amerikanischer und chinesischer KI-Technologie: „Europa spielt nicht in derselben Liga."

DIGITALE VORBEREITUNG UND HYBRIDE TEILNAHME

Die ganzjährige Digitalplattform it-sa 365 begleitet IT-Sicherheitsverantwortliche mit Fachinformationen und Networking-Möglichkeiten. Die Plattform unterstützt die individuelle Messeplanung mit Funktionen wie Ausstellerübersicht, detaillierter Produktsuche, Chat-Optionen und Terminvereinbarung. Mithilfe eines digitalen Hallenplans können Routen zu Ausstellern, Programmpunkten und Serviceeinrichtungen bereits im Vorfeld festzulegt werden.

Für Remote-Teilnehmer bietet der hybride Expo-Channel „it-sa@home" die Möglichkeit, wichtige Vorträge zu verfolgen. Laut Veranstalter werden ausgewählte „it-sa insights"-Vorträge gestreamt, Referenten kommen zu digitalen Q&A-Sessions ins Studio in Messehalle 7. Zudem finden Live-Interviews mit Ausstellern statt. Das hybride Format bringe „die Welt der IT-Security direkt auf die Bildschirme der Community", so die Programmankündigung. Die Nutzung von it-sa 365 ist kostenfrei, erfordert jedoch eine Registrierung (www.itsa365.de).

Statt Zero Trust lieber volle Gläser: Auf der it-sa 2024 kam beim Networking auch mal Cybeer auf den Tisch – die wohl entspannteste Sicherheitslösung der Messe. (NürnbergMesse/Frank Boxler)

TICKETPREISE

Die Ticketpreise für die it-sa betragen laut Veranstalter 67 Euro für ein Tagesticket und 112 Euro für ein Dauerticket. Parkplätze kosten 14 Euro. Neu ist ein zusätzliches Kombi-Ticket für den öffentlichen Nahverkehr, das für die Tarifgebiete Nürnberg-Fürth-Stein-Oberasbach-Zirndorf am Veranstaltungstag bis Betriebsschluss gültig ist. Die personalisierten E-Tickets sind nicht übertragbar und können online mit Kreditkarte oder PayPal bezahlt werden. Gutscheine müssen ausschließlich online im Gutschein-Shop eingelöst werden. ■

Congress@it-sa: 2024 bot das Fachprogramm mit 55 Beiträgen eine wichtige Plattform für Branchendialog und spezialisierte IT-Sicherheitsthemen. (Bild: NürnbergMesse/Thomas Geiger)

Digitale Souveränität und
die neue Rolle des Chief Resilience Officers

RESILIENZ STATT ABWEHR

Hypothetische Krisenszenarien sind für Unternehmen zur Realität geworden: Mitarbeiter dürfen nicht mehr in die USA einreisen, Anbieter blockieren plötzlich E-Mails, und internationale Verträge gelten über Nacht nicht mehr. Klassische IT-Sicherheit greift in dieser instabilen geopolitischen Ordnung zu kurz. Es geht nicht mehr nur um Abwehr, sondern um Handlungsfähigkeit unter erschwerten Bedingungen – es geht um Resilienz.

Resilienz beschreibt die Fähigkeit eines Unternehmens, auch unter Druck stabil und handlungsfähig zu bleiben und sich gezielt weiterzuentwickeln, unabhängig davon, ob es auf Cyberangriffe, Lieferkettenausfälle oder geopolitische Schocks reagieren muss. Es geht nicht darum, Störungen zu verhindern, sondern vielmehr darum, robust, agil und anpassungsfähig zu sein, wenn sie eintreten.

Wie entscheidend diese Fähigkeit ist, zeigt ein Blick in den von F24 gesponserten „Resilience: Vision 2030"-Report des Business Continuity Institute (BCI): 86,7 Prozent der über 200 befragten Fachleute aus mehr als 50 Ländern sehen in der Vermeidung von Betriebsunterbrechungen den größten betriebswirtschaftlichen Nutzen von Resilienzmaßnahmen. In der Praxis konzentrieren sich viele Unternehmen weiterhin auf die technische Verteidigung gegen Cyberbedrohungen durch Firewalls, Verschlüsselung und Patch-Management. All das ist nach wie vor wichtig, jedoch benötigen Firmen heute einen ganzheitlichen Ansatz, der über den Schutz einzelner Systeme hinausgeht. Dieser setzt sich aus unterschiedlichen Bausteinen zusammen.

CHIEF RESILIENCE OFFICER ALS NEUE FÜHRUNGSPOSITION

Ein wirksamer Resilienzansatz basiert auf drei zentralen Prinzipien: Zunächst braucht es eine umfassende Kritikalitätsanalyse, die sowohl technische als auch organisatorische Schwachstellen etwa bei Systemabhängigkeiten, Liefer-

Bild: Gorodenkoff - stock.adobe.com

ketten oder fehlenden Qualifikationen im Team sichtbar macht. Darauf folgt die Stabilisierung: Wo immer möglich, gilt es Risiken durch den Einsatz sicherer Technologien, souveräner Partner und redundanter Kommunikationswege zu minimieren. Schließlich ist strategische Steuerung entscheidend. Resilienz entsteht nicht nebenbei. Sie erfordert Verantwortung auf C-Level, klare Zuständigkeiten und eine kontinuierliche Weiterentwicklung anhand messbarer Kennzahlen (Key Performance Indicator, KPIs).

Wie eine Verankerung auf C-Level-Ebene aussehen kann, dazu haben viele bereits konkrete Ideen: Im „Resilience: Vision 2030"-Report sprechen sich 73 Prozent der Fachleute für die Einführung eines Chief Resilience Officers (CRO) aus. Benötigt werden nicht klassische Krisenmanager, sondern strategische Querschnittsverantwortliche mit Überblick über IT, Compliance, Lieferketten und Kommunikation. Ein CRO soll den notwendigen organisatorischen Rahmen schaffen: Die Person koordiniert unternehmensweite Resilienzstrategien, definiert klare Verantwortlichkeiten und fördert funktionsübergreifende Zusammenarbeit, die laut Report der zentrale Erfolgsfaktor für Resilienzprogramme ist (64,6 Prozent).

ADAPTIVE TECHNOLOGIEN ERSETZEN STATISCHE NOTFALLPLÄNE

Jedoch entsteht Resilienz nicht allein durch stabile Strukturen, sie benötigt auch Werkzeuge, die im Ernstfall Orientierung, Geschwindigkeit und Überblick ermöglichen. KI-gestützte Risikoanalysen, Echtzeit-Dashboards oder simulationsbasierte Szenarienplanung erlauben mittlerweile eine vorausschauende und dynamische Steuerung von Risiken. Damit leisten sie genau das, was eine moderne Resilienzfähigkeit erst möglich macht: schnell reagieren, gezielt entscheiden und dauerhaft lernen.

Statt statischer Notfallpläne kommen adaptive Systeme zum Einsatz, die sich kontinuierlich an neue Bedrohungslagen anpassen. Besonders in kritischen Bereichen wie Kommunikation, Governance oder Supply Chain Management liefern digitale Tools transparente Entscheidungsgrundlagen und Frühwarnmechanismen und damit genau den Zeitvorsprung, der im Ernstfall erforderlich ist. Wer Resilienz ernst nimmt, muss nicht nur in Strukturen, sondern auch in die richtigen Technologien investieren.

EUROPÄISCHE IT-PARTNER ALS SOUVERÄNITÄTS-FAKTOR

Wer auf Tools blickt, beschäftigt sich automatisch mit einem weiteren Baustein zeitgemäßer Resilienzstrategien: Ein bisher häufig vernachlässigter Hebel zur Steigerung organisationaler Resilienz liegt im Einkauf, genauer gesagt in der Wahl der IT-Dienstleister. Unternehmen, die auf europäische Anbieter setzen, stärken nicht nur ihre IT-Sicherheit, sondern auch ihre digitale Souveränität. Datenhoheit und rechtssichere Systemkontrolle sind keine Formalitäten, vielmehr handelt es sich gerade in Krisenzeiten um Überlebensbedingungen für Betriebe. Zu den Vorteilen europäischer IT-Partner zählen unter anderem:

- **Rechtssicherheit und Datenschutz:** Europäische Anbieter unterliegen nicht extraterritorialen Gesetzen wie dem US-CLOUD-Act. Dadurch bleiben Unternehmens- und Personaldaten auch im Fall geopolitischer Spannungen innerhalb des Schutzrahmens der Datenschutzgrundverordnung (DSGVO).
- **Stabile Regulierungsumgebung:** Rechtssicherheit bedeutet planbare Sicherheit. Europäische Anbieter agieren in einem demokratisch legitimierten Umfeld mit transparenten, langfristig angelegten Gesetzgebungsprozessen. Plötzliche Serviceeinschränkungen oder regulatorische Kehrtwenden sind weitgehend ausgeschlossen.
- **Lieferkettenstabilität:** Geografische, kulturelle und organisatorische Nähe kann die Zusammenarbeit stärken. Europäische Anbieter sprechen oft dieselbe Sprache, kennen die hiesigen regulatorischen Anforderungen und arbeiten mit lokalen Teams, was Prozesse stabilisieren kann.
- **Vermeidung geopolitischer Abhängigkeiten:** Unternehmen, die sich zu stark auf Anbieter aus geopolitisch instabilen Regionen verlassen, riskieren hohe Folgekosten – von rechtlicher Unsicherheit bis zu Betriebsunterbrechungen.
- **Transparenz und Innovationskraft:** Europäische Rahmenwerke wie die Verordnung über künstliche Intelligenz (AI Act) oder die überarbeitete Richtlinie über Netz- und Informationssicherheit (NIS-2) schaffen klare Standards für neue Technologien. So entstehen robuste, interoperable und zukunftsfähige Lösungen – und damit eine Grundlage für echte digitale Widerstandsfähigkeit.

Das bedeutet: Wer bewusst europäisch einkauft, priorisiert Souveränität als zentralen Baustein seiner Resilienzstrategie.

IT-SICHERHEIT WIRD ZUR VERTRAUENSFRAGE

Dass IT-Sicherheit nicht nur ein technisches, sondern auch ein politisches Thema ist, zeigen Entwicklungen wie die gezielte Instrumentalisierung digitaler Infrastrukturen durch Staaten. Das bedeutet, dass Vertrauen zum zentralen Steuerungsfaktor wird: Wer seine Kommunikation nicht souverän führen oder seine kritischen Systeme nicht rechtssicher betreiben kann, verliert im Ernstfall nicht nur Zugriff, sondern auch Handlungsfähigkeit. Damit genau das nicht passiert, braucht es eine umfassende IT-Sicherheit als starke Basis. Sie wird zur strategischen Investition in die Resilienz. Unternehmen, die diese Perspektive einnehmen, profitieren doppelt: Sie schützen nicht nur ihre Daten, sondern sichern sich Handlungsfähigkeit und damit den entscheidenden Vorsprung in einer Welt, in der Unsicherheit die neue Normalität ist. ■

ESKE OFNER
ist Head of Sales bei F24 AG.
(Bild: © F24 AG)

KI-Sicherheit durch universelle Plattformen

GEBÜNDELTE SCHUTZ-FUNKTIONEN GEGEN WACHSENDE KOMPLEXITÄT

Künstliche Intelligenz (KI) erhöht die Produktivität, führt jedoch gleichzeitig zu höheren Kosten, gesteigerter Komplexität und erweiterten Cyberrisiken – besonders in hybriden Multi-Cloud-Architekturen. Können einheitliche Plattformen für die Bereitstellung und Absicherung von Anwendungen dabei helfen, die Potenziale durch KI sicher zu erschließen?

In der Unternehmenswelt hat sich KI längst etabliert: Laut dem „State of Application Strategy Report 2025" von F5 setzen bereits 96 Prozent der Unternehmen KI-Modelle ein. Die Entwicklung beschleunigt sich weiter – innerhalb von drei Jahren sollen acht von zehn Anwendungen KI-Funktionen enthalten.

Diese Verbreitung bringt jedoch erhebliche Sicherheitsprobleme mit sich. Die KI-Anwendungen erzeugen enorme Datenmengen und vielschichtige Verkehrsmuster, die neue Angriffsvektoren schaffen. Gleichzeitig wird die unterstützende Infrastruktur zunehmend verteilter und komplexer, was die potenzielle Angriffsfläche vergrößert und die Fehleranfälligkeit bei der Bereitstellung erhöht.

Herkömmliche Sicherheitsansätze stoßen hier an ihre Grenzen, da nicht integrierte Einzellösungen isolierte Bereiche innerhalb der IT-Landschaft erzeugen. Dies erschwert ein einheitliches Sicherheitsmanagement erheblich.

PLATTFORMEN ALS LÖSUNGSANSATZ

Angesichts dieser Herausforderungen setzen einige Anbieter daher auf einheitliche Lösungen, die verschiedene Funktionen wie Lastausgleich,

Bild: KamStudio | qunoo - stock.adobe.com

API-Schutz und umfassende Analyse in einer Lösung vereinen sollen. Solche Systeme zielen darauf ab, KI-basierte Anwendungen bis zu ganzen KI-Fabriken zu unterstützen und dabei nahtlose Bereitstellung, zuverlässige Sicherheit sowie konsistente Leistung über diverse Umgebungen hinweg zu gewährleisten.

Bereits heute bietet der Markt mehrere Tools, die Anwendungen und APIs überall bereitstellen, sichern und optimieren sollen – von lokalen Rechenzentren über öffentliche Clouds bis zum Netzwerkrand (Edge Computing). Sie sind darauf ausgelegt, zentrale Transparenz, Automatisierung und Richtliniendurchsetzung mit leistungsstarkem Lastausgleich und Datenverkehrsmanagement sowie erweiterten App- und API-Sicherheitsfunktionen zu vereinen.

Von diesen Ansätzen versprechen sich Befürworter eine Entlastung der IT- und Sicherheitsteams durch mehr Einfachheit, Konsistenz und Übersichtlichkeit im Management hybrider Multi-Cloud-Architekturen.

GRUNDLEGENDE SICHERHEITSFUNKTIONEN

Für eine echte Vereinfachung des Sicherheitsmanagements müssen die Plattformen jedoch entsprechende Cybersecurity-Funktionen zur Abwehr von erweiterten Angriffen, Datendiebstahl, Datenschutzverstößen und anderen schädlichen Aktivitäten bieten.

Dabei sollten sie sich an den OWASP-Top-Ten-Schwachstellen orientieren und vor Zero-Day-Angriffen schützen.

Eine Echtzeit-Überprüfung des Datenverkehrs und die automatisierte Verwaltung von Richtlinien gehören ebenfalls zu den grundlegenden Anforderungen.

Besonders wichtig ist das Scannen von Web-Apps zur Identifizierung von Schwachstellen in großen Sprachmodellen (Large Language Models, LLMs). Mit dieser Funktionalität können Organisationen LLMs durchsuchen und Penetrationstests durchführen, um spezifische Sicherheitslücken aufzudecken, die den OWASP Top Ten für LLM-Anwendungen entsprechen.

Erheblich erschwert wird die Schwachstellensuche durch die starke API-Zunahme. Nicht geschützte oder überwachte APIs können jedoch zu Bedrohungen führen. Dazu gehören unbefugter Zugriff, Datenexfiltration, Injektionsangriffe und Denial-of-Service-(DoS)-Attacken. Daher benötigen einheitliche Plattformen leistungsfähige Tools für die Erkennung und den Schutz von APIs.

Parallel dazu nehmen clientseitige, browserbasierte Angriffe derzeit an Zahl und Intensität zu. Entsprechend müssen Unternehmen endpunktbasierte Schutzmechanismen nutzen, um die mit Datenexfiltration und bösartigen JavaScript-Angriffen verbundenen Risiken zu senken. Einheitliche Plattformen für die Softwaresicherheit sollten daher Einblick in bösartige Skripte und die von ihnen durchgeführten Aktionen ermöglichen.

SPEZIELLE KI-SICHERHEITS-HERAUSFORDERUNGEN

Neben allgemeinen Risiken müssen Firmen auch die Eigenheiten von KI-Workloads berücksichtigen. Mit der Einführung von KI- und Hybrid-Cloud-Technologien bewegen sich sensible Daten oft über verschlüsselten Datenverkehr und nicht zugelassene KI-Tools, was zu Sicherheitslücken führen kann.

Herkömmliche Schutzmaßnahmen erkennen oder verhindern jedoch meist keine Datenlecks in diesen komplexen Umgebungen. Gefordert sind daher Lösungen, die:

- Datenlecks im verschlüsselten und KI-gesteuerten Datenverkehr in Echtzeit erkennen, klassifizieren und stoppen;
- Risiken durch unautorisierte KI-Nutzung und Offenlegung sensibler Daten verhindern und
- einheitliche Richtlinien über Anwendungen, APIs und KI-Dienste hinweg durchsetzen können.

Mit diesen Funktionen lassen sich KI-Anwendungen sicher optimieren, skalieren und orchestrieren. Das ist notwendig, um die Komplexität hybrider Multi-Cloud-Infrastrukturen mit ihren sich ständig weiterentwickelnden Anforderungen an Sicherheit und Leistung zu bewältigen.

ERWARTETE VORTEILE

Die Befürworter nennen für integrierte Plattformen mehrere Vorteile: Das konsolidierte Management für hybride Umgebungen soll die Komplexität deutlich reduzieren, da Unternehmen nicht mehr mit mehreren Einzellösungen umgehen müssen. Sofern die Integration gelingt, steigert diese Vereinfachung nicht nur die betriebliche Effizienz, sondern befreit auch Sicherheitsteams für strategischere Aufgaben.

Ein weiterer Vorteil: Verbesserte Sicherheitsvorkehrungen für KI-gestützte Anwendungen sollen zudem einen proaktiven Schutz vor neuen Bedrohungen ermöglichen. Das ist wichtig, da herkömmliche Sicherheitsmaßnahmen neuartige Angriffsvektoren für KI-Anwendungen häufig nicht erkennen.

Darüber hinaus können die oft umfangreichen Analysemöglichkeiten der Plattformen wertvolle Einblicke in die Leistung und Sicherheit von Applikationen bieten. Mithilfe umsetzbarer Informationen können Unternehmen die Zuweisung von Ressourcen optimieren und die Reaktionsfähigkeit von Anwendungen für eine reibungslose Nutzererfahrung verbessern.

Letztlich sollten vollständig programmierbare Datenebenen die automatisierte Anpassung von Funktionen zur Anwendungsbereitstellung erlauben. Wenn sich Geschäftsanforderungen ändern, könnten Organisationen so dank automatisierter Anpassungen ohne umfangreiche manuelle Eingriffe reagieren. Dadurch könnten sich Innovationszyklen und Markteinführungszeiten verkürzen.

FAZIT

Die Integration von KI in Unternehmensanwendungen bringt neue Sicherheitsherausforderungen mit sich, die herkömmliche Ansätze oft nicht bewältigen können. Einheitliche Plattformen versprechen eine Lösung durch die Bündelung verschiedener Schutzfunktionen. Ob diese Konzepte die komplexen Anforderungen hybrider Multi-Cloud-Umgebungen vollständig erfüllen können, hängt von der konkreten Umsetzung und den spezifischen Unternehmensanforderungen ab. ■

STEPHAN SCHULZ
ist Senior Principal Solutions Engineer bei F5.

Kontrollierte Intelligenz

Sicherer Einsatz generativer KI-Anwendungen in Unternehmen

Cloudbasierte generative KI-Anwendungen wie ChatGPT oder Gemini haben das Potenzial, Arbeitsweisen in Organisationen grundlegend zu verändern – sie können damit effizienter, intelligenter und kreativer agieren. Dieses Potenzial birgt jedoch auch Risiken: Datenschutz, Modellkontrolle und die Integrität sensibler Informationen stehen auf dem Spiel. Doch es ist möglich, leistungsstarke KI-Systeme lokal und sicher zu betreiben: mit einem Zero-Trust-Netzwerk mit aktiver Traffic-Überwachung und mehrschichtiger Perimeterabsicherung.

Mit dem Aufstieg generativer KI-Modelle wie GPT-4, Claude oder Gemini erleben Unternehmen eine neue Welle digitaler Möglichkeiten – von automatisierter Textgenerierung über Code-Vervollständigung, Datenanalyse, Prozessautomatisierung bis hin zu intelligentem Wissensmanagement. Gleichzeitig stellt sich eine zentrale Frage: Wie lassen sich diese Tools sicher, datenschutzkonform und kontrollierbar in sensible Unternehmensumgebungen integrieren?

Besonders in regulierten Branchen – etwa dem öffentlichen Sektor, der Energieversorgung oder der Gesundheitsbranche – sind klassische cloudbasierte Modelle oft nicht zulässig. Der Grund: Prompts und Nutzungsdaten werden über das Internet an externe, meist in Drittländern gehostete Server übertragen. Dies widerspricht nicht nur internen Compliance-Vorgaben, sondern auch gesetzlichen Regelungen wie der Datenschutz-Grundverordnung (DS-GVO) oder branchenspezifischen Sicherheitsstandards.

Herausforderungen beim sicheren Einsatz generativer KI in Unternehmen

Auch außerhalb dieser Hochsicherheitsumfelder wächst das Bewusstsein dafür, dass Kontrolle über Datenströme, Modellverhalten und Zugriffspflichten essenziell ist. Kundendaten und Betriebsgeheimnisse dürfen nicht unkontrolliert nach außen gelangen. Auch sollte nicht jeder Mitarbeitende Zugriff auf alle Informationen im Unternehmen haben. Daher steigt die Nachfrage nach Lösungen, die moderne KI-Funktionalität mit lokaler Kontrolle und technischer Absicherung kombinieren.

Ein Ansatz dafür ist eine Architektur auf Basis eines Zero-Trust-Frameworks. Dieses kann generative KI-Modelle, die On-Premises im eigenen Rechenzentrum betrieben werden, zuverlässig absichern und zugleich die kontrollierte Nutzung relevanter Schnittstellen (APIs) ermöglichen.

Lokale Sprachmodelle mit vLLM: OpenAI-kompatible KI-Infrastruktur

Für die lokale Bereitstellung generativer KI-Anwendungen ist die Kombination aus einem leistungsstarken lokalen Sprachmodell und einer effizienten Inferenz-Infrastruktur entscheidend. Eine besonders effektive Lösung ist die Integration von Llama 3.3 – einem modernen Open-Source-Sprachmodell von Meta – mit dem Inferenz-Framework vLLM (Virtual Large Language Model).

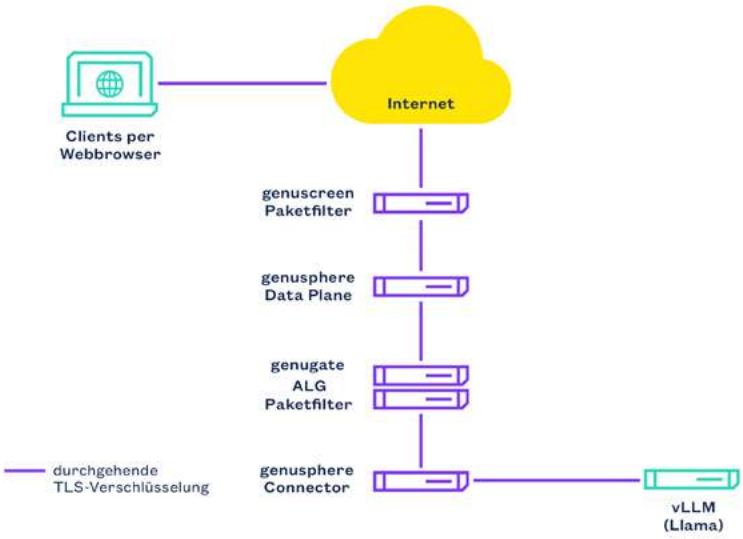
vLLM ist darauf ausgelegt, große Sprachmodelle besonders effizient bereitzustellen. Es bietet eine API, die vollständig kompatibel zur OpenAI-

Bild: Papisut – stock.adobe.com

Schnittstelle ist. Vorhandene Tools, Plugins und interne Softwarelösungen lassen sich so ohne umfangreiche Anpassungen auch lokal nutzen. Dieser Ansatz reduziert sowohl Komplexität als auch Implementierungsaufwand und ermöglicht es, bestehende Prozesse schnell und mit geringem Integrationsaufwand KI-fähig zu machen.

Architekturüberblick: Sicherer KI-Betrieb im Unternehmensnetz

Die Auswahl des richtigen Modells ist nur der erste Schritt. Mindestens ebenso wichtig ist der Aufbau einer ganzheitlich geschützten Infrastruktur. Erst die Kombination aus lokalem LLM-Betrieb und einem mehrschichtigen Zero-Trust-Ansatz bildet die Grundlage für eine kontrollierte, datenschutzkonforme und unternehmenseigene KI-Strategie.



Aufbau einer ganzheitlich geschützten Infrastruktur zum sicheren Einsatz generativer KI

Die Integration von Llama 3.3 über vLLM in ein streng kontrolliertes Netzwerkszenario umfasst mehrere Sicherheitsschichten – vom äußeren Perimeter bis hin zur aktiven Überwachung des internen Datenverkehrs.

Zwiebelmodell: Viele Schichten bringen Hacker zum Heulen

Als erste Schutzschicht dient genuscreen, die Firewall und VPN-Appliance von genua, einem Unternehmen der Bundesdruckerei-Gruppe. Sie schützt das Unternehmensnetz zuverlässig vor Angriffen aus dem Internet und ermöglicht eine feingranulare Steuerung des Netzwerkverkehrs. Selbst verschlüsselte Verbindungen lassen sich damit analysieren und kontrollieren. Auf diese Weise wird schon an der Netzwerkgrenze sichergestellt, dass ausschließlich definierter Traffic ins interne Netz gelangt – und ebenso kontrolliert wieder hinaus.

Im Inneren der Architektur agiert die robuste Application Layer Firewall genugate. Durch Zonen- und Mediendatentrennung wird der Zugriff auf kritische Infrastruktur – etwa den Server, auf dem vLLM und das Sprachmodell laufen – streng reguliert. Nur exakt definierte Kommunikation ist erlaubt. Optional lassen sich Inhalte über manuell geprüfte Freigaben weitergeben, etwa bei Dateiübertragungen. So bleibt die Kontrolle über die Datenströme jederzeit in der Hand der Organisation.

Zero Trust Application Access für interne KI-Dienste

So gerüstet erfüllt der interne Betrieb generativer KI bereits viele Sicherheitsanforderungen. In der Praxis besteht jedoch häufig der Bedarf für einen kontrollierten Zugriff auf KI-Anwendungen von außen – etwa durch mobile Mitarbeitende, externe Partner oder verteilte Organisationseinheiten. Genau hier setzt genusphere an: Die Zero Trust Application Access (ZTAA) Lösung macht interne Anwendungen sicher verfügbar, ohne Netzwerkzugriffe zu gewähren.

Im Unterschied zu klassischen VPNs oder Reverse-Proxys ermöglicht genusphere eine segmentierte Bereitstellung von Applikationen – vollständig entkoppelt vom internen Netzwerk. Zugriffsrechte werden kontextabhängig, rollenbasiert und gerätespezifisch vergeben. Das bedeutet: Nur wer unter den definierten Bedingungen berechtigt ist, kann auf bestimmte Funktionen einer Anwendung zugreifen. Daraus ergeben sich klare Vorteile:

- KI-Anwendungen wie vLLM lassen sich selektiv nach außen bereitstellen – etwa als API, Web-Oberfläche oder internes Wissensportal.
- Zugriffe erfolgen authentifiziert und kontextsensitiv, etwa mit Device Trust, Identity Federation und granularen Policies.
- Die Anwendung bleibt intern isoliert – genusphere vermittelt lediglich die Anwendungsebene, nicht die darunterliegende Infrastruktur.

Damit bietet genusphere eine skalierbare, sichere und DS-GVO-konforme Möglichkeit, generative KI auch über Standortgrenzen hinweg nutzbar zu machen – ohne Kompromisse bei Netzwerk- oder Datensicherheit eingehen zu müssen.

Diese Beschreibung zeigt: Leistungsstarke KI-Tools lassen sich souverän nutzen, wenn sie in eine durchdachte Sicherheitsarchitektur eingebettet sind. Organisationen können so von den Vorteilen generativer KI-Anwendungen profitieren – und gleichzeitig die Kontrolle über ihre eigene digitale Zukunft behalten. ■

Sie wollen mehr über Chancen und Risiken moderner KI erfahren? Im neuen Open-Access-Fachbuch **„Künstliche Intelligenz und Wir“** haben Experten von genua, der Bundesdruckerei und viele weitere namhafte Autorinnen und Autoren aus Wissenschaft und Wirtschaft ihre Fachkompetenz zu einem umfassenden Überblick über den aktuellen Stand und die Zukunft von KI gebündelt. genua sponsert den kostenlosen Zugang zum E-Book.

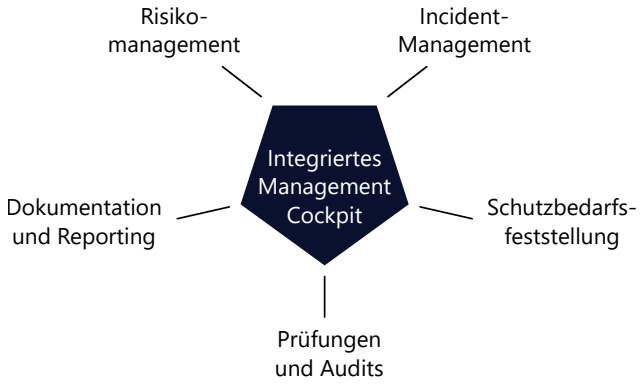
Mehr dazu hier

genua.

ibi systems iris – GRC und Information Security smarter, schneller, sicherer

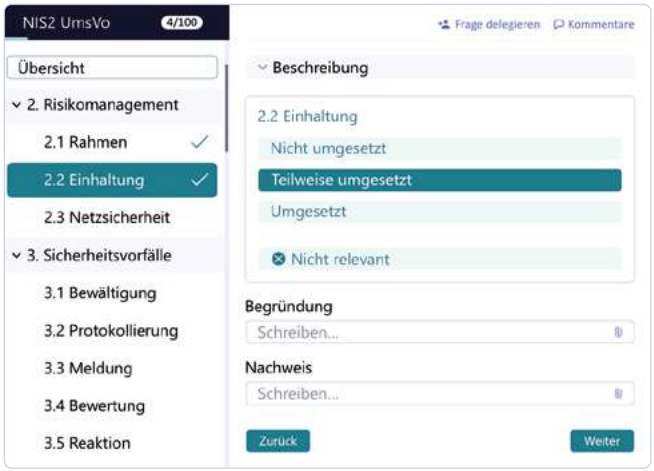
Regulatorische Vorgaben wie **NIS-2, DORA** oder die Anforderungen nach **KRITIS** stellen Unternehmen heute vor immer größere Herausforderungen. Die Komplexität steigt durch ausgelagerte IT-Services, Cloud-Infrastrukturen, heterogene Systemlandschaften und die wachsende Zahl digitaler Geschäftsprozesse. Unternehmen müssen nicht nur IT-Sicherheitsmaßnahmen implementieren, sondern auch organisatorische und prozessuale Anforderungen nachweisen und kontinuierlich überwachen. Die ISMS- und GRC-Software iris der ibi systems GmbH unterstützt Unternehmen gezielt dabei, diese Anforderungen effizient, nachvollziehbar und auditfähig umzusetzen.

Die Kernelemente der regulatorischen Vorgaben und die **Unterstützung durch iris** lassen sich wie folgt zusammenfassen:



- **Risikomanagement:** zentralisierte Erfassung und Bearbeitung von Risiken, inklusive Bewertungen und Maßnahmenplanung
- **Incident-Management:** strukturierte Bearbeitung, Klassifizierung und Nachverfolgung von Sicherheitsvorfällen
- **Schutzbedarfsfeststellung:** teilautomatisierte Ermittlung des Schutzbedarfs auf Basis der Modellierung des Informationsverbunds
- **Prüfungen und Audits:** Durchführung von Application-Security-Checks, Lieferanten-Audits und individuellen Prüfungen
- **Dokumentation und Reporting:** intelligente Dashboards mit Mappings zu Standards wie ISO 27001 oder BSI IT-Grundschutz sowie konsolidierte Auswertung der unternehmensweiten Zielerreichung

Ein zentrales Highlight von iris ist die Bereitstellung **zielgruppengerecht aufbereiteter Apps** mit Fokus auf Usability, Kollaboration und intelligenter Automatisierung. Damit lassen sich Prüfungen strukturiert planen, verschicken und durchführen. Alle Ergebnisse werden systematisch dokumentiert, Feststellungen und Maßnahmen können direkt abgeleitet und für Follow-Up-Prozesse verwendet werden.



Ein weiterer USP von iris ist die teilautomatisierte Bereitstellung **individueller Checklisten:** Je nach Kontext der Prüfobjekte werden Prüfungslisten dynamisch aufbereitet. Jede Prüfung ist so vollständig und auf die relevanten regulatorischen Anforderungen abgestimmt. Der manuelle Aufwand wird dadurch reduziert, und Unternehmen können die komplexen Anforderungen von NIS-2, DORA oder KRITIS zuverlässig erfüllen.

Darüber hinaus bietet iris die Möglichkeit, eigene **Anforderungen** mit Anforderungen aus relevanten Standards, beispielsweise ISO 27001, BSI IT-Grundschutz oder branchenspezifischen Vorgaben zu **kombinieren** und den Compliance-Grad konsolidiert zu ermitteln. Über das integrierte Management-Cockpit erhalten Unternehmen jederzeit einen Überblick in Echtzeit über ihre Zielerreichung und die Risikolage. Lücken, Optimierungspotenziale oder potenzielle Sicherheitsrisiken werden sichtbar, und Entscheidungen können datenbasiert sowie nachvollziehbar getroffen werden.

Die **ibi systems GmbH** unterstützt seit 2012 Kunden sämtlicher Branchen – von kleinen und mittleren Unternehmen (KMU) bis zu internationalen Großkonzernen – als innovativer Softwarehersteller in den Bereichen InsurTech, RegTech und Information Security. Entwicklung und Standort befinden sich ausschließlich in Deutschland, wodurch höchste Sicherheits- und Qualitätsstandards gewährleistet werden. Aktuell betreut das Unternehmen rund 60 Kunden in der DACH-Region mit über 3.000 aktiven Nutzern. ■

ibi systems GmbH
contact@ibi-systems.de
+49 941 462939-0
www.ibi-systems.de

Mehr dazu hier

iris @ it-sa 2025
Besuchen Sie uns gern auf der **it-sa in Halle 9/Stand 9-401,** wenn Sie mehr über die ISMS- und GRC-Software iris erfahren möchten.

bitkom
akademie

Ausgezeichnet weiterbilden – dreifach prämiert für Ihre Zukunft.

Wir qualifizieren die Digitalwirtschaft – seit 20 Jahren.

Seit 20 Jahren steht die Bitkom Akademie an der Spitze der digitalen Weiterbildung in Deutschland. **Mit über 400 Weiterbildungen pro Jahr** – von Live-Online-Seminaren über Zertifikatslehrgänge bis hin zu individuellen Schulungsangeboten – unterstützt die Akademie Unternehmen nachhaltig bei Ihren Digitalisierungsprojekten.

Seminarprogramm für das 2. Halbjahr 2025
Mit über 230 Terminen und mehr als 50 neuen Formaten greift die Bitkom Akademie aktuelle Herausforderungen auf – von regulatorischen Vorgaben bis hin zu strategischen Fragestellungen im digitalen Wandel.

Finden Sie jetzt Ihre Weiterbildung!

Michel Achenbach
Leiter Bitkom Akademie

Schwerpunkte des Seminarprogramms:

Künstliche Intelligenz

Seminare und Kompetenzschulungen zur Umsetzung des **AI Act** und Anwendung zukunftsweisender KI-Technologien.

IT-Sicherheit

Praxisorientierte Workshops und Zertifikatslehrgänge mit Fokus auf die Anforderungen des **KRITIS**-Dachgesetzes & **NIS2.**

Aktualisierte Premium-Lehrgänge

Neue Inhalte für Rollen wie KI-Manager, Data Scientist und CDO – abgestimmt auf aktuelle regulatorische Vorgaben.

bitkom
learning
campus

Ihre Plattform für die Skills von morgen!

Die Bitkom Akademie ist Partner.

Der Bitkom Learning Campus bietet vielfältige Weiterbildungsformate, von kuratierten Seminaren bis hin zu kostenfreien Inhalten. Mit KI-basierter Lernunterstützung stellen wir individuelle Inhalte und automatisierte HR-Prozesse bereit – auf einer intuitiven Plattform und mit persönlichem Support.

Mehr als IT-Sicherheit:

Mit F24 zur Unternehmensresilienz

2025 markiert eine Zeitenwende für unternehmerische Sicherheit: Was früher als rein hypothetische Krisenszenarien galt, wird heute Realität für viele Unternehmen. Einschränkungen bei Mitarbeitenden-Reisen in die USA, plötzlich gesperrte E-Mail-Accounts oder rechtliche Unsicherheit bei internationalen Verträgen – die instabile geopolitische Lage zeigt, dass klassische IT-Sicherheitskonzepte allein längst nicht mehr ausreichen. Heute geht es vielmehr um Resilienz: die Fähigkeit, trotz widriger Umstände handlungsfähig und agil zu bleiben.

Autorin: Eske Ofner, Head of Sales, F24 AG

Resilienz bedeutet, Risiken frühzeitig zu erkennen sowie unter Druck konzentriert und anpassungsfähig zu agieren und so schnell wie möglich zurück in den Normalzustand zu kommen– sei es bei Cyberattacken, Lieferkettenproblemen oder politischen Schocks. Der von F24 unterstützte *„Resilience Vision 2030 Report"* des Business Continuity Institute (BCI) untermauert dies eindrucksvoll: 86,7 Prozent der befragten Experten aus über 50 Ländern sehen die Vermeidung von Betriebsunterbrechungen als größten wirtschaftlichen Gewinn von Resilienzmaßnahmen.

Herausforderungen im Blick: Vom technischen Schutz zum strategischen Handeln

Noch immer besteht bei vielen Firmen die Sicherheitsstrategie aus Firewall, Antiviren-Software, Backup-Lösungen und Excel-Listen für Kommunikationskaskaden im Krisenfall. Doch solche Einzelmaßnahmen reichen nicht aus, um in einer global vernetzten Wirtschaft dauerhaft zu bestehen. F24 verfolgt daher einen ganzheitlichen Ansatz – mit Tools, die weit über den reinen Schutz einzelner Systeme hinausgehen.

Bilder: F24

Unternehmen brauchen eine Lösung, die technische, organisatorische und strategische Ebenen verbindet.

Dazu gehört:

- die Identifikation und Bewertung aller relevanten Risiken, beispielsweise in IT, Lieferkette, Personal und Recht;
- verlässliche, schnelle Kommunikation in Krisen mit automatisierten Alarmierungs- und Kommunikationslösungen von F24;
- das kontinuierliche Training und Awareness-Schulungen mit Experten, zum Beispiel über die *F24 Academy*;
- die klare Zuordnung von Verantwortlichkeiten in der Organisation, beispielsweise mit dem neuen Chief Resilience Officer (CRO).

Klare Verantwortlichkeit mit dem Chief Resilience Officer

Allem voran braucht es in der heutigen Zeit erst einmal eine strategische Führung für Unternehmensresilienz durch eine klare Verantwortlichkeit auf C-Level-Ebene. Hier setzt der Chief Resilience Officer (CRO) an, der bereichsübergreifend IT-Sicherheit, Compliance, Lieferketten sowie interne und externe Kommunikation überwacht und koordiniert – eine bisher noch junge Rolle, die aber laut *„Resilience Vision 2030 Report"* bereits von 73 Prozent der Experten als essenziell für den Erfolg von Resilienzprogrammen gesehen wird. Der entscheidende Vorteil liegt darin, dass der CRO sowohl die komplexen Zusammenhänge der Resilienz in Unternehmen versteht und gleichzeitig auch mit den modernen Tools des Krisenmanagements – wie denen von der F24 AG – souverän arbeiten kann.

Technologie, die Resilienz wirklich ermöglicht

Resilienz lebt nicht nur von klaren Strukturen, sondern auch von Technologien, die in Echtzeit Orientierung und Übersicht bieten. F24 unterstützt mit Lösungen wie *TopEase* das ganzheitliche Risikomanagement: Risiken werden systematisch erfasst, bewertet und durch automatisierte Workflows in die Krisenprozesse eingebunden. Künstliche Intelligenz unterstützt heute schon bei der Auswertung von Chat-Protokollen, automatisiert Übersetzungen und generiert präzise Alarmierungstexte. So entsteht insgesamt ein Echtzeit-Überblick, mit dem man Bedrohungen frühzeitig erkennt, adäquat priorisiert und eine adaptive Steuerung schafft – statische Notfallpläne gehören damit der Vergangenheit an.

Verlässliche, schnelle Kommunikation in Krisen

Tritt der Krisenfall ein, zählt jede Sekunde. Verzögerungen bei der Informationsweitergabe können potenziell katastrophale Folgen haben. Die FACT24-Lösung von F24 bietet hierfür mit vorab angelegten Krisenszenarien automatisierte Alarmierungskaskaden, die Mitarbeiter und Stakeholder per SMS, App, E-Mail oder Telefon erreichen. Über intuitive Dashboards gelingt die koordinierte Steuerung von Kommunikationsströmen und die Nachverfolgung aller Maßnahmen. So sichert FACT24 die notwendige Transparenz und Kontrolle bei hohem Tempo.

Bild: Gorodenkoff – stock.adobe.com

Digitale Souveränität: Grundpfeiler moderner Resilienz

Ein oft unterschätzter Hebel für nachhaltige Resilienz ist die bewusste Wahl des Resilienz-Anbieters. In Zeiten geopolitischer Fragmentierung bedeutet die Entscheidung für europäische Lösungen langfristige Planbarkeit und ein stabiles regulatorisches Umfeld mit transparenten Gesetzen und Standards – ohne extraterritoriale Eingriffe wie etwa durch den US CLOUD Act. Unternehmen, die auf F24 setzen, schützen nicht nur ihre digitale Souveränität und Handlungsfähigkeit, sondern haben auch die Möglichkeit, auf Module zuzugreifen, die Krisenfälle direkt entsprechend den geforderten Richtlinien wie DORA (Digital Operational Resilience Act) für Behörden aufbereiten können.

Resilienz aktiv gestalten – mit F24

Der Weg von der reinen IT-Sicherheit hin zu digitaler Resilienz erfordert einen ganzheitlichen Ansatz aus Technologie, Führung und Kultur. F24 unterstützt Unternehmen dabei mit einem Produktportfolio, das Business-Continuity-Management, Krisenmanagement, Alarmierung, Governance und Compliance in Echtzeit abbildet.

Zudem begleitet F24 Organisationen dabei, Resilienz als kulturelles und organisatorisches Prinzip zu leben. Die *F24 Academy* schult Mitarbeitende für Krisenszenarien und sorgt mit regelmäßigen und strukturierten Trainings dafür, dass Software nicht nur vorhanden ist, sondern auch effizient genutzt wird – damit aus Tools echte Wettbewerbsvorteile entstehen. ■

Treffen Sie die F24 auf der it-sa Expo & Congress 2025!

Wann? 7.–9. Oktober 2025
Wo? Halle 6, Stand 102

Mehr dazu hier

F24

Warum Unternehmen ihre Sicherheitsarchitektur überdenken sollten

Cyber Security ist längst kein reines IT-Thema mehr – sie betrifft das gesamte Unternehmen. Ganzheitliche Sicherheitsstrategien, digitale Souveränität und der gezielte Einsatz künstlicher Intelligenz (KI) spielen dabei eine zentrale Rolle. Doch wer Angreifern stets einen Schritt voraus sein will, braucht mehr als Tools. Gefordert sind strategische Weitsicht, klare Strukturen und der Blick fürs Ganze.

Autor: Timo Schlüter, Business Owner Cyber Security bei Arvato Systems (www.arvato-systems.de)

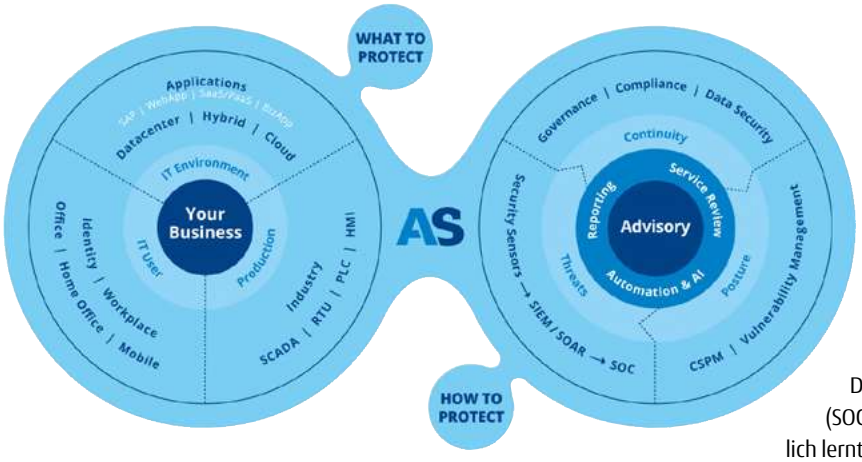
Die aktuellen Herausforderungen im Bereich Cyber Security sind vielschichtig: Cyberkriminalität hat sich zu einem hoch industrialisierten Geschäftsfeld entwickelt. Ebenso steigen die regulatorischen Anforderungen unaufhörlich – ein Umstand, der viele Unternehmen operativ überfordert. Auch ist die IT-Landschaft stark gewachsen und diversifiziert: Multi-Cloud-Umgebungen, vernetzte OT- und IoT-Anwendungen sowie hybride Arbeitsmodelle führen zu einer unüberschaubaren Anzahl an Angriffsflächen. Dass eine solche Infrastruktur schwer zu überwachen und zu schützen ist, liegt auf der Hand. Mehr noch: Diese Komplexität erschwert es, eigene Abhängigkeiten zu erkennen und effektiv zu managen. Um dieser Dynamik wirksam zu begegnen, braucht es vor allem zweierlei: digitale Souveränität als strategische Leitplanke und anpassungsfähige Sicherheitsarchitekturen.

Wettbewerbsfaktor digitale Souveränität

Digitale Souveränität ermöglicht es Unternehmen, selbstbestimmt Entscheidungen über ihre IT-Infrastruktur und Datenhaltung zu treffen. Diese Unabhängigkeit ist eine Voraussetzung, um Cyberbedrohungen schnell und effektiv zu managen. Dafür gilt es jedoch, Lock-in-Effekte zu reduzieren, sich also nicht ausschließlich an einen Anbieter zu binden. Besonders wirksam sind hier hybride Betriebsmodelle, die auf eine Kombination aus privaten und öffentlichen Cloud-Diensten setzen. Ebenso wichtig ist eine starke Governance der Daten und Prozesse, die zeigt, wo und wie Daten gespeichert und verarbeitet werden. Konzepte wie Zero Trust, Data Sovereignty Frameworks und Confidential Computing unterstützen dabei, den Datenfluss ins und aus dem Unternehmen zu kontrollieren und zu sichern.

Cyber Security: (k)eine Frage der Technologie

Doch Vorsicht: Eine Fokussierung allein auf Tools führt meist zu Silodenken, Insellösungen und losgelösten Einzelmaßnahmen, die letztlich wirkungslos bleiben. Ziel der IT-Sicherheit muss es jedoch sein, das Unternehmen businessfähig zu machen und nicht nur Daten und Systeme zu schützen. Damit das gelingt, muss Cyber Security selbst als Geschäftsprozess verstanden werden. Nur durch eine ganzheitliche Herangehensweise, die Sicherheitsmaßnahmen als integralen Bestandteil der Unternehmensführung sieht und diese kontinuierlich an die sich ändernden Geschäftsprozesse und Bedrohungslagen anpasst, lässt sich Cyber Security wirksam und dauerhaft verbessern.



Dauerbrenner Cyber Security

Die Bedrohungslage entwickelt sich ständig weiter – ebenso die regulatorischen Anforderungen. Entsprechend ist Cyber Security auch kein abgeschlossenes Projekt, sondern ein permanenter, dynamischer Prozess. Unternehmen müssen daher ihre Sicherheitsstrategien kontinuierlich überprüfen, anpassen und weiterentwickeln.

Damit das gelingt, braucht es eine ganzheitliche Perspektive. Technische Maßnahmen wie Bedrohungsmonitoring, Schwachstellenmanagement oder automatisierte Reaktionsmechanismen sind essenziell, genügen allein aber nicht. Sie wirken nur, wenn sie Teil einer Sicherheitsarchitektur mit klar definierten Zuständigkeiten sind, die fest im Unternehmen und in etablierte Prozesse eingebunden ist. Ebenso wichtig ist es, diese Schutzmechanismen regelmäßig zu testen – etwa durch Red Teaming, Krisenübungen oder Planspiele zur Notfallreaktion.

Doch Cyber Security muss auch in der Firmenkultur verankert sein. Nur wenn die Belegschaft sensibilisiert ist und Sicherheit als Teil ihres Arbeitsalltags versteht, kann eine entsprechende Strategie tatsächlich greifen. Wer Cyber Security als lebendigen Bestandteil der Unternehmensführung versteht, schafft nicht nur mehr Sicherheit, sondern auch die Resilienz, die nötig ist, um trotz wachsender Risiken handlungsfähig zu bleiben.

Zwischen Tool-Overload und Fachkräftemangel

Die Umsetzung moderner Cyber Security scheitert in der Praxis häufig an mehreren Faktoren. Zum einen wissen viele Unternehmen nicht, wo sie anfangen sollen – oder verlieren sich im Überangebot an verfügbaren Sicherheitstools. Zum anderen fällt es ihnen schwer, sich im Dschungel an Regulatorien zurechtzufinden. Der Aufbau interner IT-Expertise wird wiederum oft durch den eklatanten Fachkräftemangel ausgebremst. Entlastung versprechen hier Managed Security Service Provider (MSSPs): Dienstleister wie Arvato Systems verfügen über das nötige Fachwissen und übernehmen zugleich die kontinuierliche Überwachung der Systeme.

Künstliche Intelligenz: Fluch und Segen

Auch die KI spielt eine immer größere Rolle in der Cyber Security. Cyberkriminelle nutzen sie, um ihre Attacken zu automatisieren, zu personalisieren und zu skalieren. Für die Unternehmen wiederum bietet KI enorme Chancen in puncto Verteidigung, etwa durch die frühzeitige Erkennung von Anomalien und automatisierte Reaktionen. Voraussetzung für den erfolgreichen Einsatz von KI in Unternehmen ist jedoch eine solide Datenbasis. Eine saubere Configuration Management Database (CMDB) hilft, die eigene IT-Infrastruktur besser zu verstehen und schneller auf Angriffe zu reagieren.

Das Problem: Bei vielen KI-Modellen fehlt die Transparenz darüber, wie sie zu ihren Entscheidungen kommen. Auch Verzerrungen in der Bewertung von Risiken oder Anomalien sind kritisch. Beides fördert nicht gerade das Vertrauen in KI-gestützte automatisierte Sicherheitsprozesse. Solange das der Fall ist, bleiben Hybrid-Modelle das Mittel der Wahl: Der Mensch übernimmt die Federführung bei Entscheidungen, während die KI Vorschläge macht und Routineaufgaben erledigt. Die Zukunft könnte jedoch in adaptiven Security Operations Center (SOCs) liegen, in denen KI nicht nur unterstützt, sondern kontinuierlich lernt, Risiken neu bewertet und potenzielle Angriffswege simuliert. Damit wäre proaktives Handeln möglich – und Unternehmen wären den Angreifern stets einen Schritt voraus.

Fazit: Cyber Security – der Schlüssel zur Zukunftsfähigkeit

Cyber Security ist keine Frage von Technik allein. Sie ist ein strategisches Thema, das tief in Geschäftsprozesse, Governance und Unternehmenskultur eingebettet sein muss. Digitale Souveränität, ein ganzheitlicher Blick auf Sicherheit und der gezielte Einsatz von KI sind zentrale Bausteine, um Unternehmen widerstandsfähig gegenüber aktuellen und zukünftigen Bedrohungen zu machen. Unternehmen, die Cyber Security als ein geschäftskritisches und erfolgsrelevantes Thema behandeln, sichern ihre Handlungs- und Zukunftsfähigkeit – auch dann, wenn sich Bedrohungslagen sowie technologische und regulatorische Rahmenbedingungen verändern. ■

Sie haben Fragen rund um Cybersecurity oder andere IT-Themen? Unsere Experten beraten Sie gern! Kontaktieren Sie uns oder **besuchen Sie uns auf der it-sa: 7.–9.10.2025 in Nürnberg, Halle 7A-416** (Bitkom Security Area). Wir freuen uns auf Sie!

Steigen Sie noch tiefer in das Thema ein. Auf dem Cybersecurity Summit 2025 gab Speaker Timo Schlüter von Arvato Systems mit seinem Vortrag ***„Vom Kostenfaktor zum Business Enabler – Cyber Security neu positionieren"*** einen praxisnahen Einblick in die Cyber-Security-Landschaft von heute und morgen.

Hier geht's zum Video

Arvato Systems GmbH
Reinhard-Mohn-Straße 18
33333 Gütersloh

Ansprechpartner:
Timo Schlüter, Business Owner Cyber Security
Telefon +49 5241 80 70770
E-Mail: cybercare@arvato-systems.de
Internet: arvato-systems.de

Mehr dazu hier

ARVATO SYSTEMS

Was Sie bei einem NIDS für die OT beachten sollten

Das IT-Sicherheitsgesetz und die Implementierung der NIS-2-Direktive fordern für kritische Anlagen den Einsatz eines Systems zur Angriffserkennung. Ein netzbasiertes Sicherheitsmonitoring ermöglicht die Einhaltung der Compliance-Vorschriften auch in sensiblen industriellen Umgebungen und erfüllt die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Autor: Uwe Dietzmann, Sales Manager, Rhebo GmbH

Im April 2025 öffneten bisher nicht identifizierte Akteure über Fernzugriff die Abflussventile des Damms am norwegischen Risevatnet-See. Zuvor hatten sie über das schwache Passwort einer OT-Komponente Zugriff zur Steuerungstechnik erlangt. Erst vier Stunden später fiel den Betreibern auf, dass pro Sekunde 497 Liter mehr Wasser in das darunterliegende Flussbett abgegeben wurden. Zwar kam es zu keinen Schäden, doch der Vorfall verdeutlicht drei Realitäten:

1. OT-Netzwerke werden mittlerweile gezielt angegriffen.
2. Firewalls allein sind machtlos in einer Angriffslandschaft, die immer stärker Techniken nutzt, welche die Perimetersicherung gezielt umgehen oder durch signaturbasierte Abwehr nicht erkennbar sind.
3. OT-Netzwerke kranken noch immer an ihrer Vergangenheit, in der Cybersicherheit keinerlei Rolle gespielt hat.

Letzteres bestätigen auch Ergebnisse aus Schwachstellenbewertungen im Rahmen von Rhebo Industrial Security Assessments in OT-Umgebungen industrieller und kritischer Anlagen. In allen untersuchten Netzwerken fanden sich veraltete, unsichere Protokolle und Authentifizierungsmethoden. In über der Hälfte aller Assessments wurden verwundbare Systeme und Verbindungsversuche ins Internet detektiert (siehe Abb. 1).

Weltweit nimmt zudem die Zahl der identifizierten Schwachstellen in IT- und OT-Systemen zu. In den ersten fünf Monaten des laufenden Jahres wurden rund 20.000 CVEs (Common Vulnerabilities and Exposures) veröffentlicht, ein Zuwachs von 16 Prozent gegenüber dem Vorjahreszeitraum. Während das Bekanntwerden von Schwachstellen grundsätzlich positiv zu werten ist, stecken viele Anbieter und Nutzer in einem enormen Patch-Backlog. Vor allem in OT-Umgebungen birgt das Patching von Komponenten ein hohes Risiko längerer Stillstandzeiten. Zugleich überholen laut Googles M-Trends Report Schwachstellen (33 %) und gestohlene Zugangsdaten (16 %) klassische Phishing-Kampagnen (14 %) als initiale Angriffsvektoren. Auch Innentäter sind mit 5 Prozent nicht unerheblich. Ein Großteil der Angriffe läuft damit an Firewalls vorbei.

Ein NIDS stellt die innere Sicherheit her

Das BSI empfiehlt deshalb bereits seit mehreren Jahren den Einsatz eines Sicherheitsmonitorings mit Anomalieerkennung in industriellen Umgebungen – erstmals 2019 für Produktionsnetzwerke (BSI-CS 134) und zuletzt im März 2025 für Umspannwerke (BSI-CS 153). Bei diesen netzbasierten Intrusion-Detection-Systemen (NIDS) geht es nicht um einen Ersatz der bestehenden Sicherheitsinfrastruktur aus Firewalls, Authentifizierung und Rechtemanagement, die auf die Prävention von Vorfällen setzen. Vielmehr steht die Detektion von Vorgängen und sicherheitsrelevanten Ereignissen im Vordergrund, die durch die präventiven Maßnahmen zunehmend nicht abgedeckt werden können. Dazu gehören insbesondere die bereits erwähnten Angriffsvektoren über Schwachstellen und gestohlene Zugangsdaten, aber auch über die Lieferkette (Supply Chain Compromise) sowie verschleiernde Angriffstechniken wie Living-Off-The-Land (LOTL).

Bild: ImageFlow - stock.adobe.com

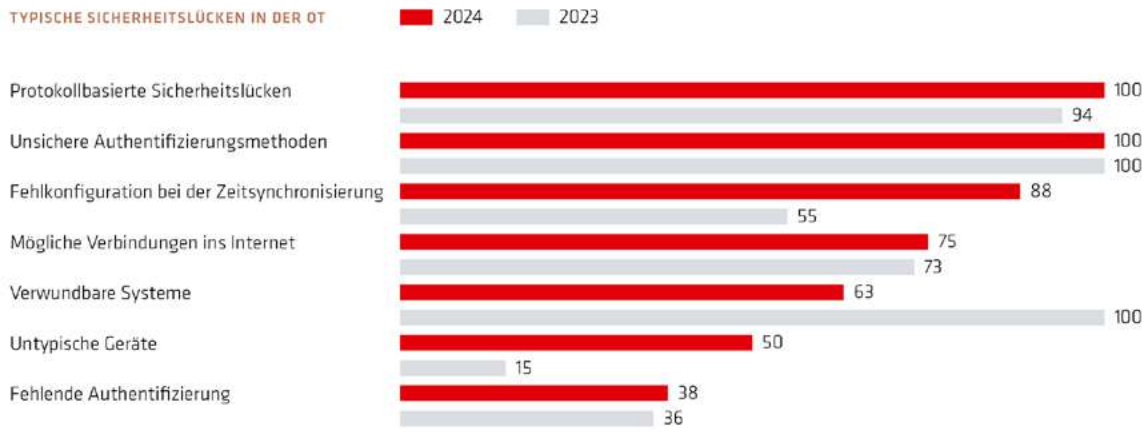


Abb. 1: Entwicklung der häufigsten OT-Sicherheitsrisiken zwischen 2023 und 2024

NIDS ergänzen damit die präventiven Maßnahmen in einer erweiterten, komplexeren Risikolandschaft. Diese Ergänzung erfolgt über zwei Prinzipien:

1. Das NIDS überwacht nicht den Perimeter (auch wenn es dort ebenfalls eingesetzt werden kann), sondern das gesamte innere Netzwerk – in industriellen Anlagen somit die gesamte OT (siehe Abb. 2).

2. Das NIDS nutzt Anomalieerkennung, um neuartige oder verschleierte Angriffstechniken zu erkennen, die durch die Signaturbibliotheken nicht abgedeckt sind.

Das netzbasierte Angriffserkennungssystem Rhebo Industrial Protector beispielsweise spiegelt dafür den Netzwerkverkehr über einen Mirrorport oder Netzwerk-Tap und analysiert kontinuierlich die Pakete auf Abweichungen vom zu erwartenden Kommunikationsverhalten. Dabei werden sowohl OT- als auch IT-Protokolle berücksichtigt. Abweichungen werden nach ihrem Risiko bewertet und den Verantwortlichen inklusive der Meta- und forensischen Daten gemeldet.

Neben sicherheitsrelevanten Ereignissen (SRE) detektiert Rhebo Industrial Protector auch technische Fehlerzustände, die in der OT zu unerwünschten Latenzen oder Übertragungsfehlern führen und die industriellen Echtzeitprozesse gefährden können.

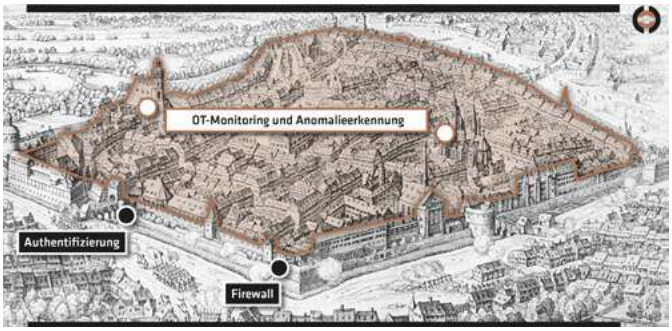


Abb. 2: Ein NIDS stellt die Innenansicht und damit die innere Sicherheit eines OT-Netzwerks sicher.

Der Teufel steckt im Detail

Ein NIDS sollte insbesondere in der OT einigen Prämissen folgen, um die empfindlichen industriellen Prozesse nicht zu stören und nicht zum eigenen Sicherheitsrisiko zu werden:

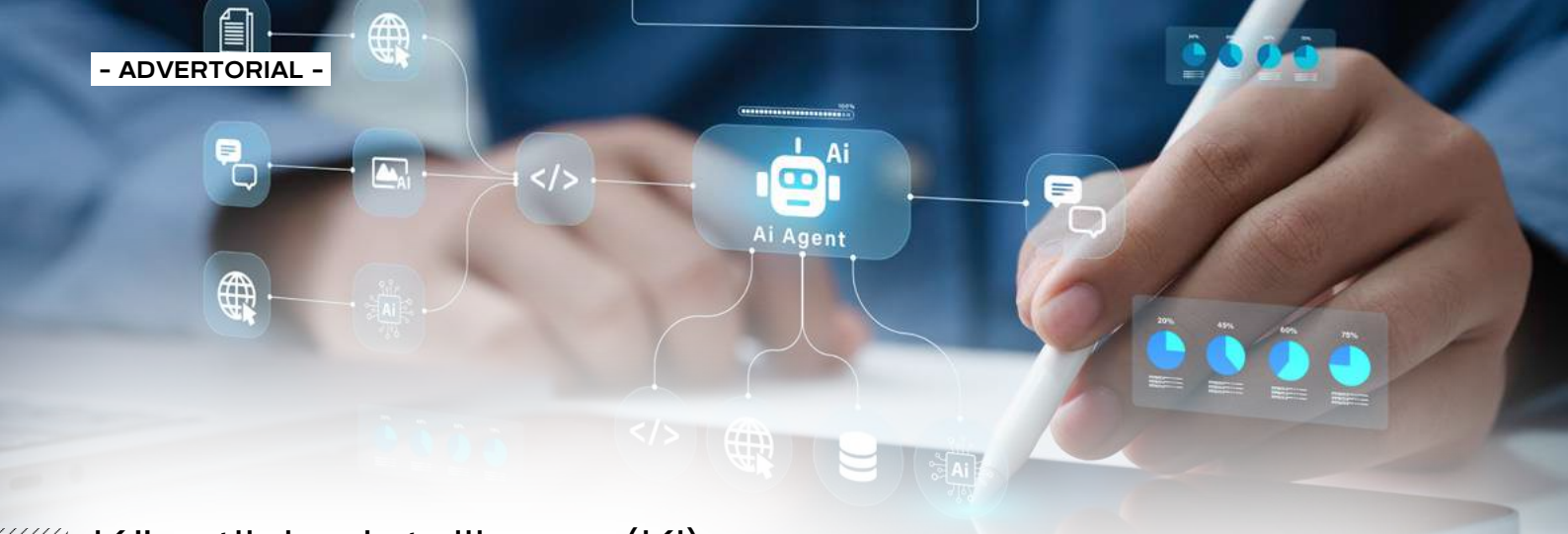
- Das Monitoring erfolgt passiv, um die limitierten Datenkapazitäten der OT-Infrastruktur nicht zu belasten.
- Detektion und Meldung sind rückwirkungsfrei, es erfolgt kein automatisches Blockieren von Verkehr.
- Das für die OT entwickelte NIDS kann über Schnittstellen zu SIEM-Systemen in die übergeordnete Unternehmens-Cybersicherheit eingebunden werden. Damit schließt das NIDS die bestehende Sichtbarkeits- und Protokollierungslücke zur OT, die in vielen Unternehmen-SIEMs noch immer besteht.
- Das NIDS kann On-Premises eingesetzt werden, es besteht kein separater Fernzugang oder Cloud-Zwang. Insbesondere bei Lösungen aus nicht-europäischen Ländern und mit Cloud-Anbindung sollte genau nachgefragt werden, wie das Datenhandling erfolgt und zum Beispiel mit dem US CLOUD Act umgegangen wird. Aus Perspektive der digitalen Souveränität lohnt ein Blick auf europäische und deutsche Anbieter.
- Da OT-Sicherheit in vielen Unternehmen noch Neuland ist und oftmals mit einem NIDS erstmalig Sichtbarkeit in der OT geschaffen wird, sollte auf einen verlässlichen Service seitens des Anbieters geachtet werden. Das betrifft vor allem die Aspekte Baselining und Training-on-the-job.
- Auch die Lizenzstruktur sollte genau geprüft und mit der voraussichtlichen Entwicklung der eigenen OT abgeglichen werden. Eine Abrechnung nach der Anzahl der überwachten Assets oder dem Traffic-Volumen kann mittelfristig die Kosten für ein NIDS nach oben treiben. Weiterhin sollte vorab geklärt werden, welche Funktionen des NIDS als Add-on hinzugekauft werden müssen. Auch das kann die Total Cost of Ownership mitunter stark erhöhen. Rhebo setzt deshalb auf eine transparente, stabile Preispolitik – ohne dynamische Faktoren wie Anzahl der Assets oder Funktionen.

Ein dediziert für die OT entwickeltes NIDS schafft unter diesen Voraussetzungen Sichtbarkeit und Sicherheit in einer sich stark verändernden OT, in der Vernetzung, Fernwirkung und Flexibilität immer wichtiger werden. ■

Mehr dazu hier

Rhebo
a Landis+Gyr company

- ADVERTORIAL -



Künstliche Intelligenz (KI)

Warum AI Gateways zum Schutz nötig sind

KI-Agenten benötigen Zugang zu Ressourcen wie Dienste, Tools und Daten, um ihre Aufgaben zu erfüllen. Aber dieser Zugriff darf nicht unbegrenzt sein. Damit er nur im entsprechenden Kontext erlaubt ist, sind sogenannte AI Gateways erforderlich, die auf APIs basieren.

Autor: Stephan Schulz,
Senior Prinicipal Solutions Engineer, F5

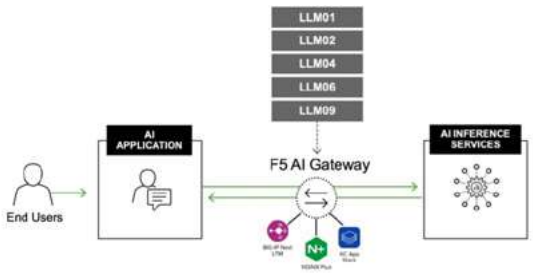
Alle aktuellen Geschäftsanwendungen stellen ihre Funktionen über APIs (Application Programming Interface) bereit. Dabei konsolidieren Gateways API-übergreifende Funktionen wie Benutzerzugriff, Autorisierung und Service-Erkennung. Auch für KI-Agenten sind APIs von entscheidender Bedeutung, denn sie benötigen eine klare Abgrenzung, auf welche Ressourcen sie zugreifen dürfen und welchen Sicherheitskontext sie für jede ihrer Aktionen verwenden sollen.

Wenn ein Agent mehrere Aufgaben ausführt, sind eventuell verschiedene Autorisierungen unter Verwendung unterschiedlicher Sicherheitskontexte nötig. Auch Eingaben und Antworten variieren stark und entwickeln sich im Laufe der Zeit weiter. Zudem steigt der Bedarf an leistungsfähigen APIs mit der Anzahl der Agenten. APIs müssen daher einen angemessenen Zugriff automatisch und in extrem großem Umfang ermöglichen.

Der KI-Torwächter

Bestehende Lösungen für die API- und Anwendungssicherheit reichen daher nicht aus, um KI-Modelle und -Anwendungen zu schützen. Der F5 AI Gateway sichert, beschleunigt und überwacht dagegen speziell KI-gestützte Anwendungen. Dabei erfüllt er die wichtigsten Anforderungen für ihre Bereitstellung und die OWASP LLM Top Ten-Liste für die Sicherheit.

Zusätzliche Funktionen ermöglichen die Berichterstattung über eine Vielzahl von Metriken mithilfe von OpenTelemetry, die sorgfältige Beachtung von Audit-Protokollanforderungen, semantisches Caching, Ratenbegrenzung und inhaltsbasiertes Modell-Routing. Sie gewährleisten die Unterstützung aller drei Anforderungen an die Bereitstellung und Sicherheit von KI: beobachten, schützen und beschleunigen. Dabei können Unternehmen die Lösung durch ein Plug-in-Ökosystem an individuelle und neue Anforderungen anpassen. Es wird durch ein Software Development Kit (SDK) für Python, Rust und Go unterstützt.



OWASP LLM TOP TEN	
LLM01	PROMPT INJECTION
LLM02	INSECURE OUTPUT HANDLING
LLM03	TRAINING DATA POISONING
LLM04	MODEL DENIAL OF SERVICE
LLM05	SUPPLY CHAIN
LLM06	SENSITIVE INFO DISCLOSURE
LLM07	INSECURE PLUGIN DESIGN
LLM08	EXCESSIVE AGENCY
LLM09	OVERRELIANCE
LLM10	MODEL THEFT

F5 AI Gateway erfüllt die Anforderungen zur Bereitstellung und Echtzeit-Sicherheit von Anwendungen, inklusive der OWASP LLM Top Ten.

Bild: Deemerwha studio - stock.adobe.com

Datenlecks erkennen und verhindern

Hinzu kommt das Erkennen und Verhindern von Datenlecks in KI-gestützten Anwendungen. Dazu integriert die Lösung eine proprietäre Echtzeit-Datenklassifizierungs-Engine überall dort, wo KI-Eingaben und -Antworten erfolgen. Sie bewertet jeden Inhalt inline, sodass KI-Konversationen nahtlos fortgesetzt werden, während die Sicherheit für die Inferenz gewährleistet ist. Dabei erkennt AI Gateway ein breites Spektrum sensibler Inhalte, etwa:

- personenbezogene Daten (Personally Identifiable Information, PII) wie Identifikationsnummern, E-Mail-Adressen, Post-Adressen und Telefonnummern;
- Finanzdaten einschließlich Kontonummern, Kreditkartennummern und Transaktionsaufzeichnungen;
- Gesundheitsdaten bis hin zu Behandlungsnotizen;
- sensible Informationen wie Quellcode oder Konfigurationsdateien;
- vertrauliche Dokumente, die im Unternehmen bleiben müssen.

Wenn die Lösung zu schützende Inhalte erkennt, steuern vordefinierte Richtlinien den Datenfluss. Dies geschieht durch Protokollierung des Ereignisses für Audits, Schwärzung des sensiblen Textes oder vollständige Blockierung der Eingabeaufforderung oder Antwort. Mit der Durchsetzung von Richtlinien in Echtzeit stellen Unternehmen sicher, dass sensible Daten niemals die Umgebung verlassen oder zur Erzeugung von Ausgaben beitragen.

Einfache Einrichtung

Als Bestandteil der F5 ADSP (Application Delivery and Security Platform) ist AI Gateway einfach einzurichten und zu optimieren. Teams können mit minimalem Aufwand Richtlinien erstellen und Erkennungsparameter für verschiedene Umgebungen verfeinern. Erweiterte Erkennungsfunktionen lassen sich mit eingesetzten Sicherheitstools verbinden, beispielsweise mit SIEM- (Security Information and Event Management) und SOAR- (Security Orchestration, Automation and Response) Plattformen. So können Analysten Vorfälle schnell korrelieren und automatisierte Reaktionen auslösen.

Für Teams, die Anwendungen entwickeln, erfolgt der Inline-Durchsetzungsprozess transparent. Dabei bleibt die Geschwindigkeit und Effizienz der KI-Interaktionen gewahrt. Benutzer erhalten nur konforme Antworten, während Administratoren von Transparenz und Sicherheit in großem Maßstab profitieren, ohne die Nutzererfahrung zu beeinträchtigen.

Governance und Skalierbarkeit

KI-Implementierungen erstrecken sich oft über interne Systeme, verwaltete Cloud-Dienste und externe Inferenzpunkte über verschiedene Regionen hinweg. Als Teil von F5 ADSP stellt AI Gateway sicher, dass Sicherheitsstandards in diesen Umgebungen konsistent durchgesetzt werden, auch während des Modell-Routings. Dies umfasst:

- kontinuierliche Prüfung und Überwachung des Datenzugriffs und der Datenübertragung in jeder Bereitstellungsumgebung;
- starke Authentifizierung und Autorisierung sowie Berechtigungsverwaltung und rollenbasierte Zugriffskontrolle (RBAC), um Benutzeraktionen am Prinzip der geringsten Berechtigung auszurichten;
- Inline-Bewertung jeder Eingabe und Antwort, die Inhalte sofort blockiert oder redigiert, ohne auf externe Proxys oder Endpunkt-Agenten angewiesen zu sein.

Durch diese Funktionen müssen Unternehmen ihre Governance-Richtlinien nur einmal festlegen. Anschließend werden sie überall dort, wo KI-Teams tätig sind, konsistent angewendet.

Erweiterbarkeit für individuelle Anforderungen

Unternehmen definieren sensible Daten unterschiedlich, von Kundenlisten über geistiges Eigentum bis hin zu domänenspezifischen Regeln. Entsprechend ist AI Gateway hochgradig erweiterbar. So können Entwickler benutzerdefinierte Detektoren erstellen, Routing-Logik für große Sprachmodelle (LLM) definieren und erweiterte Bereinigungsregeln implementieren. Die Detektoren lassen sich in Durchsetzungsrichtlinien integrieren und bieten Echtzeit-Anpassungen sowie eine einheitliche Durchsetzungsebene, ohne den Betrieb zu stören.

Verbesserte Beobachtbarkeit

Governance hängt von der vollständigen Transparenz des Datenflusses ab – von Benutzer-Prompts zu KI-Modell-Antworten und zurück. AI Gateway bietet eine erweiterte Protokollierung, die jede auf eine Eingabe angewendete Transformation und Antwort sowie Metadaten aufzeichnet. Unternehmen können somit die gesamte Datenpipeline hinweg prüfen oder visualisieren, damit Entwicklungsteams Fehler schneller beheben, Compliance-Teams die Einhaltung von Unternehmensrichtlinien überprüfen und Betriebsteams die Interaktion von KI-Tools mit der zugrunde liegenden Infrastruktur kontinuierlich optimieren.

Fazit

Mit AI Gateway verbessern Unternehmen die Interaktion zwischen Anwendungen, APIs und großen Sprachmodellen (LLMs). Die leistungsstarke containerisierte Lösung optimiert die Performance, Beobachtbarkeit und Sicherheit – und senkt die Kosten. Sie ermöglicht Betriebs- und Sicherheitsteams eine reibungslose Einführung von KI-Diensten mit einer deutlich höheren Qualität der Datenausgabe und einem besseren Nutzererlebnis. ■

Für mehr Informationen besuchen Sie uns gern auf der it-sa (Halle 7A-531).

Mehr dazu hier

Souveräne IT-Sicherheit in der Praxis

Autor: Martin Mangold, Senior Vice President Platform & Operations, DriveLock SE

Ohne digitale Souveränität wird es auch mit der europäischen Souveränität nichts", sagte Claudia Plattner – jetzt Präsidentin des BSI – im Jahr 2022, als sie noch IT-Leiterin der Europäischen Zentralbank war. Mit dieser Aussage unterstreicht sie die Relevanz der digitalen Souveränität für den europäischen Raum.

Der Begriff der digitalen Souveränität

Zunächst geht es um die Begriffsklärung, denn „digitale Souveränität" ist eine facettenreiche Vokabel. Verortet wird „Souveränität" zunächst auf der staatlichen Ebene, wenn es darum geht, die Handlungsfähigkeit von Staaten zu beschreiben, insbesondere die Fähigkeit des Staates, digitale Vorgänge zu kontrollieren, die einen Einfluss auf sein Territorium haben und bei denen der Staat selbst oder staatliche Institutionen betroffen sind. Der Begriff beschränkt sich aber nicht nur auf die Kontrolle über digitale Prozesse und Technologien. Er umfasst darüber hinaus zusätzlich folgende Aspekte:

1. **Digitale Selbstbestimmung:** Individuen und Organisationen sollen die Kontrolle über ihre eigenen Daten und Informationen haben. Dies bedeutet, dass sie kontrollieren können, wer auf die Daten zugreifen darf, und die Möglichkeit, datengetriebene Prozesse (Wie kontrolliere ich Daten, den Zugriff auf diese und wer/was sie nutzt?) aktiv zu gestalten.

2. **Unabhängigkeit von externen Technologien und Diensten:** Die Abhängigkeit von Technologiekonzernen birgt Risiken, etwa durch den sogenannten Hersteller-Lock-in. Dieser erschwert Kunden aufgrund technischer oder wirtschaftlicher Barrieren den Wechsel von Produkten oder Dienstleistungen eines bestimmten Herstellers. Die Reduzierung von Wahlmöglichkeiten durch Hersteller-Monopole hat unmittelbaren Einfluss auf die digitale Selbstbestimmung.

3. **Datenkontrolle und -schutz:** Daten haben einen Bedeutungsgehalt, der weit über den Ort ihrer Speicherung hinausgeht. Kontrolle über

Bild: Intelligent Horizons - stock.adobe.com

die Daten beinhaltet daher nicht nur deren physischen Schutz, sondern auch die Sicherstellung ihrer Integrität sowie die Kontrolle über ihre Verwendung.

Resilienz: Anpassungsfähigkeit an Herausforderungen

Im Kontext der „digitalen Souveränität" spielt der Begriff „Resilienz" eine wichtige Rolle. Er bezeichnet die Fähigkeit, auf unerwartete Herausforderungen zu reagieren und trotzdem funktionsfähig zu bleiben. Konkret bedeutet dies:

- **Anpassungsfähigkeit:** Flexibilität im Umgang mit (gesetzlichen) Änderungen, die erhebliche Auswirkungen auf die Datensicherheit und -integrität haben können, zum Beispiel dem US-Cloud-Act. In diesem Zusammenhang bedeutet Resilienz, dass sich ein IT-System und die dahinterstehenden Prozesse schnell an neue Rahmenbedingungen anpassen können, ohne die eigenen Schutzstandards zu gefährden.
- **Sicherheitsstrategien:** Robuste Sicherheitsmaßnahmen, die unter anderem bei verstärkten Cyberangriffen wirksam bleiben. Eine resiliente IT-Infrastruktur ist nicht nur gegen Angriffe gehärtet, sondern kann schnell wiedergestellt werden, sollte ein Angriff erfolgreich sein.
- **Kontinuität:** Sicherstellung der Verfügbarkeit und Integrität der IT-Dienste – auch bei Störungen –, um die Handlungsfähigkeit von Staaten und Unternehmen zu gewährleisten.
- **Transparenz:** Kommunikation und Aufklärung gegenüber der Bevölkerung, um Vertrauen zu stärken und Unsicherheiten zu minimieren.

Digitale Souveränität in der Praxis

Sicherheit und Souveränität: Zwei Seiten derselben Medaille

Um digitale Souveränität in der Praxis zu gewährleisten, müssen Sicherheit und digitale Souveränität zusammen gedacht und umgesetzt werden. Diese strategische Herangehensweise ermöglicht es, resiliente Strukturen aufzubauen und Sicherheitsrisiken zu reduzieren.

Security Controls: Maßnahmen gegen Cyberangriffe

Ein zentrales Element dieser Strategie sind die Security Controls – also Maßnahmen gegen Cyberangriffe, die entlang der gesamten Kill Chain positioniert werden. Diese umfassen mehrere Bereiche:

- **Mitarbeitende:** Schulung und Sensibilisierung für Cybergefahren, um menschliche Fehler zu minimieren und ein hohes Sicherheitsbewusstsein zu fördern. Es geht darum, eine Sicherheitskultur zu etablieren.
- **Endgeräte:** Schutz vor unbefugtem Zugriff und Malware, um die Integrität und Vertraulichkeit der auf den Geräten gespeicherten Daten sicherzustellen.
- **Applikationen:** Sicherstellung der Integrität und Authentizität von Software. Nur vertrauenswürdige Anwendungen dürfen ausgeführt und eingesetzt werden. Darüber hinaus geht es um die Kontrolle, was Applikationen tun dürfen bzw. auf welche Daten sie zugreifen dürfen.
- **Daten:** Verschlüsselung und Zugangskontrollen, um die Vertraulichkeit und Sicherheit sensibler Informationen zu gewährleisten.

Digitale Souveränität geht jedoch über reine Sicherheitsmaßnahmen hinaus und umfasst auch die Kontrolle über digitale Prozesse, Daten und Technologien.

- **Digitale Prozesse:** Integration und transparente Steuerung der IT-Prozesse zur Sicherstellung einer nahtlosen und sicheren Zusammenarbeit der Systeme
- **Daten:** Schutz sensibler Daten vor unbefugtem Zugriff und sichere Verwaltung gemäß den gesetzlichen Datenschutzrichtlinien
- **Technologien:** Einsatz souveräner IT-Lösungen, die nicht von externen Anbietern abhängig sind, um die Kontrolle und die Flexibilität über die eingesetzten Technologien zu gewährleisten

Wenn Sicherheit und digitale Souveränität Hand in Hand gehen, erhöht dies die Widerstandsfähigkeit (Resilienz) der IT-Infrastrukturen von Staaten und Unternehmen. Dies stellt ihre Unabhängigkeit und Selbstbestimmung in der digitalen Welt sicher.

Fazit

Digitale Souveränität ist keine isolierte Herausforderung, sondern ein integraler Bestandteil einer modernen Cybersicherheitsstrategie. Staat und Unternehmen müssen gemeinsam die Verantwortung für Sicherheit, digitale Selbstbestimmung und Resilienz übernehmen. Dies erfordert nicht nur den Aufbau souveräner IT-Infrastrukturen, sondern auch die Entwicklung ganzheitlicher Sicherheitskonzepte.

Souveränität wird schnell als „Abschottung" verstanden. Das ist sie ausdrücklich nicht. Vielmehr geht es um die Fähigkeit, Kontrolle und Selbstbestimmung auszuüben. In einer global vernetzten Welt ist es entscheidend, flexibel und handlungsfähig zu bleiben, um die digitale Souveränität in Europa zu gewährleisten. Nur so kann, wie von Claudia Plattner betont, die digitale Souveränität ein Grundpfeiler der europäischen Souveränität werden. ■

Quellen:

https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html

https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/eckpunktpapier-digitale-souveraenitaet.pdf?__blob=publicationFile&v=4

https://www.inside-it.ch/lex-laux-was-ist-digitale-souveraenitaet

https://de.wikipedia.org/wiki/Digitale_Souver%C3%A4nit%C3%A4t

https://www.netzwoche.ch/news/2023-12-08/warum-digitale-souveraenitaet-aufgabe-des-staates-ist

Mehr dazu hier

DriveLock

Mobiles Outdoor-Data-Center „asfm-TMC-09s mobile DataCenter" zur Miete/zum Mietkauf oder auch Direktkauf – sofort verfügbar.

Egal ob Backup oder IT-Erweiterung – Leistung lokal vor Ort.

Das asfm-mobile DataCenter als 3-Raum-System komplett mit aller Infrastruktur ausgestattet zur IT-Installation vorbereitet. Vier 19-Zoll-Racksysteme mit intelligenten PDUs, USV-Batterie-Anlage 20 kVA, Klimatechnik 20 kW, Branddetektion mit NOVEC 1230 Minimax Löschsystem, Brandfrühesterkennungssystem, Überwachung Temperaturen und Techniksysteme mit Monitoringsystem und GSM-Meldetechnik Ereignisse per SMS und optional Videokameras im Inneren, alles nach Stand der Technik an „Bord" und sofort einsatzbereit. Komplette Anlage VdS-geprüft und abgenommen.

asfm GmbH

active service facility management

asfm GmbH

+49 (0) 2224 – 989 220

Mehr dazu hier

Titelstory der asfm GmbH erschienen im Magazin BODENSEE WIRTSCHAFT & WISSENSCHAFT, Ausgabe 01/25

PDF

PCert® –

Bereit für bewährte Post Quantum Migration, kryptografische Inventur, Risikomanagement, Prüfung und Optimierung des Managements Ihrer PKI?

Wie meistern Sie Ihre Herausforderungen des kryptografischen Wechsels Ihrer gesamten Infrastruktur ohne einen vollständigen Überblick?

Kennen Sie alle Ihre internen Schwachstellen oder Risiken?

Kann Ihr Unternehmen Compliance nachweisen?

Die automatisierte, skalierbare Enterprise-Plattform PCert® von Data-Warehouse ist die Lösung.

Regulierungen fordern, existierende Schwachstellen oder Risiken in digitalen Kernsystemen aufzudecken. Dies ist eine umfassende Herausforderung an C-Suites. Wir helfen Ihrem Unternehmen beim Aufbau eines vollständigen kryptografischen Inventars, das es Ihnen ermöglicht, mit einer transparenten und minimal-invasiven Integration Compliance zu erreichen und nachzuweisen.

Auch US-Behörden nutzen PCert®-Ergebnisse, um neue Standards für PQM zu definieren.

Sprechen Sie mit uns, um Ihre Strategie zu optimieren. **Wir sind auf der it-sa 2025 in Nürnberg, Halle 7, Stand 307**

Data-Warehouse GmbH

Data-Warehouse GmbH – Software aus Deutschland

Beethovenstr. 33–35
85521 Ottobrunn
https://datawh.info
info@dwh.gmbh

Mehr dazu hier

Industrial Cybersecurity „Made in Germany"

Die Absicherung von OT- und IoT-Infrastrukturen ist für Industrieunternehmen eine wichtige Herausforderung. Unterschiedlichste Geräte und Dienste müssen sicher und geschützt kommunizieren können. Auch **KI-Agenten** müssen authentifizierbar sein und zuverlässig in Zero Trust-Architekturen eingebunden werden.

PKI- und Lifecycle-Management

Der deutsche IT-Security-Hersteller ECOS Technology zeigt auf der **it-sa 2025 (Halle 9/9-248)** die neueste Version seiner PKI- und Key-Management-Lösung ECOS TrustManagementAppliance (TMA). Die TMA deckt sämtliche Funktionen rund um das Erstellen, Speichern, Verteilen, Verlängern und Zurückziehen von Zertifikaten und Schlüsseln ab. Mit sicheren Maschinenidentitäten wird so die Grundlage für Industrial Cybersecurity geschaffen.

Zertifikate und Schlüssel jetzt auch VS-NfD-konform managen

Die ECOS TrustManagementAppliance hat durch das BSI die offizielle Einsatzerlaubnis für den Schutzbedarf „Verschlusssachen – nur für den Dienstgebrauch" (VS-NfD) erhalten. Die Lösung kann dadurch als Basis für eine sichere Public-Key-Infrastruktur auch in besonders geschützten Netzwerken in Industrie und Verwaltung beim Umgang mit eingestuften vertraulichen Inhalten zum Einsatz kommen.

Kontakt

ecos

ECOS Technology GmbH

Sant' Ambrogio-Ring 13 a-b
55276 Oppenheim
Tel: +49 6133 939-222
E-Mail: info@ecos.de
www.ecos.de/iot

Mehr dazu hier

Forschung trifft Praxis:
Das Lernlabor Cybersicherheit

Lernlabor Cybersicherheit, © Fraunhofer IESE

Cyberangriffe gehören zum Alltag – vom mittelständischen Unternehmen bis hin zu kritischen Infrastrukturen. Doch welches Wissen und welche Kompetenzen sind nötig, um Bedrohungen wirksam abzuwehren?

Das **Lernlabor Cybersicherheit** unter dem Dach der Fraunhofer Academy liefert in anwendungsorientierten Weiterbildungen erprobtes Wissen aus aktuellen Forschungsprojekten. So qualifizieren sich Fachkräfte, Teams und Organisationen für die drängendsten Herausforderungen der IT-Sicherheit. Der Verbund aus führenden Fraunhofer-Instituten und ausgewählten Hochschulen überführt wissenschaftliches Know-how direkt in die Praxis. Ob offene Seminare, Inhouse-Trainings oder Intensivformate im Lernlabor: Die Weiterbildungen decken ein breites Themenspektrum ab – von Anwendersicherheit über IT-Forensik bis hin zu Cloud Security und künstlicher Intelligenz (KI). Branchenspezifische Schulungen adressieren u. a. Industrie sowie Energie- und Wasserversorgung. Neu im Portfolio ist das Training „IT-Sicherheitsrichtlinien nutzergerecht gestalten und erfolgreich etablieren".

Besuchen Sie uns auf der it-sa: Halle 6, Stand 6-416!

Fraunhofer ACADEMY

Lernlabor Cybersicherheit

Mehr dazu hier

Fraunhofer Academy Lernlabor Cybersicherheit
Hansastraße 27 c
80686 München
cybersicherheit@fraunhofer.de
www.cybersicherheit.fraunhofer.de

Bild: Arsyifa - stock.adobe.com

it sa EXPO CONGRESS
HOME OF IT SECURITY

Ransomware-Angriffe

WIE UNTERNEHMEN IHRE PRODUKTION TROTZ IT-TOTAL-AUSFALL SICHERN

Bild: Vera - stock.adobe.com

Wenn Ransomware-Angriffe Unternehmen treffen, fällt häufig die gesamte IT-Systemlandschaft für mehrere Wochen aus. Durch die enge Verzahnung der IT mit der Operational Technology (OT) beeinträchtigt das oft auch den Produktionsbetrieb. Eine Analyse der Kernprozesse und die darauf basierenden, gut geplanten Fallback-Maßnahmen sichern den laufenden Betrieb und vermeiden hohe Ausfallkosten.

Cyberangriffe auf produzierende Unternehmen haben in den vergangenen Jahren stark zugenommen. Selbst Ransomware-Angriffe auf die Office-Welt können durch die wachsende Abhängigkeit der OT von der IT-Infrastruktur die Produktion lahmlegen und letztlich in die Insolvenz führen. Steht beispielsweise das Enterprise Resource Planning (ERP) nicht mehr zur Verfügung, kommt es zu erheblichen Einschränkungen in der Produktion, da zentrale Abläufe wie Materialbedarfsplanung, Auftragssteuerung oder Lagerverwaltung ausfallen.

Die Behebung eines Ransomware-Befalls und die Wiederherstellung betroffener Systeme erfordern je nach Komplexität zwischen vier und sechs Wochen. Damit Unternehmen trotz Ransomware-bedingter IT-Ausfälle ihre Produktion aufrechterhalten können, ist eine strukturierte Vorbereitung notwendig.

KERNPROZESSE DEFINIEREN: WAS IST ÜBERLEBENSWICHTIG?

Zu Beginn müssen die Verantwortlichen definieren, was Überlebensfähigkeit für das Unternehmen bedeutet. Hierzu identifizieren sie die minimal überlebensfähigen Kernprozesse, die für den erwartbaren Zeitraum aufrechterhalten werden müssen. Dafür müssen folgende Fragen beantwortet werden:

- Wie hoch muss der Cashflow sein, um eine Insolvenz abzuwenden (etwa 25 Prozent des Regelumsatzes)?
- Welche Top-Kunden sind hierfür mit welchen Produkten zu beliefern?

Daraus leiten sich die Kernprozesse ab, die während einer Krise zwingend weiterlaufen müssen. In der Praxis zeigen sich jedoch häufig Probleme: Prozesse sind nicht sauber definiert oder geschnitten, Verantwortlichkeiten unklar oder gar nicht festgelegt. Eine saubere Dokumentation des gesamten Produktionsprozesses – unterteilt in Subprozesse von Auftragseingang bis zur Lieferung zum Kunden – wäre zwar enorm hilfreich, ist in der Praxis aber nur selten vorhanden.

Pragmatischer ist es daher, zunächst bis zu drei Subprozesse zu skizzieren, etwa die Anlieferung von Rohstoffen, die Produktion und das Warehouse-Management. Diese werden anschließend in Cluster unterteilt, um geeignete Interviewpartner zur Beantwortung von Detailfragen zu identifizieren. Interviews helfen zu verstehen, welchen Beitrag der jeweilige Subprozess leistet. Sind erste Subprozesse so festgehalten, stellt sich im nächsten Schritt die Frage nach den IT-Abhängigkeiten.

IT-ABHÄNGIGKEITEN SYSTEMATISCH ERFASSEN

Die im Prozess involvierten Personen nehmen die Verfügbarkeit von IT-Systemen oft als selbstverständlich hin. Umso wichtiger ist es, einmal den vollständigen Prozessablauf im Tagesgeschehen mit einem kritischen Blick zu begleiten und alle Abhängigkeiten zu dokumentieren. Strukturierte Fragebögen helfen bei der Situationsaufnahme und dienen der späteren Aufarbeitung der Informationen. Konkrete Rückfragen zu IT-Ausfällen zeigen oft die gelebten Ad-hoc-Maßnahmen auf. Ein Fragebogen kann dabei wie in Abbildung 1 aufgebaut sein.

Ist die Prozesskette aufgenommen, lassen sich die Abhängigkeiten zu IT-Systemen ebenfalls in Cluster zusammenfassen. Es bietet sich an, lokal betriebene Systeme (On-Premises) von Cloud-Diensten zu trennen. Zudem sollten die Verantwortlichen für jedes System einen Eigner benennen, der aussagekräftige Informationen zu bereits getroffenen Resilienzmaßnahmen liefern kann – auch wenn die Qualität in der Praxis oft hinter den Erwartungen zurückbleibt.

Cluster	Prozess	Verantwortung	Welche Systeme sind für die Durchführung notwendig?	Welche Inputs sind notwendig und welche Outputs werden erzeugt?	Welche Auswirkungen entstehen, wenn die Systeme nicht zur Verfügung stehen?	Gibt es ein alternatives System auf welches zurückgegriffen werden kann?
Produktion	Anbringung Etikett mit Seriennummern auf Endprodukt	Alan Smithee	Prozessleitsystem SAP Production Planning SAP Material Management	Input: - zusammengebautes Endprodukt - Freigabe der Qualitätssicherung - Seriennummer Output: - Endprodukt mit Seriennummer-Ettiket	Ohne das Prozessleitsystem kann die Produktion nicht durchgeführt werden. Ein manuelles Aufbringen der Etiketten wäre möglich, würde den Prozess aber erheblich verlangsamen. Ohne die SAP-Module können keine fortlaufenden Seriennummern erzeugt werden.	Aktuell existieren keine Ausweichsysteme für das Prozessleitsystem und das zentrale SAP-System.

Abbildung 1: Beispielhafter Fragebogen zur Prozessaufnahme (Bild: rt-solutions.de GmbH)

Mithilfe dieser Informationen lässt sich eine erste Resilienzbewertung der Kernprozesse vornehmen, um den Ist-Stand zu vervollständigen. Als pragmatischer Ansatz bietet sich eine zweiteilige Ampel-Einstufung an:

- **Grün:** Es sind Fallback-Mechanismen vorhanden, sodass der Prozess trotz Ausfall der IT-Systeme mit der erforderlichen Mindestkapazität lauffähig ist.
- **Rot:** Es sind keine oder unzureichende Maßnahmen zur Aufrechterhaltung vorhanden, sodass unsicher ist, ob die erforderliche Mindestkapazität aufrechterhalten werden kann.

Diese Bewertung dient der Priorisierung von Maßnahmen und gibt einen guten Überblick über den aktuellen Stand der Cyberresilienz. Ist sie abgeschlossen, besteht der nächste Schritt darin, ein strukturiertes Vorgehen für den Ransomware-Angriff festzuhalten.

LEITFADEN FÜR DEN ERNSTFALL

Da Ransomware-Angriffe eine hohe Eintrittswahrscheinlichkeit bei gleichzeitig schwerwiegenden Auswirkungen aufweisen, bietet sich dieses Szenario als erstes Playbook an. Weitere Szenarien können die Verantwortlichen später analog behandeln. Ein Playbook ist eine Zusammenfassung strukturierter Anweisungen, um das Szenario zu überstehen. Es besteht aus sieben Kapiteln: Vorbereitung, Erkennung, Eindämmung, Notbetrieb, Kommunikation, Wiederherstellung und Nachbereitung.

Vorbereitung

Im Bereich Vorbereitung sind die Ansprechpartner für die IT-Systeme sowie für die betroffenen Fachbereiche zu hinterlegen, um diese im Notfall schnell informieren zu können. Bei Bedarf sind auch externe Kontakte – etwa Behörden, Berater oder Forensiker – aufzunehmen. Existieren regulatorische Meldepflichten, so bietet es sich an, die einzuhaltenden Zeiträume hier zu dokumentieren.

Erkennung

Dieses Kapitel definiert erwartbare Muster des jeweiligen Szenarios; bei Ransomware beispielsweise ungewöhnliche Dateiverschlüsselungen oder Meldungen zur Forderung eines Lösegelds. Zusätzlich sind hier Meldeketten zur Eskalation festzulegen.

Eindämmung und Notbetrieb

Das Kapitel „Eindämmung" listet Sofortmaßnahmen wie das Isolieren nicht betroffener Systeme oder die Deaktivierung von Remote-Zugängen. Die Prozesskette wird damit in einen Minimalzustand versetzt, der zunächst nicht lauffähig ist. Die anschließende Überführung in den Notbetrieb hält das benötigte Niveau an Produktion aufrecht, damit das Unternehmen überlebensfähig bleibt. Hierbei werden nur die Kernprozesse aufrechterhalten, während alle nicht erforderlichen Abläufe ruhen. Da IT-Systeme nicht zur Verfügung stehen, müssen vorab Strategien und Alternativprozesse mit den Verantwortlichen erarbeitet werden. Hier gibt die Ampel-Einstufung die Priorisierung vor. Prozesse mit grüner Einstufung sind bereits abgedeckt, ein Ausfall im gewählten Szenario ist daher nicht realistisch. Für Prozesse mit roter Einstufung müssen hingegen geeignete Fallback-Mechanismen definiert werden.

Fällt etwa das zentrale SAP-System aus, welches die Seriennummern für die Endmontage eines Produktes liefert, so muss vorab ein Nummernkreis definiert werden, der im Notbetrieb ohne SAP zu verwenden ist. Eine Berechnung der Notproduktionskapazität bei erwartbarem Ausfall von bis zu sechs Wochen ergibt die Anzahl der vorzuhaltenden Nummern. Ein vorbereiteter manueller Ablauf, etwa über ein Kanban-Board auf Papier, führt durch den Prozess und verhindert Fehler. Vorgaben, wo beispielsweise reservierte Seriennummern zu finden sind und wie ihre Verwendung zu dokumentieren ist, um diese nach Wiederherstellung in das SAP zu übertragen, ergänzen das Playbook.

Kommunikation

Wichtig ist, dass alle Fallback-Mechanismen definiert sind, kontrolliert ablaufen und alle involvierten Personen informiert werden. Die hierzu notwendige Kommunikation ist ebenfalls Bestandteil des Playbooks, falls die regulären Kommunikationskanäle wie Telefonanlagen oder Unified Messaging (UM) nicht zur Verfügung stehen. Ausgedruckte Kontaktlisten mit (gegebenenfalls privaten) Mobilfunknummern müssen mindestens vorhanden sein.

Wiederherstellung und Nachbereitung

Die Wiederherstellung beschreibt den Übergang vom Not- zurück in den Regelbetrieb, einschließlich der Überführung aller Zwischenprozesse – etwa Lagerbewegungen oder Rechnungen – in die Normalsysteme. Bei der Nachbereitung können die während des Notbetriebes gewonnenen Lessons Learned im Playbook dokumentiert werden.

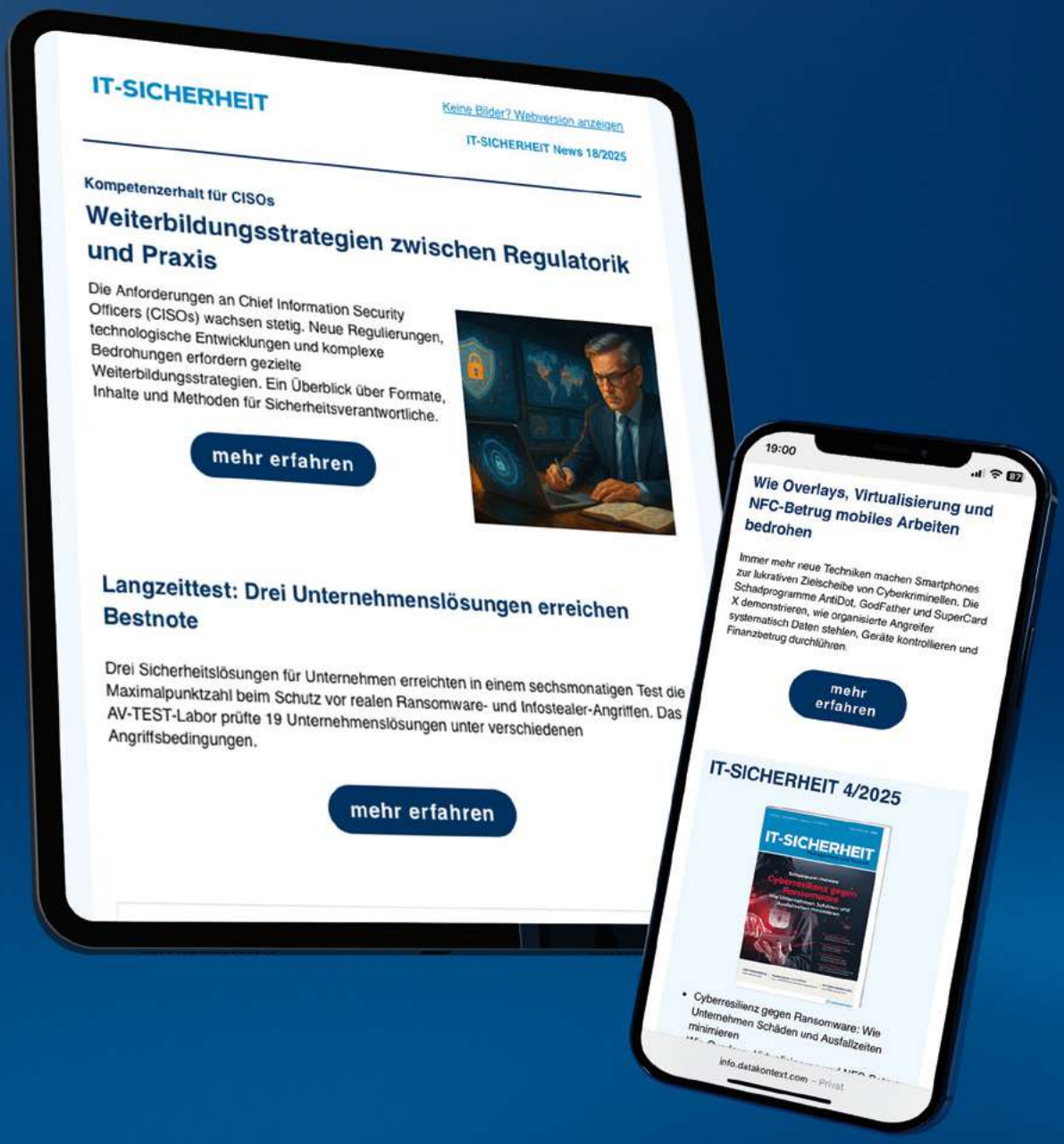
Darüber hinaus sollten Unternehmen das Playbook regelmäßig proben – sei es in Tabletop-Simulationen mit allen Beteiligten oder im Rahmen geplanter IT-Wartungen. Auf diese Weise wird es kontinuierlich verbessert, und die Verantwortlichen sind auf den Ernstfall vorbereitet.

FAZIT

Das Vorgehen am Beispiel eines Ransomware-Angriffs bereitet Unternehmen systematisch auf schwerwiegende Ereignisse vor. Die im Playbook definierten Fallback-Mechanismen lassen sich auch auf weniger gravierende Zwischenfälle übertragen. Werden weitere Prozesse durch Playbooks abgedeckt, steigt die Unabhängigkeit der Produktion – und die Einbußen im Notbetrieb sinken deutlich. ■

JULIUS PAFFRATH
ist IT-Security-Consultant und Datenschutzbeauftragter bei der rt-solutions.de GmbH.

GEORG LUKAS
ist Head of OT Security bei der rt-solutions.de GmbH.



Der Wissensvorsprung im Themengebiet IT-Sicherheit direkt in Ihr Postfach.

Abonnieren Sie jetzt den kostenfreien IT-SICHERHEIT Newsletter: **itsicherheit-online.com/newsletter**

Blackout-Resilienz in der Praxis

RECHENZENTREN RÜSTEN SICH FÜR GROßFLÄCHIGE STROMAUSFÄLLE

Die Abhängigkeit von digitaler Infrastruktur nimmt zu, doch Deutschlands Stromnetze sind überlastet, und Stromausfälle werden wahrscheinlicher. Rechenzentren müssen daher heute deutlich mehr leisten als nur die sichere Speicherung von Daten. „Blackout-Resilienz 2025" bedeutet deshalb, Energiequellen zu diversifizieren, intelligente Speicher einzubinden und Prozesse so zu optimieren, dass selbst bei einem großflächigen Netzausfall kritische Systeme unterbrechungsfrei weiterlaufen.

Kritische IT-Infrastruktur vor großflächigen Stromausfällen zu schützen, ist eine zentrale Voraussetzung für jeden professionellen Rechenzentrumsbetrieb. Angesichts der stetig zunehmenden Abhängigkeit von digitalen Dienstleistungen, verschärfter regulatorischer Anforderungen und der Häufung extremer Wetterereignisse sind heute ganzheitliche Konzepte erforderlich, die deutlich über den klassischen „Dieselgeneratorsatz" hinausgehen. Moderne Resilienzsysteme integrieren dezentrale Energiequellen, intelligente Puffertechnologien, digitales Asset-Management und organisatorische Verfahren in einem orchestrierten Ablauf, dessen Ziel es ist, einen unterbrechungsfreien Betrieb selbst in Szenarien mehrtägiger Netzausfälle zu gewährleisten.

MEHRSCHICHTIGE ENERGIEVERSORGUNG

Das Herzstück moderner Blackout-Resilienz bildet die Mehrfachversorgung über verschiedene Energiequellen. Die klassische Netzeinspeisung über zwei voneinander unabhängige Hochspannungsanschlüsse ist ebenso unverzichtbar wie die zunehmende Integration erneuerbarer Erzeugungsanlagen direkt am Standort. Solaranlagen auf Dachflächen, vertikale Windkraftsysteme auf dem Gelände sowie Biogas-Kleinkraftwerke liefern vor Ort erzeugte Energie, reduzieren Spitzenlasten im öffentlichen Netz und stellen Basisstrom bereit.

Damit diese Energie jederzeit nutzbar bleibt, setzen Betreiber auf modulare Speicher – von Lithium-Ionen-Blöcken über Redox-Flow-Systeme bis zu Schwungradspeichern. So entsteht ein verbundener Energiemix, der nahtlos zwischen Netz, Speicher und Eigenproduktion umschaltet. Während Schwungräder dank ihres hohen Trägheitsmoments sofortige Kurzschlussleistung für Millisekunden bereitstellen, decken Batterien mittelfristige Versorgungslücken ab und ermöglichen so einen unterbrechungsfreien Übergang zu Diesel- oder Brennstoffzellen-Generatoren.

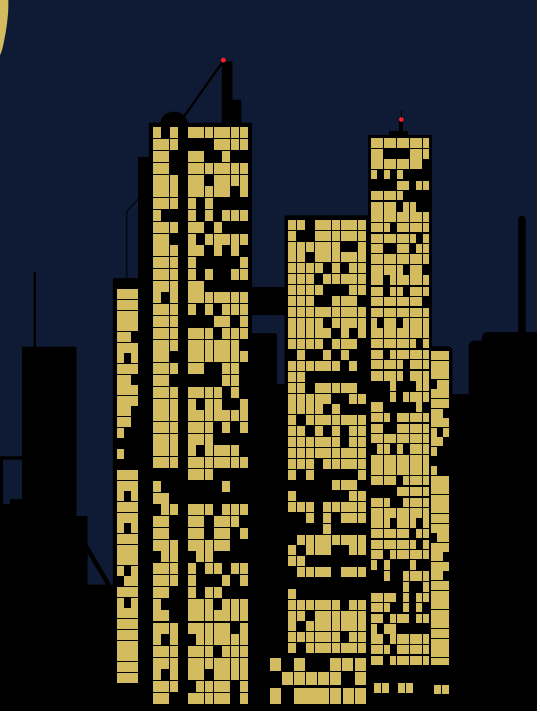
AUTOMATISIERTE NOTSTROMSYSTEME MIT KI-UNTERSTÜTZUNG

Die zweite Absicherungsebene bilden hochautomatisierte Notstromaggregate auf Diesel- und Erdgasbasis. Moderne Notstromaggregate verfügen über automatisierte Startsequenzen, die bei einem Netzausfall innerhalb von fünf Sekunden die Last übernehmen. Eine umfassende Sensorik überwacht dabei Parameter wie Öltemperatur, Abgasdruck, Vibrationen und Kraftstoffqualität.

Diese Daten fließen in KI-gestützte Analytikplattformen, die auf Grundlage historischer Betriebswerte Wartungsintervalle berechnen und Instandhaltungen einleiten, bevor kritische Verschleißgrenzen erreicht sind. So lassen sich Ausfallzeiten reduzieren und die Verfügbarkeit von Aggregateflotten lässt sich auf über 99,9 Prozent steigern.

Parallel dazu gewinnen wasserstoffbetriebene Brennstoffzellen zunehmend an Bedeutung. Aufgrund ihres emissionsarmen Betriebs und ihres leisen, modularisierbaren Aufbaus sind sie eine sinnvolle Ergänzung für Betreiber, die Nachhaltigkeitsziele verfolgen oder in dicht besiedelten Gebieten tätig sind. In Kombination mit einem intelligenten Microgrid-Management koordinieren sie die Eigenproduktion, Batteriespeicher und den Fremdnetzbezug. Im Inselbetrieb,

Bild: fotografiedk - stock.adobe.com



einem automatischen Wechselmodus, der bei Netzausfall greift, versorgen Brennstoffzelle und Speicher gemeinsam kritische Lasten für mehrere Stunden oder Tage. Über OPC-UA-Schnittstellen oder REST-APIs können externe Wartungsdienste nahezu alle Parameter aus der Ferne überwachen und den Betrieb optimieren.

REDUZIERUNG VON RISIKEN

Gleichzeitig nimmt die geografische Diversifikation von Rechenzentren zu. Mithilfe von Software-Defined-Networking und virtualisierten Plattformen wird die Workload-Orchestrierung in Echtzeit gesteuert. Im Fall eines großflächigen Stromausfalls in einer Netzregion verlagern Lastmanager virtuelle Maschinen automatisch zu Standorten mit stabiler Energieversorgung. Rechenzentren in unterschiedlichen Netzausbauregionen – teils sogar in verschiedenen europäischen Ländern – bilden so ein resilientes Netzwerk. Dieses stellt Dienste weltweit ohne Unterbrechung bereit. Die Multisite-Strategie reduziert zudem regulatorische Risiken, da sich unterschiedliche lokale Stromversorgungsmodelle und Stärken nutzen lassen.

Ein weiterer Baustein sind adaptive Kühlkonzepte, die den Energieverbrauch im Notstrombetrieb deutlich senken. Dabei werden klassische Kaltwassersätze mit variabler Drehzahlregelung durch freie Kühlung ergänzt. In kühlen Nächten oder Wintermonaten wird dabei die Außenluft zur Wärmeabfuhr genutzt. Verteilte Flüssigkeitskühlkreisläufe mit Direktverdampfung arbeiten zudem effizienter als luftbasierte Systeme. Sinkt die verfügbare Netzleistung, drosselt die intelligente Steuerung automatisch weniger kritische Verbraucher, verschiebt Rechenjobs in Phasen mit ausreichender Kühlkapazität und vermeidet so thermische Instabilitäten.

SIMULATION VON BLACKOUT-SZENARIEN

Neben der technischen Absicherung ist auch eine gründliche organisatorische Vorbereitung entscheidend. Dazu gehören die Schulung des Personals und die Durchführung strukturierter Notfallübungen. In speziell eingerichteten Command-Centern lassen sich realistische Blackout-Szenarien simulieren – von kurzen Spannungseinbrüchen bis hin zu tagelangen Komplettausfällen. Mithilfe digitaler Zwillinge der gesamten Anlage können Tests verschiedenster Störfälle ohne Risiko für den Live-Betrieb durchgeführt werden.

Die gewonnenen Erkenntnisse fließen direkt in aktualisierte Betriebsanleitungen, Eskalationspfade und Kommunikationsprotokolle ein. Klare Rollenverteilungen und festgelegte Entscheidungsbefugnisse stellen sicher, dass die Abläufe im Ernstfall reibungslos funktionieren.

Darüber hinaus trägt die Einhaltung internationaler Standards wesentlich zur Überprüfbarkeit der Resilienzmaßnahmen bei. Zertifizierungen nach ISO 22301 (Business Continuity Management), ISO 27001 (Informationssicherheit) und IEC 61000-4-34 (Störfestigkeit gegen Spannungsunterbrechungen) liefern externe Validierung. Regelmäßige Audits umfassen sowohl technische Komponenten als auch dokumentierte Prozesse und Warnstufen. Darin festgehaltene Service-Level-Agreements mit Energieversorgern und Treibstoffzulieferern sichern prioritäre Belieferung in Krisensituationen und sollen garantieren, dass Ersatzteile und Verbrauchsmaterial umgehend zur Verfügung stehen.

TRANSPARENZ UND KOOPERATION SIND ENTSCHEIDEND

Ebenso ermöglicht die zunehmende Digitalisierung eine noch feinere Abstimmung aller Elemente. Predictive-Maintenance-Plattformen aggregieren Daten aus Sensoren, Logfiles und Netzmonitoren, werten sie mit Machine-Learning-Algorithmen aus und prognostizieren die Restlebensdauer von Komponenten. Intelligente Lastmanager passen den Energiebezug kontinuierlich an Live-Tarife und Netzbelastungen an. Über blockchainbasierte Services lassen sich Verbrauch und Kapazitäten zwischen Partnern transparent und manipulationssicher handhaben, was den Einstieg in virtuelle Kraftwerke erleichtert.

Eine bewährte Praxis stellt zudem die enge Kooperation mit lokalen Netzbetreibern und Behörden dar. Betreiber von Rechenzentren nehmen an regionalen Blackout-Arbeitsgruppen teil und erhalten frühzeitig Informationen zu geplanten Abschaltungen, Netzhinweisen und Wartungsfenstern. Diese Echtzeitdaten speisen das interne Monitoring und erlauben eine automatisierte Anpassung der Umschaltstrategien. Gemeinsame Notfallpläne mit Feuerwehr, Polizei und technischen Hilfsdiensten beschleunigen die Bereitstellung von Hubschrauber-Landeflächen für Wartungsteams und die Lieferung kritischer Bauteile.

FAZIT

Um gegen Stromausfälle resilient zu sein, ist heute ein abgestimmtes Zusammenspiel aus Technik, Organisation und Partnerschaften erforderlich. Dezentrale Erzeugung, vernetzte Energiespeicher, digitale Zwillinge, KI-gestützte Analytik und sorgfältig erprobte Notfallprotokolle bilden gemeinsam ein hochverfügbares Gesamtsystem. Der Fokus hat sich von punktuellen Backup-Lösungen zu umfassenden, dynamisch anpassbaren Infrastrukturen verschoben. Nur wer alle Komponenten – von der Solarzelle bis zum Wartungsplan – in einen integrierten Ablauf einbindet, kann seinen Kunden auch in einem ernsthaften Blackout-Szenario eine ununterbrochene Versorgung bieten. Diese ganzheitliche Herangehensweise ist entscheidend für die Blackout-Resilienz von Rechenzentren im Jahr 2025 und bildet die Grundlage für zukünftige Innovationen. ■

JEROME EVANS
ist Geschäftsführer der firstcolo GmbH. Seit 20 Jahren befasst er sich mit IT-Dienstleistungen, speziell Datacentern, und kümmert sich um den Aufbau und Betrieb von Rechenzentren.

Gut vorbereitet auf den digitalen Ernstfall

WIE SICH MIT EINEM ISMS SICHERHEITSKULTUR IM UNTERNEHMEN ETABLIEREN LÄSST

Die NIS-2-Richtlinie der EU soll die Cybersicherheit durch erhöhte Vorsichtsmaßnahmen weiter verbessern. Viele mittelständische und kleinere Unternehmen müssen jetzt die Vorgaben umsetzen und fragen sich, wie der Sprung vom Pflichtprogramm zur gelebten Sicherheitsstrategie gelingen kann. Moderne digitale Lösungen zum Aufbau von Informationssicherheits-Managementsystemen (ISMS) unterstützen dabei. Dazu zählen die Entwicklungen des Aachener Softwarehauses ConSense GmbH, die ihren Fokus auf die Praxis richten und dabei den Menschen in den Mittelpunkt stellen.

Daten sind in unserer digitalen Welt ein wertvolles Wirtschaftsgut – und damit heiß begehrt. Das spiegelt sich auch in zunehmenden Cyberangriffen wider: Tagtäglich finden sich Nachrichten von versuchten oder erfolgreichen unbefugten Zugriffen, dem Diebstahl wertvoller Informationen oder Ramsomware-Attacken auf Unternehmensnetzwerke. Diese Taten verursachen nicht nur Ärger und Aufwand, sie haben enorme wirtschaftliche Schäden zur Folge und beeinträchtigen das Image eines Unternehmens. Cyberkriminalität betrifft längst nicht mehr nur große Konzerne, sondern auch zunehmend mittelständische oder kleine Unternehmen. Das Risiko, einem Hackerangriff zum Opfer zu fallen, wird dabei von den Verantwortlichen oft unterschätzt.

IT-SICHERHEIT WIRD ZUR PFLICHT – NICHT NUR FÜR GROßUNTERNEHMEN

Um diesen Gefahren entgegenzuwirken, hat die EU ihre Anforderungen an die Cyberresilienz von Unternehmen mit der 2023 in Kraft getretenen NIS-2-Richtlinie verschärft. Diese muss in Deutschland aktuell in nationales Recht umgesetzt werden und soll voraussichtlich ab Anfang 2026 gelten. Im Gegensatz zum Vorgänger NIS-1 bezieht die Regelung zusätzliche Branchen ein, zum Beispiel Chemie, Industrie/Produktion, Öffentliche Verwaltung, Post- und Kurierdienste sowie weitere. Für Unternehmen aus den betroffenen Branchen gilt sie ab 50 Beschäftigten und nimmt auch Führungskräfte stärker in die Pflicht. Zu deren Aufgaben gehört es künftig, geeignete Organisationsstrukturen zu schaffen, die den Schutz vor Kriminalität aus dem

◀ *Informationssicherheit mit System: Nicht auf Gesetzesvorgaben warten, sondern schon jetzt vorsorgen – das schützt vor wirtschaftlichen Schäden. (Bildquelle: ©Gorodenkoff, AdobeStock & ConSense GmbH)*

Netz erhöhen. Unter anderem müssen sie dafür die notwendigen personellen und finanziellen Ressourcen bereitstellen und für eine laufende Kontrolle sorgen. Damit liegt die Verantwortung für Cybersicherheit in der Führungsetage und nicht mehr allein in der IT-Abteilung. Gleichzeitig erhöht sich auch die Haftung im Schadensfall, wenn die Richtlinie nicht umgesetzt wird.

Es genügt demnach nicht mehr, IT-Sicherheitsmaßnahmen nach bestem Wissen und Gewissen umzusetzen. Die betroffenen Betriebe sind dazu verpflichtet, strukturierte, nachweisbare Prozesse einzuführen. Das bedeutet, dass viele Unternehmen künftig organisatorisch und technisch nachrüsten müssen. Damit stehen sie oft vor einer doppelten Herausforderung, denn vielfach fehlen sowohl Ressourcen als auch Orientierung. Erfahrungen aus der Praxis zeigen: Vor allem kleinere und mittlere Unternehmen tun sich mit der Umsetzung eines ISMS schwer und schrecken häufig vor dem Aufwand, der mit dessen Einführung verbunden ist, zurück. Dabei kann ein ISMS interne Abläufe sogar vereinfachen. Richtig umgesetzt sorgt es dafür, dass Prozesse genau beschrieben, Zuständigkeiten geklärt und Risiken sichtbar gemacht werden. Wenn Mitarbeiter verstehen, welchen Nutzen die Maßnahmen für die Sicherheit der Organisation haben, steigt auch die Akzeptanz.

ISMS ALS STRATEGISCHES WERKZEUG

Ein wirksames Informationssicherheits-Managementsystem ist kein einmaliges Projekt, sondern ein lebendiger Prozess. Er umfasst organisatorische, personelle und technische Maßnahmen – vom Berechtigungskonzept über Notfallpläne bis zur regelmäßigen Bewertung von Risiken – und wird kontinuierlich weiterentwickelt. Das ISMS bietet Unternehmen einen strukturierten Rahmen, um sensible Daten zu schützen, gesetzliche Anforderungen zu erfüllen und das Vertrauen von Geschäftspartnern nachhaltig zu stärken. Als digitale Lösung unterstützt es dabei, regulatorische Anforderungen, die die Sicherheit von Informationen zum Ziel haben (neben der NIS-2 auch ISO 27001, TISAX und weitere), effizient und transparent zu managen.

Bei der Suche nach geeigneten Werkzeugen, die den strukturierten Aufbau eines ISMS unterstützen, stellen sich viele Unternehmen die Frage, inwieweit moderne Softwarelösungen diesen Schritt erleichtern können. Die Antwort darauf fällt in der Praxis eindeutig aus: Der Einsatz einer darauf abgestimmten Software bringt erhebliche Vorteile mit sich, sowohl bei der Einführung als auch im laufenden Betrieb. Die Unterstützung durch eine passende Software reduziert die Komplexität der Aufgabe durch klare Strukturen, eindeutige Zuständigkeiten und automatisierte Abläufe.

Insgesamt sorgt ein digitales System für Nachvollziehbarkeit und vor allem auch für Rechtssicherheit. Die ConSense GmbH, die Software zum Aufbau von Qualitätsmanagementsystemen (QMS) und Integrierten Managementsystemen (IMS) entwickelt, hat die Dynamik rund um Cybersicherheit frühzeitig erkannt. Sie setzt auf Lösungen, mit denen sich akzeptierte und in Unternehmen wirklich gelebte Managementsysteme etablieren lassen, beispielsweise im Bereich der Informationssicherheit. Dr. Alexander Künzer aus der Geschäftsführung der ConSense GmbH erklärt: „Ein ISMS dient dazu, Risiken systematisch zu erkennen, zu bewerten und steuerbar zu machen. Dabei geht es nicht nur um Firewalls und Zugriffsberechtigungen, sondern vor allem um die Frage, wie sich Sicherheitskultur ganzheitlich im Unternehmen verankern lässt."

Strategisches Werkzeug ISMS: Mit organisatorischen, technischen und personellen Maßnahmen zu mehr Cybersicherheit (Bildquelle: ©Gorodenkoff, AdobeStock & ConSense GmbH)

MEHR ALS NUR EINE TECHNISCHE LÖSUNG

Das Aachener Unternehmen hat zu diesem Zweck das Modul ConSense GRC (Governance, Risk & Compliance) entwickelt, das die Basissoftware ergänzt. Es bietet eine geeignete Plattform, um ein ISMS aufzubauen und zu verwalten. Die Softwarelösung verknüpft relevante Normen wie die NIS-2 oder auch die ISO 27001, die Datenschutzgrundverordnung (DSGVO) und weitere mit den im System abgebildeten Strukturen der Organisation.

Ein zentrales Element ist das integrierte Asset-Management, mit dem sich eine vollständige Übersicht aller schutzrelevanten Werte in einem Unternehmen aufbauen lässt, sodass eine fundierte Grundlage für die Risikobewertung entsteht. Mit Features wie einem detaillierten Rollen- und Rechtemanagement sowie dem Maßnahmentracking unterstützt es die Planung, Umsetzung und Kontrolle von Sicherheitsmaßnahmen. Durch integrierte Workflows und automatische Erinnerungsfunktionen wird der Aufwand für Abstimmung und Pflege des Systems deutlich reduziert. Das unterstützt Betriebe dabei, komplexe Zusammenhänge systematisch abzubilden, und verhilft zu mehr Transparenz, Konsistenz und Nachvollziehbarkeit aller Aktivitäten rund um Cybersicherheit.

ConSense zeigt mit der Softwarelösung außerdem, welche Vorteile es hat, ein ISMS nicht isoliert zu sehen, sondern es in ein Integriertes Managementsystem einzubetten. Denn viele Unternehmen verfolgen neben Informationssicherheit auch andere normative Vorgaben, da-

ISMS-Softwarelösung von ConSense: In systematischen Schritten Risiken erkennen, bewerten, steuern – und Sicherheitsvorkehrungen kontinuierlich verbessern (Bildquelle: ConSense GmbH)

runter zu Bereichen wie Qualitätsmanagement, Umwelt-, Arbeitsschutz- und Datenschutzmanagement, Compliance und mehr. Unter dem Dach IMS lassen sich Synergien ausschöpfen: Informationen können bereichsübergreifend genutzt, Verantwortlichkeiten zentral gesteuert und Audits kombiniert werden. Doppelte Arbeit lässt sich auf diese Weise vermeiden. Das Management der verschiedenen Normen und Vorgaben wird transparenter, effizienter und weniger fehleranfällig.

Die Technologie ist allerdings nur ein Teil der Lösung, unterstreicht Dr. Alexander Künzer: „Wir entwickeln Softwarelösungen, die sich nicht nur an den Normen orientieren, sondern auch an den Bedürfnissen der Menschen. Das zeigt sich zum Beispiel in der Anwendung: Die Software strukturiert, dokumentiert und erinnert. Auf diese Weise unterstützt sie Mitarbeitende, die Verantwortung tragen."

ISMS SCHRITTWEISE UND MIT AUGENMAß EINFÜHREN

Erfahrungen von ConSense zeigen, dass kleinere und mittlere Unternehmen vor dem Aufwand, den der Aufbau eines ISMS mit sich bringt, oft erst einmal zurückschrecken. Hier kann der Experte jedoch beruhigen: „Die Einführung eines ISMS ist kein bürokratischer Kraftakt, sondern eine strategische Chance, Informationssicherheit systematisch und wirksam in Unternehmen zu verankern. In klar strukturierten Schritten lässt sich ein robustes Sicherheitsniveau aufbauen, das spürbaren Mehrwert für die Organisation und die Mitarbeitenden erzielt." Nach den Erfahrungen der Aachener Profis hat sich eine schrittweise Einführung in der Praxis bewährt. Dazu hat ConSense typische Projektphasen definiert.

Zu Beginn stehen die initiale Vorbereitung und der Projektstart, in dem ein fachlich versiertes Projektteam unter der Leitung eines ISMS-Verantwortlichen gebildet wird. Eine wichtige Maßnahme besteht darin, Verantwortung zu verankern. Denn wer kein klares Mandat hat, stößt schnell an Grenzen. Der Rückhalt der Geschäftsführung bei der Einführung eines ISMS ist daher entscheidend. Der Projektumfang wird definiert und vom Management mit Ressourcen und einem offiziellen Kick-off unterstützt. Anschließend folgt eine Phase, in der der Kontext der Organisation analysiert wird. Sie umfasst die Identifikation und Bewertung interner und externer Einflussfaktoren, relevanter Stakeholder sowie deren Anforderungen an die Informationssicherheit.

Darauf aufbauend wird ein systematisches Risikomanagement etabliert. Hierzu gehören die Festlegung von Methodik, die Bewertung von Informationswerten und die Ableitung geeigneter Maßnahmen. Im nächsten Schritt wird das ISMS-Rahmenwerk aufgebaut, inklusive Leitlinien, Sicherheitszielen und verbindlicher Richtlinien zu Kernthemen wie Zugriffssteuerung, Incident-Management oder Backup. Die darauffolgende Phase umfasst die Umsetzung technischer und organisatorischer Maßnahmen gemäß den Vorgaben der befolgten Richtlinie (ISO 27001, NIS-2 oder weitere) – von Verschlüsselung über Netzwerksicherheit bis zu Schulungen und Notfallplänen.

Parallel dazu erfolgt eine strukturierte Dokumentation und Nachweisführung sämtlicher ISMS-relevanter Unterlagen und Abläufe. Sobald das ISMS in Betrieb ist, beginnt die Phase der Überwachung, etwa durch vorab definierte Kennzahlen, interne Audits und regelmäßige Management-Reviews. Korrekturmaßnahmen und kontinuierliche Verbesserung sind zentrale Elemente, um Abweichungen zu analysieren, Sicherheitsvorfälle aufzuarbeiten und das ISMS weiterzuentwickeln. Wer sich beispielsweise nach ISO 27001 zertifizieren lassen will, ist nun bereit für die Zertifizierungsvorbereitung, bevor das externe Audit stattfinden kann.

CYBERSECURITY WIRD ZUM WETTBEWERBSVORTEIL

Die Einrichtung eines ISMS ist kein Selbstzweck. Unternehmen, die Sicherheitsprozesse durchdacht aufsetzen, steigern nicht nur ihre Resilienz, sie erhöhen auch ihre Attraktivität als Geschäftspartner, denn viele Branchen – von der Automobilindustrie bis zum Gesundheitswesen – verlangen heute nachvollziehbare Standards entlang der gesamten Lieferkette. Ein softwarebasiertes ISMS wird damit zum strategischen Vorteil.

Von noch mehr Effizienz profitieren Unternehmen, die ihr ISMS in ein Integriertes Managementsystem einbetten. Dr. Alexander Künzer unterstreicht: „Unsere Lösungen zeigen, wie sich regulatorische Anforderungen mit betrieblicher Realität vereinen lassen. So wird aus IT-Sicherheit mehr als nur ein Kontrollinstrument – nämlich ein wirkungsvoller Beitrag zu Qualität, Vertrauen und unternehmerischer Zukunftsfähigkeit." ■

DR. STEPHAN KILLICH,
Geschäftsführung, ConSense GmbH, Aachen

So gelingt Informationssicherheit mit System:

WARUM EIN ISMS IM ZEITALTER VON NIS-2, ISO 27001 & CO. IMMER WICHTIGER WIRD

IT-Sicherheit rückt durch gesetzliche Vorgaben wie die NIS-2-Richtlinie zunehmend in den Fokus. Damit werden zentrale digitale Lösungen für das Management immer gefragter. Im Interview erklärt Harald Lenders, Senior Reklamations- und Incident-Manager beim Aachener Softwareentwickler ConSense GmbH, warum strategische Softwarelösungen wie ConSense ISMS dabei eine zentrale Rolle spielen. Ein Gespräch über Integration statt Insellösungen – und über Cybersicherheit als Haltung, nicht als Projekt.

IT-Sicherheit ist derzeit quer durch alle Branchen ein viel diskutiertes Thema. Was beobachten Sie aktuell bei Ihren Kunden?

Die NIS-2-Richtlinie der EU hat das Thema IT-Sicherheit stärker in den Fokus gerückt. Viele Unternehmen sind inzwischen dafür sensibilisiert, aber verunsichert. Die Wege der Umsetzung erscheinen ihnen diffus, und was konkret gefordert wird, ist den Verantwortlichen nicht immer klar. Viele unterschätzen den Aufwand, aber vor allem auch den Nutzen, den ein systematisch aufgebautes ISMS in digitaler Form bieten kann. Dies gilt insbesondere, wenn eine spezialisierte Lösung wie ConSense GRC eingesetzt wird, die ein ISMS mit allen sicherheitsrelevanten Anforderungen zentral abbildet.

Was raten Sie Unternehmen, die jetzt aktiv werden wollen?

Zuallererst: Nicht abwarten, bis die Richtlinie zum geltenden Gesetz geworden ist. Durch die Neuwahlen hat sich die Umsetzung in nationales Recht zwar verzögert, aber NIS-2 kommt auf jeden Fall. Und die wesentlichen Elemente eines ISMS wie Dokumentation, Verantwortlichkeiten und Risikobewertung lassen sich schon heute mit dem aktuellen Wissensstand aufbauen. Wer systematisch vorsorgt, gerät später nicht in die Defensive, wenn es doch einmal zu einem Vorfall kommt – denn dann muss nachgewiesen werden, wie Risiken bewertet und Maßnahmen umgesetzt wurden.

Die zweite wichtige Empfehlung lautet: Nicht isoliert denken. Ein ISMS funktioniert am besten, wenn es in bestehende Strukturen eingebunden wird, zum Beispiel in ein Integriertes Managementsystem (IMS). Hier kommen Lösungen wie unsere Software ins Spiel, die Informationssicherheit nahtlos in ein übergreifendes IMS integrieren.

Wie unterstützt ConSense bei der Umsetzung?

Wir haben Softwarelösungen entwickelt, die komplexe Anforderungen greifbar machen. Unser GRC-Modul, das die ConSense Basissoftwarelösungen ergänzt, verknüpft alle sicherheitsrelevanten Elemente – von der Asset-Analyse bis zur Risikobewertung. Unternehmen behalten den Überblick, wissen, wo sie stehen, und können Maßnahmen gezielt planen und steuern.

Was unterscheidet Ihre Lösungen von anderen?

Wir denken aus der Sicht unserer Anwenderinnen und Anwender: Unsere Softwarelösungen sollen dabei unterstützen, Normen zu erfüllen, und dabei einfach, intuitiv nutzbar und selbsterklärend sein. Sie helfen dabei, zu strukturieren und zu vereinfachen, etwa durch Funktionen wie das Asset-Management oder die zentrale Verwaltung aller Nachweisdokumente. Ziel ist es, unseren Kunden den Arbeitsalltag sicherer zu gestalten, ohne dabei Prozesse unnötig zu verkomplizieren und zu verlangsamen.

Sie setzen demnach auf Integration statt auf Insellösungen?

Ganz genau, unsere Stärke liegt in der Verbindung. Wir ermöglichen, dass Unternehmen nicht nur Informationssicherheit abbilden, sondern sie als Teil ihres Managementsystems wirklich leben. Eine geeignete Software wie unsere ist nicht nur ein Werkzeug, sondern ein strategisches Instrument für eine strukturierte, effiziente und auditierbare Informationssicherheit. Im Zusammenspiel mit weiteren Managementsystemen wird sie zum zentralen Baustein eines ganzheitlichen Compliance- und Risikomanagements.

Was wünschen Sie sich für die Zukunft dieses Themas?

Mit unseren Erfahrungen aus der Praxis wünschen wir uns bei ConSense mehr Bewusstsein dafür, dass Cybersicherheit kein Projekt, sondern eine Haltung ist. Und dass es hier nicht nur um Technik geht. Am Ende machen Menschen den Unterschied aus – in der Umsetzung, in der Verantwortung und im Umgang mit Risiken. Darauf richten wir mit unseren Softwarelösungen unseren Fokus. ■

(Bildquelle: ©MD NAZMUL, AdobeStock & ConSense GmbH

Von der Norm zur Wirkung (2):
Sicherheit beginnt mit Governance –
wie drei Regelwerke Führung, KPIs und
Automatisierung verbinden

VERTRAUEN SCHAFFEN DURCH STRUKTUR

Regulatorische Vorgaben nehmen zu, doch Regeln allein schaffen keine Sicherheit. Wer sie lediglich „abarbeitet“, erstickt in Detailarbeit. Wer sie dagegen als gestaltbare Struktur versteht, gewinnt Transparenz, Geschwindigkeit und Vertrauen – intern wie extern. Dieser Artikel zeigt, wie Normen und Richtlinien von ISO bis NIS-2 zu einem gemeinsamen Führungs- und Steuerungsinstrument werden können – mit bis zu 60 Prozent weniger Implementierungsaufwand. ISO 27001 liefert das Betriebssystem, NIS-2 schärft die Führungsverantwortung, und SOC-2 stärkt das Kundenvertrauen.

Cyberresilienz ist heute nicht nur ein IT-Thema oder eine Toolfrage, als vielmehr ein Zeichen von Führung. Unternehmen stehen verstärkt im Fokus europäischer Regulierung: die Network and Information Security Directive 2 (NIS-2) verschärft die Anforderungen an Governance und Meldepflichten, System and Organization Controls 2 (SOC-2) rückt das Vertrauen von Kunden in den Vordergrund, und ISO 27001 definiert einen internationalen Standard für Informationssicherheit. Gleichzeitig wächst der Druck durch eine kaum beherrschbare Flut an Vorschriften und Anforderungen – mit entsprechenden Haftungsrisiken für die Führungsebene.

Viele Organisationen reagieren darauf noch immer mit Insellösungen und reaktiver Dokumentation. Das Ergebnis: hoher Aufwand, wenig Wirkung. Wer dagegen Struktur, Prozesse und Verantwortlichkeiten klar definiert und digital unterstützt, kann regulatorische Anforderungen nicht nur erfüllen, sondern damit auch eine echte Wirkung auf die eigene Wertschöpfung erzielen – weil jeder im Unternehmen versteht, wie Standards und gesetzliche Vorgaben ineinandergreifen und sich dadurch auf die Kernprozesse konzentrieren kann. Vertrauen entsteht so nicht nur bei Kunden, Aufsichtsbehörden und im eigenen Management, sondern auch im operativen Geschäft.

Die Geschäftsleitung verantwortet Ziele, Risikomaßnahmen und Wirksamkeit. Der ISO-27001-Standard gibt die Struktur vor, NIS-2 konkretisiert Governance-Pflichten und behördliche Durchgriffsrechte. Wirkung entsteht erst durch prozess- und risikobasierte Umsetzung, deren Nachweise im Arbeitsfluss anfallen (Evidence-by-Design).

MESSBARE EFFIZIENZGEWINNE DURCH STRUKTUR

Regulierung wird häufig als Belastung empfunden – tatsächlich eröffnet sie aber die Chance, Transparenz und Effizienz messbar zu steigern. Unsere Erfahrungswerte aus mittelständischen Umsetzungen, basierend auf System-Logs und Workflow-Metriken, zeigen unter anderem:

- 30 bis 60 Prozent weniger Audit-Vorbereitungszeit (Evidenz automatisch aggregiert)
- 25 bis 40 Prozent geringere Durchlaufzeit für Maßnahmen (klare Owner, Eskalationen)
- 15 bis 25 Prozent schnellere Störungsbehebung (Mean Time to Recovery, MTTR) durch Key-Performance-Indicator-(KPI)-gesteuerte Playbooks

Effizienzgewinne sind also möglich – doch wie lassen sie sich dauerhaft sichern? Die Antwort liegt in einer gemeinsamen Struktur. Diese liefert die ISO 27001. Die Fassung aus 2022 bündelt 93 Controls in vier Themen: Organisational, People, Physical, Technological. Das schafft Anschlussfähigkeit an NIS-2, SOC-2 und sektorale Regeln, zum Beispiel an den Digital Operational Resilience Act (DORA) (siehe Tabelle 1). Der ISO-27002:2022-Standard liefert dazu die notwendigen Umsetzungshinweise. Weitere Rahmenwerke und Regelwerke bauen auf dieser Basis auf und lassen sich somit integrativ umsetzen (siehe Tabelle 2).

Ebene	ISO 27001 (2022)	SOC-2 (Trust Services Criteria)	NIS-2 (2022/2555)
Zweck	Aufbau und Betrieb eines Informationssicherheits-Managementsystems (ISMS)	Nachweis von Kontrollen gegenüber Kunden und Partnern	Cyberresilienz und Governance für wesentliche Einrichtungen
Scope	Organisation, Prozesse, Assets, Lieferkette	Dienste, Systeme oder gesamte Organisation	Betreiber kritischer und wesentlicher Dienste in der EU
Nachweis	Annex-A-Kontrollen, internes und externes Audit	SOC-2 Typ I/II Bericht mit unabhängiger Auditor-Opinion	Managementsystem, KPIs, Berichte an Behörden
Fokus	systematisches Risikomanagement und kontinuierliche Verbesserung	Vertrauen und Transparenz in Serviceleistung	C-Level-Verantwortung, Meldepflichten, Sanktionen
Taktung	Re-Zertifizierung alle drei Jahre, jährliche Überwachungsaudits	jährlicher SOC-2-Report (Typ II über 12 Monate)	laufende Compliance, regelmäßige Behördenprüfungen

Tabelle 1: Vergleich der zentralen Regelwerke – Zweck, Umfang und Nachweisverpflichtungen im Überblick

Bild: ChatGPT Image

Norm/Richtlinie	Relevanz für Governance	Hinweis
ISO 27001:2022	ISMS Grundstruktur und Annex A Controls	Harmonized Structure
ISO 27002:2022	Control Guidance und Implementation Ideas	Detailtiefe
SOC-2 (AICPA TSP 100)	Kundenvertrauen und Due Diligence	Attestation Bericht
EU NIS-2	Mindestanforderung an Cyberresilienz und Meldepflichten	Vorstand Verantwortung
ISO 22301	Business Continuity Synergie	Notfallplanung
CIS Controls v8	technische Benchmarks	Quick Wins

Tabelle 2: Ergänzende Normen und Richtlinien – Governance-Relevanz und praktische Anwendungshinweise

Ergänzend konkretisiert die Durchführungsverordnung (EU) 2024/2690 die technischen und methodischen Anforderungen der NIS-2-Risikomaßnahmen. Die European Union Agency for Cybersecurity (ENISA) liefert seit Juni 2025 hierfür einen technischen Implementierungsleitfaden inklusive Mapping-Tabellen (Evidence-Beispiele und Schwellen).

PROCESS FIRST: DER ROTE FADEN IN FÜNF SCHRITTEN

Regulatorik wirkt oft abstrakt – doch sie entfaltet ihre Wirkung erst dann, wenn sie konsequent in die alltäglichen Prozesse übersetzt wird. Ein „Process First"-Ansatz verbindet Geschäftslogik, Risiko, Kontrollen, Evidenz und Kennzahlen zu einem roten Faden, der sich durch das gesamte Unternehmen zieht. Anhand von fünf Schritten lässt sich nachvollziehen, wie Organisationen Struktur und Wirksamkeit methodisch aufbauen können.

1. Prozessinventar und Informationsflüsse

Der erste Schritt besteht darin, die Wertschöpfung sichtbar zu machen. Dazu kartieren die Verantwortlichen End-to-End-Prozesse wie Lead-to-Cash, Procure-to-Pay oder Incident-to-Resolution. Innerhalb dieser Abläufe gilt es, die sogenannten „Kronjuwelen" zu identifizieren – also die Daten und Assets, die für den Geschäftserfolg kritisch sind, etwa Patienten-, Konstruktions- oder Zahlungsdaten. Für jedes Informationsobjekt wird der Schutzbedarf nach Vertraulichkeit, Integrität und Verfügbarkeit (Skala von 1 bis 5) festgelegt. Anschließend lassen sich Informationsflüsse über Systeme, Schnittstellen und Lieferketten hinweg nachzeichnen.

So entsteht ein Katalog von Prozessen, Daten und Flüssen, der nicht nur die IT, sondern das Geschäft in den Mittelpunkt stellt. Typische Artefakte sind Prozesslandkarten, Datenkataloge und Schutzbedarfsprofile. Die Qualität lässt sich messen – etwa über den Abdeckungsgrad dokumentierter Prozesse oder die Aktualität des Asset-Katasters.

Beispiel: Im Prozess Order-to-Cash werden Kunden- und Zahlungsdaten im Customer Relationship Management (CRM) und Enterprise Resource Planning (ERP) verarbeitet. Der Schutzbedarf liegt bei C/I/A = 4/4/5. Kritische Schnittstellen sind der Webshop, das Payment-Gateway und das ERP.

2. Risiko Modell nach ISO-Logik

Sobald Prozesse und Informationsflüsse klar sind, stellt sich die Frage: Wo muss man zuerst handeln? Hier hilft ein standardisiertes Risikomodell nach ISO-Logik. Für jeden Prozess oder Datenfluss werden Szenarien formuliert, die Bedrohung, Schwachstelle und mögliche Auswirkungen kombinieren.

Die Verantwortlichen bewerten dies nach Eintrittswahrscheinlichkeit und Auswirkung – beispielsweise jeweils auf einer Skala von 1 bis 5. Multipliziert ergibt sich ein Risikowert von 1 bis 25, ergänzt um definierte Toleranzen und die Risikobereitschaft des Unternehmens. Entscheidend ist die Verknüpfung mit Geschäftskennzahlen wie Umsatz pro Stunde, Vertragsstrafen oder regulatorische Konsequenzen – so wird Risiko ökonomisch priorisiert.

Beispiel: Der Ausfall des Payment-Gateways hätte eine Wahrscheinlichkeit von 3 und eine Auswirkung von 5. Das ergibt einen Wert von 15 (rot) und erfordert sofortige Maßnahmen sowie ein Management-Review.

3. Controls-Library (Mapping)

Im dritten Schritt bauen Organisationen einen konsistenten Maßnahmenkatalog auf. Statt Normtexte isoliert in Dokumente zu übertragen, dient die ISO 27001 als Master-Register. Die einzelnen Controls werden um Mappings zu NIS-2 und SOC-2 ergänzt, sodass ein gemeinsames Register entsteht.

Jede Control erhält einen Steckbrief mit Ziel, Scope, Owner, Evidenzquelle, Schwellenwerten und Prüffrequenz. Der Status (implementiert, in Arbeit, geplant) sowie die Wirksamkeit (ausreichend, vorhanden, nicht wirksam) werden kontinuierlich verfolgt. Auf diese Weise entsteht ein System, das nicht nur prüfbar, sondern auch steuerbar ist.

Beispiel: Das Zugriffsmanagement wird in ISO 27001 (A.5/A.8), NIS-2 (Art. 21(2)a) und SOC-2 (CC6.x) adressiert. Evidenz liefern Identity-Logs, Genehmigungsworkflows und Rezertifizierungsprotokolle.

4. Evidence-Pipelines

Ein zentrales Prinzip lautet: Audit-Ready by Design. Nachweise sollten im Arbeitsfluss anfallen, nicht erst kurz vor einer Prüfung. Dafür definieren und erfassen Unternehmen Evidenzquellen wie Tickets, Logs, Konfigurationen oder Schulungsnachweise. APIs, Hash-Verfahren und

Zeitstempel sorgen für Integrität und Nachvollziehbarkeit – und das unabhängig vom jeweiligen Stadium.

Die Nachweise werden in einem Evidence-Hub kuratiert, mit Metadaten versehen und such- sowie reportfähig gemacht. So können Auditoren selbst zugreifen, ohne dass die Teams hektisch Dokumente zusammensuchen müssen.

Beispiel: Im Patch-Management bündelt der Hub automatisch die Genehmigungs-Workflows, Baselines, Logs und Scan-Reports zu einem Change-Vorgang – inklusive Chain of Custody.

5. KPI-/Review-Taktung mit Eskalation

Damit das System nicht statisch bleibt, braucht es klare Kennzahlen und feste Review-Zyklen. Verantwortliche definieren ein Set aus Governance-, Risiko- und Prozess-KPIs, die in Heatmaps oder Ampel-Scores visualisiert werden. Monatliche Kurz-Reviews zeigen Abweichungen und Fortschritte, quartalsweise Management-Reviews beleuchten Top-Risiken, Budgetentscheidungen und die Wirksamkeit des ISMS. On-Demand-Reviews greifen bei Vorfällen.

Wichtig ist, dass Kennzahlen Entscheidungswirkung entfalten: Abweichungen müssen Maßnahmen nach sich ziehen, für die jeweils ein Owner, eine Frist und ein Eskalationspfad definiert sind.

Beispiel: Für die Mean Time to Detect (MTTD) und die Mean Time to Recovery (MTTR) gilt ein Ziel von 24 Stunden. Wird dieses eingehalten, bleibt der Status grün – und es sind keine Maßnahmen erforderlich. Liegt die Dauer zwischen 24 und 36 Stunden, wird der Status gelb und der Team-Lead informiert. Bei einer Überschreitung von 36 Stunden wechselt der Status auf rot, was eine C-Level-Eskalation und ein Post-Incident-Review auslöst.

ROLLENVERTEILUNG: VOM VORSTAND BIS ZUR FACHABTEILUNG

Regulatorik wird erst wirksam, wenn sie konkrete Rollen und Verantwortlichkeiten adressiert. ISO 27001, SOC-2 und NIS-2 fordern nicht nur Strukturen, sondern auch klare Zuweisungen: Wer trägt Verantwortung, wer steuert die Umsetzung, wer liefert Nachweise? Die folgenden drei Perspektiven zeigen, wie sich Aufgaben und Pflichten vom Vorstand bis in die Fachabteilungen übersetzen lassen.

1. Geschäftsführung/Vorstand

Für die Unternehmensleitung ist Cyberresilienz keine delegierbare Aufgabe mehr. NIS-2 verpflichtet Vorstände und Geschäftsführer ausdrücklich, Sicherheitsmaßnahmen zu genehmigen, deren Umsetzung zu überwachen und sich regelmäßig schulen zu lassen. Haftung und Sanktionen bei Verstößen stellen klar: Sicherheit ist eine Frage der Governance, nicht nur der Technik!

Quartalsweise treffen Vorstände Entscheidungen über die Risikobereitschaft, Budgets und die Wirksamkeit zentraler Maßnahmen. Ein Governance-Dashboard liefert dafür verdichtete Kennzahlen: Welche Risiken sind im Trend, wie aktuell und vollständig ist die Evidenzbasis, wo liegen Abweichungen bei Kontrollen oder Lieferanten? Diese Zahlen sollen nicht zur Folien-Dekoration verkommen, sondern zu klaren Beschlüssen führen – „ausreichend", „nachschärfen" oder „eskalieren".

Typische Stolperfallen sind reine KPI-Präsentationen ohne Konsequenzen oder Tool-Käufe ohne nachvollziehbaren Nutzen. Gegensteuern lässt sich, indem jede Abweichung automatisch ein Maßnahmen-Ticket auslöst und Investitionen an einem Business-Case pro Control-Cluster gemessen werden.

2. CISO/Compliance Lead

Der Chief Information Security Officer (CISO) oder Compliance-Lead ist der methodische Treiber des Systems. Er sorgt dafür, dass Risiken systematisch bewertet, Kontrollen konsistent dokumentiert und Nachweise zuverlässig gesammelt werden. NIS-2 fordert dabei ausdrücklich die Berücksichtigung der Lieferkette; ISO 27001 verlangt interne Audits und regelmäßige Performance-Bewertungen.

In der Praxis bedeutet das: Der CISO pflegt eine Controls-Library auf Basis von ISO 27001 und ergänzt sie um NIS-2- und SOC-2-Bezüge. Er führt das Risikoregister und sorgt dafür, dass Kennzahlen nicht nur technisch, sondern auch im Lichte der Geschäftsziele interpretiert werden. Über Evidence-Pipelines stellt er sicher, dass Nachweise aus Tickets, Logs oder Konfigurationsänderungen automatisch versioniert vorliegen – auditbereit ohne Last-Minute-Sammlungen.

Regelroutinen wie wöchentliche Risiko-Sichtungen, monatliche Control Reviews und quartalsweise interne Audits schaffen einen Rhythmus, der das System lebendig hält. Die größte Gefahr liegt in einem „Papier-ISMS", das ohne echte Evidenz betrieben wird, oder in einem Übermaß an Kennzahlen, die niemand mehr nutzt. Darum gilt: maximal zehn Kern-KPIs, alles Weitere als Detailbericht.

3. Fachabteilungen/Ops Teams

Für Fachbereiche und operative Teams (Ops-Teams) heißt Sicherheit vor allem: klar definierte Aufgaben, schneller Nachweis, minimale Zusatzlast. Sie liefern Logs und Events, verifizieren Incidents oder Changes im 1-Click-Workflow und dokumentieren Prozessänderungen über Change-Tickets. Evidenz entsteht direkt an der Quelle – durch Checklisten, Abnahmeprotokolle oder Konfigurations-Baselines.

Kennzahlen wie die Service-Level-Agreement-(SLA)-Trefferquote bei Maßnahmen, die First-Time-Fix-Rate oder der Rückgang wiederkehrender Fehler machen Fortschritte sichtbar. Unterstützt werden die Teams durch kontextsensitive Checklisten, Microlearnings und standardisierte Playbooks, die manuelle Ticketarbeit reduzieren.

Fallstricke entstehen, wenn IT-Sicherheit als zusätzliche Arbeit empfunden wird. Das lässt sich vermeiden, indem Sicherheitsaufgaben in die bestehenden Arbeitsabläufe integriert werden – mit klarer „Definition of Done", die auch die Evidenz einschließt. Ebenso wichtig: Ereignisse müssen mit Kontext angereichert werden, etwa durch Ticket- oder Asset-Referenzen, damit sie für Audits nachvollziehbar bleiben.

Alle drei Ebenen – Vorstand, CISO und Fachabteilungen – tragen Verantwortung für Cyber-Resilienz. Tabelle 3 und die Mini-Checkliste (siehe Kasten) zeigen, welche Aufgaben die drei Ebenen konkret übernehmen und welche Belege dafür mindestens erforderlich sind.

HEALTHCARE-PROVIDER MIT 750 MITARBEITERN

Wie diese Prinzipien in der Realität greifen können, zeigt ein Praxisbeispiel: Ein mittelständischer Healthcare-Dienstleister stand vor der Aufgabe, gleichzeitig die Anforderungen aus ISO 27001, SOC-2 und NIS-2 zu erfüllen. Anstatt

Aktivität	Vorstand	CISO/Compliance	Process Owner	Control Owner	Evidence Steward
Risk-Appetite/Toleranzen festlegen	A/R	C	C	I	I
Controls-Library und Mapping pflegen	I	A/R	C	R	C
Evidenz-Pipelines betreiben	I	A/R	C	C	R
Management-Review (Cl. 9.3)	A/R	R (Vorlage)	C	C	C
Meldungen nach Art. 23	I	A/R (Prozess)	C	C	R (Nachweise)

Tabelle 3: Rollen und Verantwortlichkeiten (RACI-Kurzbild) – Legende: Accountable (A), Responsible (R), Consulted (C), Informed (I)

MINI-CHECKLISTE JE ROLLE (MINIMAL VIABLE EVIDENCE)

- ✓ *Vorstand: Beschlussprotokolle (Risk-Appetite, Maßnahmen, Budget), Schulungsnachweis gem. NIS 2 Art. 20(2).*
- ✓ *CISO/Compliance: aktuelles Controls-Register (Owner, Frequenz, Evidenz), Risikobericht (Top-3 + Trend), Melderegeln Art. 23.*
- ✓ *Ops-Teams: verknüpfte Change/Incident-Tickets mit Log-/Konfig-Evidenz, Checklisten-Abnahmen.*

drei getrennte Projekte aufzusetzen, entschied sich das Unternehmen für einen integrierten Ansatz: Es bündelte alle Maßnahmen in einem einzigen Controls-Register.

Bereits in den ersten beiden Wochen erfolgte der technische und organisatorische Aufbau: Das Team importierte die Library in ein GRC-Tool, ordnete Rollen und Verantwortlichkeiten zu und stellte die Verbindung zum Security Information and Event Management (SIEM) her. Damit war die Grundlage gelegt, dass Prozesse, Kontrollen und Nachweise aus einer Quelle gesteuert werden konnten.

In den folgenden Wochen richtete das Team die Data-Pipelines ein. Klinische Anwendungen und Firewalls lieferten kontinuierlich Log-Streams, die mithilfe von KI-basierten Parsern automatisch klassifiziert wurden. So entstanden aus reinen Datenflüssen direkt verwertbare Evidenzen, die dem Controls-Register zugeordnet waren.

Ab Woche sieben stand der Evidence-Hub im Mittelpunkt. Sämtliche Audit-Artefakte – von Richtliniendokumenten über Reports bis zu System-Logs – wurden dort automatisiert versioniert und mit Hashwerten signiert. Damit war jede Änderung nachvollziehbar, und die Beweiskette blieb lückenlos dokumentiert.

Zum Abschluss, nach rund zwölf Wochen, zeigte sich der praktische Nutzen: Der CISO konnte mit wenigen Klicks den geforderten NIS-2-Report erstellen. Innerhalb von Sekunden lag ein vollständiges Archiv mit KPIs, Richtlinien und Event-Nachweisen vor – ein Audit-Ready-Paket, das nicht nur die Aufsichtsbehörde, sondern auch das Management überzeugte.

Das Ergebnis war bemerkenswert: über 60 Prozent weniger Vorbereitungsaufwand für Audits, keine schwerwiegenden Abweichungen (Major Non-Conformities) beim Erst-Audit und eine deutlich verbesserte Transparenz für den Vorstand, der nun regelmäßig einen Ampel-Score zur Governance-Situation erhielt.

GOVERNANCE-HEALTH

Zielbild: *Der Vorstand sieht monatlich Top-3-Risiken, Ampel-Score, Evidenz-Status (Aktualität/Qualität).*

So geht's: *Prozessrisiken (ISO 27001) auf NIS-2-Maßnahmen mappen; Evidenz-Artefakte (Workflows, Logs, Doks) automatisch versionieren; Review-Kadenzen und Eskalation festlegen.*

Effekt: *schnellere Entscheidungen, adressierte Haftung, Audit-Readiness als Nebenprodukt*

FAZIT

Die Erfahrungen zeigen: Wirksame Governance entsteht nicht durch die Ansammlung einzelner Tools, sondern durch eine klare Struktur und die konsequente Verknüpfung mit Prozessen und Risiken. Gerade die ISO 27001 bietet hier die Integrationsschiene, an die sich weitere Regelwerke wie NIS-2, SOC-2 oder auch DORA und der Cyber Resilience Act (CRA) nahtlos anschließen lassen.

Ein zentrales Prinzip lautet, Evidenz im Fluss zu erzeugen: Nachweise entstehen dort, wo Arbeit passiert – im Ticket, im Log oder in der Konfigu-

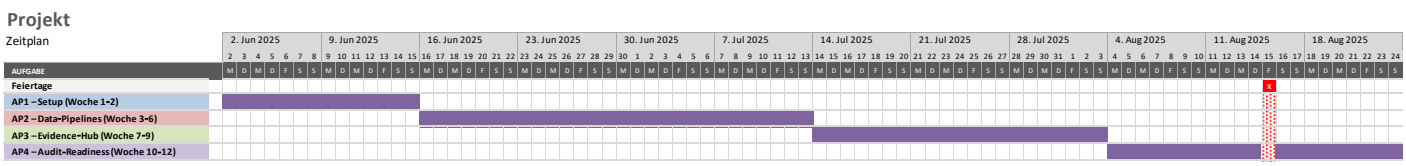


Abbildung 1: GANTT-Diagramm zum Healthcare-Beispielprojekt (Bild: SECaaS.IT)

ration. So wird Auditfähigkeit nicht nachträglich erzwungen, sondern automatisch mitgeliefert. Ebenso wichtig sind die Verankerung von KPIs und Reviews. Sie machen Wirksamkeit messbar und übersetzen den Plan-Do-Check-Act-(PDCA)-Zyklus in den Alltag. Nur wer Abweichungen regelmäßig diskutiert und Entscheidungen trifft, schafft echte Steuerung.

Ein nachhaltiges Governance-System sollte außerdem vendor-neutral und API-first sein, also herstellerunabhängig und mit offenen Schnittstellen gestaltet werden. Es ist damit revisionssicher, skalierbar und offen für zukünftige Anforderungen – unabhängig davon, welche Plattform oder welcher Regulator zukünftig hinzukommt.

Struktur und klare Verantwortlichkeiten sind jedoch nur die Grundlage, um Vertrauen zu schaffen. Ohne einen systematischen Umgang mit Risiken bleibt selbst das beste Governance-System unvollständig. Der nächste Schritt besteht darin, Intuition und Bauchgefühl mit Methode zu verbinden. Im nächsten Artikel unserer Serie, „Ohne Risikokompass bleibt jede Kontrolle blind", zeigen wir, wie Risikomanagement nach ISO 31000 funktioniert, welche Rolle Kennzahlen dabei spielen und warum erst die Verbindung von Strategie und operativer Steuerung echte Resilienz schafft. ■

Literatur

[1] ISO (2022): ISO 27001:2022 – Information Security Management Systems – Requirements. Geneva: ISO.

[2] AICPA (2017): Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Durham: AICPA.

[3] EU (2022): Directive (EU) 2022/2555 – NIS 2. Official Journal of the European Union.

[4] ENISA (2024): Threat Landscape for Health Sector. Athens: ENISA.

[5] Gartner (2023): Market Guide for Integrated Risk Management. Stamford.

[6] NIST (2023): Special Publication 800 218: Secure Software Development Framework. Gaithersburg: NIST.

[7] ISO (2022): ISO/IEC 27002:2022 – Information security controls. (Überblick & Katalog)

[8] BSI Group (2022): ISO 27002:2022 – Information security controls update (Überblick 93 Controls/4 Themen).

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.***

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.

Jeder Beitrag entwickelt praxisnahe Lösungsansätze und zeigt, wie diese in Rollen, Abläufen und Kennzahlen

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.

JÖRG SPÖCKER,
Rechtsanwalt und Geschäftsführer der SECaaS.IT, ist Experte für IT-Sicherheit, IT-Governance und Datenschutz mit internationaler Projekterfahrung. Er verbindet juristisches Wissen mit technischer Expertise.

Strategieentwicklung für Cybersicherheit

VIER HEBEL FÜR DIGITALE RESILIENZ

Vielerorts behandeln Organisationen Cybersicherheit noch immer als rein technisches Problem. Sie gilt als Aufgabe der IT und nicht als strategisches Thema für die Unternehmensleitung. Dabei zeigen die skandinavischen Länder, dass ein anderer Umgang möglich ist: Dort wird Informationssicherheit längst als Führungsaufgabe verstanden und in Prozesse, Technologien und Kultur integriert. Auch deutsche Unternehmen müssen jetzt umdenken und sich auf vier zentrale Handlungsfelder konzentrieren.

Im April 2025 traf ein schwerer Cybervorfall den britischen Handelskonzern Marks & Spencer (M&S). Über eine kompromittierte Drittanbieter-Schnittstelle griffen Angreifer Kundendaten ab, hebelten Kassensysteme aus, und der Onlineshop blieb für mehrere Wochen offline. Der geschätzte Schaden beläuft sich auf rund 350 Millionen Euro. Zusätzlich sah sich M&S mit einer Sammelklage in Schottland konfrontiert. Der Reputationsschaden war enorm, das Kundenvertrauen schwer erschüttert.

Cyberrisiken betreffen also längst nicht mehr nur Serverräume, sie bedrohen ganze Geschäftsmodelle. Ob Lieferkette, Verkaufsprozesse oder Kundenkommunikation: Eine erfolgreiche Attacke kann jedes Glied digitaler Wertschöpfungsketten destabilisieren. Besonders betroffen sind mittelständische und große Industrieunternehmen mit komplexen, oft fragmentierten digitalen Infrastrukturen.

Hinzu kommt: Firmen sehen sich mit einer exponentiell wachsenden Datenflut konfrontiert. Laut IDC wurden 2024 weltweit rund 150 Zettabyte an Daten erzeugt – bis 2035 könnte diese Menge auf mehr als 600 Zettabyte anwachsen.

Eine fast unvorstellbare Datenmenge. Zum Vergleich: Wenn man alle jemals gedruckten Bücher digitalisieren würde, bräuchte man etwa 50 Terabyte Speicherplatz. Ein Zettabyte wären dann ungefähr der Speicherbedarf von 20 Millionen „Weltbibliotheken".

In dieser Realität entstehen neue Risiken: Je mehr Daten Betriebe speichern, verarbeiten und übertragen, desto mehr Angriffsflächen gibt es – und desto dringlicher wird der Schutz. Doch wer Daten nur als Bedrohung sieht, übersieht das Potenzial: Strategisch eingesetzt, können sie Geschäftsmodelle transformieren – vorausgesetzt, sie werden strukturiert gesichert und intelligent genutzt.

Das Beispiel M&S und die exponentiell wachsende Datenflut verdeutlichen, wie dringend ein Umdenken erforderlich ist: Cybersicherheit muss als unternehmensweite Führungsaufgabe verankert werden – nicht reaktiv, sondern strategisch. Damit das gelingt, braucht es klare Prioritäten. Vier Handlungsfelder sind dabei

Bild: Fazla - stock.adobe.com

entscheidend, wenn Unternehmen ihre digitale Widerstandskraft nachhaltig stärken wollen:

1. DIGITALE FUNDAMENTE ABSICHERN: RESILIENZ BEGINNT IN DER INFRASTRUKTUR

Klassische IT-Sicherheitsprinzipien – Vertraulichkeit, Integrität und Verfügbarkeit – greifen heute zu kurz, wenn physische Netzelemente, Unterseekabel, Rechenzentren oder Glasfaserverbindungen selbst zur Zielscheibe werden. Die Digitalisierung von Produktionsprozessen, gepaart mit geopolitischen Spannungen, rückt die Infrastruktur selbst zunehmend ins Zentrum sicherheitspolitischer Überlegungen.

Skandinavien geht hier voran: Unternehmen investieren in Redundanzen, alternative Datenrouten, dezentrale Backup-Rechenzentren und Notfallprotokolle. Ziel ist es, physische Ausfallsicherheit als Grundlage digitaler Resilienz zu schaffen.

Diese Investitionen sind essenziell, denn datenintensive Anwendungen wie durch künstliche Intelligenz (KI) gestützte Analysen, Internet-of-Things-(IoT)-Plattformen oder digitale Zwillinge brauchen eine zuverlässige, latenzarme Anbindung. Glasfaser ist dabei kein Komfortmerkmal, sondern Voraussetzung für unternehmerische Handlungsfähigkeit. Wer Ausfallszenarien ernst nimmt, schafft Vertrauen – bei Kunden, Investoren und Behörden gleichermaßen.

2. KRYPTOGRAFIE WEITERDENKEN: STRATEGIEN FÜR DAS POST-QUANTEN-ZEITALTER

Quantencomputer sind längst nicht mehr bloßes Zukunftsszenario – erste Anwendungen zeigen bereits, wie Angreifer konventionelle Verschlüsselungstechniken kompromittieren könnten. Das „Steal now, decrypt later"-Prinzip bedroht heute gespeicherte Daten: Informationen, die derzeit scheinbar sicher sind, könnten morgen öffentlich werden.

Skandinavische Länder begegnen dieser Herausforderung bereits. Dort integrieren Unternehmen quantenresistente Algorithmen in sicherheitskritische Systeme – oft im Schulterschluss zwischen Staat und Wirtschaft. Auch deutsche Firmen sollten jetzt handeln und ihre kryptografischen Systeme auf „Crypto Agility" ausrichten – also auf die Fähigkeit, flexibel zwischen verschiedenen Verschlüsselungsstandards zu wechseln, ohne den laufenden Betrieb zu gefährden.

Gleichzeitig wächst das Datenvolumen weiter: Quantenanwendungen erzeugen riesige Datenmengen, beispielsweise in Forschung, Finanzanalyse, Logistik oder KI-Modellen. Wer auf diese Entwicklung vorbereitet sein will, braucht skalierbare, sichere Datenarchitekturen, die sowohl die heutigen Anforderungen erfüllen als auch für die nächsten zehn Jahre tragfähig sind.

3. MENSCH UND MASCHINE ABSICHERN: AUTOMATISIERUNG TRIFFT SICHERHEITSKULTUR

Der häufigste Angriffsvektor bleibt der Mensch: Phishingmails, Social Engineering, schwache Passwörter oder fehlerhafte Konfigurationen führen oft zu erfolgreichen Angriffen – nicht weil die Technik versagt, sondern weil sie falsch bedient wird.

Moderne Sicherheitsarchitekturen verbinden deshalb technologische Frühwarnsysteme mit einer lebendigen Sicherheitskultur. So können Firmen beispielsweise KI-basierte Analysesysteme einsetzen, die Netzwerkaktivitäten rund um die Uhr auswerten und automatisiert auf Unregelmäßigkeiten reagieren – ohne Zeitverlust, ohne manuelle Verzögerung.

Doch Technologie allein reicht nicht: Wer IT-Sicherheit nachhaltig verankern will, muss das Bewusstsein stärken – durch realistische Simulationen, Gamification, individuelle Schulungen, Social-Engineering-Tests und aktives Vorleben durch die Führungsebene. Gerade im Umgang mit sensiblen Daten braucht es klare Prozesse, Rollenkonzepte und Verantwortlichkeiten, denn nur wenn Technik und Verhalten zusammenspielen, entsteht echte Resilienz.

4. GETEILTES WISSEN ALS SICHERHEITSFAKTOR: KOOPERATIONSMODELLE ETABLIEREN

Cyberbedrohungen enden nicht an der Unternehmensgrenze, sondern wirken entlang globaler Wertschöpfungsketten. Ein kompromittierter Lieferant oder IT-Dienstleister kann ganze Branchen destabilisieren. Deshalb braucht es Kooperationsmodelle, in denen Organisationen Sicherheitswissen teilen, analysieren und weiterentwickeln.

Best Practice aus Dänemark: Dort existiert ein staatlich initiiertes Sicherheitsnetzwerk, in dem Unternehmen Vorfälle anonym melden und im Gegenzug aggregierte Lagebilder und konkrete Handlungsempfehlungen erhalten. Dieses Prinzip ließe sich auch auf deutsche Branchen übertragen – etwa über sektorübergreifende Computer Emergency Response Teams (CERTs), Verbände oder Konsortien.

Auch der Austausch zu Themen wie Datenarchitektur, Speicherstrategien oder KI-Einsatz schafft Mehrwert. Wer Wissen teilt, erkennt Muster früher, reagiert schneller und entwickelt gemeinsam Standards, von denen alle profitieren.

FAZIT: SICHERHEIT IST KEIN TOOL – SONDERN STRATEGISCHE KOMPETENZ

Cybersicherheit ist kein Projekt, kein Audit, kein einzelnes Softwareprodukt. Sie ist ein kontinuierlicher Prozess, der tief in Strategie, Technologie und Unternehmenskultur verankert sein sollte. Die nordischen Länder zeigen, wie dieser Dreiklang funktionieren kann. Wer dort Resilienz aufbaut, denkt vernetzt, plant langfristig und investiert gezielt.

Und: Daten sind kein Störfaktor, sondern Rohstoff und Erfolgsfaktor zugleich. Wer sie schützt, strukturiert nutzt und durch intelligente Systeme auswertet, schafft nicht nur Sicherheit, sondern auch Zukunftsfähigkeit. In einer Welt, in der digitale Souveränität zur Standortfrage wird, entscheidet strategische Cybersicherheit über Wettbewerbsfähigkeit, Innovationskraft und das Vertrauen der nächsten Generation. ■

ANDREAS GERHARDT
ist Experte für die digitale Transformation und CEO von GlobalConnect in Deutschland.

Cybersicherheit 2030

NEUN HANDLUNGSFELDER FÜR STRATEGISCHE RESILIENZ

Unternehmen, die heute die Weichen für ihre digitale Sicherheit stellen, investieren nicht nur in Schutz, sondern auch in ihre Zukunft. In einer zunehmend fragmentierten Bedrohungslandschaft werden proaktive Maßnahmen so zum entscheidenden Wettbewerbsvorteil.

Die Cyber-Security-Landschaft entwickelt sich rasant und wird bis 2030 von grundlegenden Veränderungen geprägt sein. Laut einer Deloitte-Analyse müssen Unternehmen nun von reaktiven Schutzmaßnahmen zu proaktiver strategischer Planung übergehen. Cybersicherheit ist längst mehr als ein IT-Thema – sie ist ein strategischer Erfolgsfaktor für Organisationen. Wer heute nicht handelt, riskiert morgen erhebliche finanzielle Verluste, Reputationsschäden und rechtliche Konsequenzen durch Datenverluste oder Systemausfälle.

HYPERDIGITALISIERUNG VERSCHÄRFT BEDROHUNGSLAGE

Was wir heute erleben, geht über die bisher bekannte Digitalisierung einzelner Bereiche hinaus: Hyperdigitalisierung beschreibt die rasante, flächendeckende Durchdringung aller Lebens- und Wirtschaftsbereiche mit digitalen Technologien. Entwicklungen wie Cloud-Infrastrukturen, das Internet of Things (IoT), KI-gestützte Prozesse, Quantencomputing, vernetzte Lieferketten und hybride Arbeitsmodelle erzeugen eine nie dagewesene Dynamik in der unternehmerischen Welt – und damit auch neue Angriffsflächen für Cyberkriminelle. Gleichzeitig nutzen kriminelle Akteure immer raffiniertere Angriffsarten.

Diese Entwicklung stellt Sicherheitsarchitekturen vor enorme Herausforderungen: Die Bedrohungslage verschärft sich schneller, als viele Systeme reagieren können. Geopolitische Spannungen erschweren die Etablierung globaler Standards, während Unternehmen teils auch mit Angriffen staatlicher Akteure rechnen müssen. Gleichzeitig nimmt die regulatorische Komplexität durch Rahmenwerke wie NIS-2, DORA oder KRITIS zu. Hinzu kommt, dass technologische Innovationen wie künstliche Intelligenz (KI) zwar Effizienzgewinne versprechen, aber zugleich neue Angriffsszenarien eröffnen.

Angesichts dieser sich zuspitzenden Bedrohungslage ist es nicht nur notwendig, auf aktuelle Risiken zu reagieren, sondern auch proaktiv in die Zukunft zu blicken. Wer heute versteht, wie sich Angriffsvektoren, Technologien und regulatorische Rahmenbedingungen entwickeln könnten, schafft langfristig die Grundlage für nachhaltige Resilienz und strategische Handlungsfähigkeit.

VIER SZENARIEN ZUR ORIENTIERUNG

Wie sich Unternehmen in diesem komplexen Umfeld positionieren können, zeigen vier Zukunftsszenarien (siehe Abbildung 1), die Deloitte in der IT-SICHERHEIT 6/2024 vorgestellt hat. Die Analyse basiert auf der KI-gestützten Auswertung von rund 157.000 Datenpunkten und wurde in Gesprächen mit über 30 CIOs und CISOs validiert. Sie zeigt ein Spektrum, das vom „Cyber-Security-Paradies" mit harmonisierten Standards bis zum „Recht des Stärkeren" mit fragmentierten Regulierungen reicht.

Die vier Szenarien unterscheiden sich entlang zweier zentraler Achsen: dem Grad der Zusammenarbeit bei Technologie und Regulierung sowie der strategischen Bedeutung von Cybersicherheit. Während das „Cyber-Security-Paradies" international harmonisierte Standards und strategische Relevanz von Sicherheit vorsieht, beschreibt das Szenario „Kosteneffizienz statt Sicherheit" eine Welt vereinheitlichter Regulierung, in der Cybersecurity jedoch als reiner Kostenfaktor betrachtet wird. Als wahrscheinlichstes Szenario gilt „differenziertes Vertrauen", bei dem trotz fragmentierter Regulierungslandschaft Cybersicherheit hohe Relevanz besitzt.

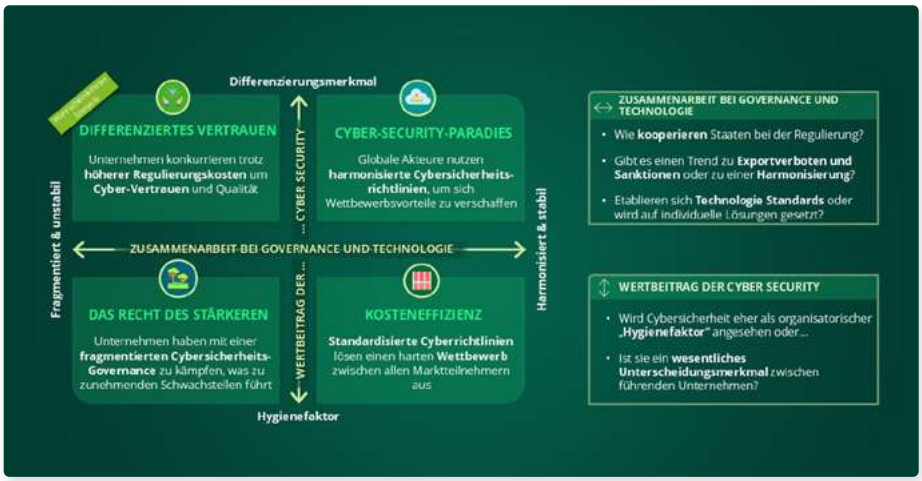


Abbildung 1: Überblick über die vier Cybersecurity-Szenarien 2030 (Bild: Deloitte)

Bild: Johannes | Digital Vision Lab - stock.adobe.com

Entscheidend für Unternehmen sind jedoch nicht die Szenarien selbst, sondern die strategische Vorbereitung. Dafür haben die Autoren der Studie neun konkrete Handlungsfelder identifiziert, die unabhängig vom eintretenden Szenario wirksam sind – sogenannte „No Regret Moves".

TECHNOLOGISCHE VORREITERSCHAFT ALS GRUNDPFEILER

Die erste Priorität liegt laut der Analyse bei Investitionen in Forschung, Entwicklung und modernste Sicherheitstechnologien. Unternehmen sollten kontinuierlich neue Verfahren evaluieren und pilotieren – von KI-gestützter Bedrohungserkennung bis zu quantensicheren Verschlüsselungen. Besondere Bedeutung gewinnen dabei Advanced Endpoint Detection and Response (EDR), Security-Information-and-Event-Management-(SIEM)-Systeme, Cloud Security Posture Management (CSPM) und automatisierte Threat-Hunting-Plattformen.

Diese Technologien ermöglichen eine frühzeitige Erkennung und Abwehr komplexer Angriffe, verbessern die Transparenz über IT-Umgebungen und unterstützen Unternehmen dabei, Sicherheitsvorfälle schneller sowie gezielter zu analysieren und zu beheben. Die kontinuierliche Weiterentwicklung technologischer Fähigkeiten ist essenziell, um auf neue Bedrohungen reagieren zu können.

Dabei geht es nicht nur um die Implementierung einzelner Tools, sondern um die systematische Entwicklung einer zukunftsfähigen Technologielandschaft. Firmen müssen in der Lage sein, neue Bedrohungen frühzeitig zu identifizieren und geeignete Gegenmaßnahmen zu entwickeln. Dies erfordert sowohl finanzielle Investitionen als auch den Aufbau entsprechender Kompetenzen im eigenen Unternehmen.

STRATEGISCHES TALENTMANAGEMENT

Das zweite zentrale Handlungsfeld betrifft das Talentmanagement in einer sich verschärfenden Fachkräftekrise. Cybersicherheit ist bereits heute das Skillcluster mit den am meisten unbesetzten Stellen, und der Bedarf steigt weiter. Die Lage wird sich weiter verschärfen, da die dynamische Bedrohungslage kontinuierlich Strategen und Architekten erfordert, die in der Lage sind, komplexe Systeme einzuführen und zu überwachen.

Mit der fortschreitenden Digitalisierung und dem rasanten Fortschritt im Bereich der künstlichen Intelligenz steigt der globale Wettbewerb um qualifizierte Cybertalente deutlich an. Organisationen sollten daher gezielt in die Identifikation, Anwerbung und Weiterentwicklung von Fachkräften investieren. Hierfür sollten Unternehmen auch neue Wege gehen, etwa Kooperationen mit Hochschulen, praxisorientierte Bootcamps oder Programme für Quereinsteigerinnen.

Auch berufsbegleitende Ausbildungsmodelle wie Cybersecurity-Traineeships können wertvolle Zugänge zu neuen Talentpools schaffen. Zur Bindung bestehender Fachkräfte tragen wettbewerbsfähige Gehälter, gezielte Weiterbildungsangebote, Zertifizierungen und flexible Arbeitsmodelle bei, die individuelle Entwicklung und langfristige Perspektiven fördern.

Die Herausforderung liegt dabei nicht nur in der quantitativen Verfügbarkeit von Fachkräften, sondern auch in der qualitativen Weiterentwicklung. Cybersicherheits-Experten müssen in der Lage sein, mit der sich schnell entwickelnden Bedrohungslandschaft Schritt zu halten und gleichzeitig strategische Entscheidungen für ihre Organisationen zu treffen.

SECURITY BY DESIGN UND WERTORIENTIERTE INTEGRATION

Das dritte Handlungsfeld umfasst die nahtlose Integration von Cybersicherheit in alle Geschäftsprozesse. Sicherheit darf kein Add-on sein, sondern muss von Anfang an in alle Prozesse, Produkte und Technologien eingebettet werden – von der Entwicklung über den Betrieb bis zur Wartung. „Security by Design" sollte zum Standard werden. Das bedeutet in der Praxis, dass Sicherheitsaspekte systematisch in jede Phase integriert werden.

Dies umfasst die Bedrohungsmodellierung in der Planungsphase, sichere Programmierpraktiken und automatisierte Code-Analysen in der Entwicklung bis zu regelmäßigen Sicherheitsbewertungen, Patch-Management und Zugriffskontrollen im Betrieb.

CISOs spielen dabei eine zentrale Rolle: Sie können die Relevanz von Sicherheitsmaßnahmen stärken, indem sie die Wahrnehmung auf der Führungsebene verändern. Wurde Cybersicherheit bislang oft als rein präventive Maßnahme und Kostenfaktor betrachtet, zeigt eine wertorientierte Perspektive, dass moderne Sicherheitsarchitekturen auf Basis des Zero-Trust-Ansatzes nicht nur Risiken minimieren, sondern auch einen messbaren Return on Investment (ROI) erzielen.

Dieser ROI entsteht durch die Vermeidung von Ausfallzeiten, geringere Kosten bei Sicherheitsvorfällen, Effizienzgewinne durch Automatisierung und ein gestärktes Vertrauen von Kunden und Partnern, was zu einer verbesserten Marktposition führt. Cybersecurity wird damit vom Kostenfaktor zum strategischen Erfolgsfaktor.

PARTNERSCHAFTEN STÄRKEN UND AUTOMATISIERUNG VORANTREIBEN

Weitere zentrale Handlungsfelder umfassen den Aufbau strategischer Partnerschaften und die Nutzung von Automatisierung. IT-Sicherheit lässt sich in vielen Bereichen effektiver umsetzen, wenn Unternehmen auf starke Partnerschaften setzen. Der Aufbau vertrauensvoller Kooperationen mit Behörden, Brancheninitiativen und Technologieanbietern schafft Synergien und erhöht die kollektive Resilienz.

Automatisierte Sicherheitsprozesse und risikobasierte Ansätze ermöglichen zudem eine skalierbare und reaktionsschnelle Cyberabwehr. Künstliche Intelligenz kann dabei helfen, Anomalien frühzeitig zu erkennen und Reaktionen zu orchestrieren.

REGULATORISCHE COMPLIANCE

NIS-2, DORA und KRITIS zeigen, dass strategische Vorteile durch die schnelle und konsequente Umsetzung regulatorischer Anforderungen entstehen. Unternehmen sollten nicht nur reagieren, sondern proaktiv Strukturen schaffen, die regulatorische Anforderungen frühzeitig erfüllen – und so Marktzugang und Vertrauen sichern.

Besonders NIS-2 bringt neue Pflichten mit sich – etwa Meldefristen, Sicherheit in der Lieferkette und stärkere Einbindung des Managements. KRITIS ergänzt dies auf nationaler Ebene durch Auditpflichten und Nachweisanforderungen für Betreiber kritischer Infrastrukturen. Wer hier vorbereitet ist, stärkt nicht nur seine Compliance, sondern seine gesamte Widerstandsfähigkeit.

Bild: jah_CK - stock.adobe.com

TREND SCOUTING, ZERO TRUST UND DIGITAL TRUST

Das institutionalisierte Trend Scouting bildet ein weiteres kritisches Handlungsfeld. Die kontinuierliche Beobachtung technologischer, geopolitischer und gesellschaftlicher Entwicklungen ist Voraussetzung für strategische Anpassungsfähigkeit. Wer früh erkennt, kann früh handeln.

Um Trend Scouting systematisch zu verankern, sollten Unternehmen gezielt Ressourcen aufbauen, etwa durch dedizierte Threat-Intelligence-Teams, die relevante Entwicklungen analysieren und bewerten. Auch die regelmäßige Teilnahme an Fachkonferenzen, der aktive Austausch in Branchenforen sowie die Mitgliedschaft in Netzwerken tragen dazu bei, frühzeitig relevante Signale zu erkennen. Ergänzend empfiehlt sich das Abonnieren spezialisierter Fachpublikationen, Security-Feeds und Analysedienste, um kontinuierlich über neue Bedrohungen, Technologien und regulatorische Veränderungen informiert zu bleiben.

Zero Trust als Architekturprinzip ersetzt implizites Vertrauen durch kontinuierliche Validierung nach dem Motto „Never trust, always verify". Es bildet die Grundlage für eine moderne, adaptive und widerstandsfähige Sicherheitsarchitektur, die Identitäten, Geräte, Daten und Netzwerke gleichermaßen schützt. Dieses Prinzip wird durch eine Architektur umgesetzt, die auf der kontinuierlichen Überprüfung interner und externer Faktoren basiert und eine adaptive Sicherheitsstrategie ermöglicht, die sich flexibel an neue Bedrohungslagen anpassen lässt.

Das neunte Handlungsfeld ist „Digital Trust" als Benchmark. Es beschreibt das Vertrauen von Nutzern in die Sicherheit und Zuverlässigkeit digitaler Systeme und wird zunehmend zur Voraussetzung für die erfolgreiche Einführung neuer Technologien und die Akzeptanz datengetriebener Geschäftsmodelle. Es basiert auf Faktoren wie Datenintegrität, der konsequenten Einhaltung gesetzlicher Vorschriften und einem sicheren Zugriffsmanagement. Aber auch die Benutzerfreundlichkeit spielt eine Rolle, genauso wie die Frage, inwiefern neue Technologien den Menschen befähigen, auch in kritischen Situationen handlungsfähig zu bleiben.

WEICHENSTELLUNG FÜR DIE DIGITALE ZUKUNFT

Cybersicherheit wird im Jahr 2030 nicht mehr durch technische Reaktion auf Angriffe definiert sein, sondern durch vorausschauende strategische Planung. Unternehmen, die Cybersicherheit bereits heute als integralen Bestandteil ihrer Geschäftsstrategie und Resilienz als Führungsaufgabe begreifen, sichern sich gegen Risiken ab und schaffen Vertrauen sowie Zukunftsfähigkeit.

Wer heute seine Systeme versteht, Fachkräfte ausbildet und regulatorische Vorgaben ernst nimmt, wird morgen zu den Gewinnern gehören. Durch strategische Voraussicht, gezielte Investitionen in Talente und die Integration von Cybersicherheit in die Kernbereiche des Unternehmens können Organisationen nicht nur Risiken minimieren, sondern auch neue Chancen im digitalen Wandel erschließen.

Im Zentrum steht dabei nicht das Festhalten an einem bestimmten Zielbild, sondern die Fähigkeit zur Anpassung und robusten Reaktion auf Veränderungen. Wer heute in Szenarien denkt, kann morgen souverän handeln – und seine Organisation sicher durch ein zunehmend komplexes digitales Umfeld steuern. Strategische Voraussicht, kontinuierliche Weiterentwicklung und eine klar verankerte IT-Sicherheit auf Führungsebene sind dabei zentrale Erfolgsfaktoren.

Jetzt ist der Zeitpunkt, aktiv zu werden. Wer heute die richtigen Weichen stellt, stärkt nicht nur seine Sicherheit, sondern auch seine Wettbewerbsfähigkeit und langfristige Resilienz in einer zunehmend vernetzten und komplexen Welt. ■

FABIAN MIHAILOWITSCH
ist Partner und Leiter des Bereichs Enterprise Security bei Deloitte.

Alternativen zu iOS und Android

WEGE ZUR MOBILEN UNABHÄNGIGKEIT

Bild: Malambo C/peopleimages.com - stock.adobe.com

Geopolitische Spannungen rücken digitale Souveränität verstärkt in den Fokus. Viele Unternehmen sehen ihre Abhängigkeit von ausländischer IT-Infrastruktur inzwischen als erheblichen Risikofaktor. Dabei geraten auch mobile Endgeräte zunehmend in den Blick. Welche Alternativen jenseits von Apple und Google existieren, und wie Unternehmen mehr Unabhängigkeit gewinnen können, zeigt unser Autor.

Die Abhängigkeit deutscher Unternehmen von ausländischen Technologieanbietern hat laut einer Bitkom-Studie ein bedenkliches Ausmaß erreicht. Die Untersuchung „Digitale Souveränität – Wie abhängig ist unsere Wirtschaft?" offenbart, dass 90 Prozent der deutschen Unternehmen Endgeräte importieren. Bei Software-Anwendungen sind es 75 Prozent, bei Cybersicherheitslösungen 72 Prozent.

Besonders problematisch: 81 Prozent der Firmen sehen sich als abhängig von Digitalimporten aus den USA an, davon bezeichnen sich 41 Prozent als stark abhängig. Zudem bereiten die politischen Entwicklungen den Verantwortlichen Sorgen – 78 Prozent zeigen sich beunruhigt wegen der Dominanz der USA, 68 Prozent wegen der Chinas.

Eines ist klar: Angesichts der Weltlage und der politischen Entwicklungen müssen sich Organisationen dringend mit diesem Thema befassen und prüfen, wie sie Abhängigkeiten reduzieren können.

MOBILE GERÄTE MITBEDENKEN

Wer sich mit dem Thema digitale Souveränität beschäftigt, sollte auch mobile Geräte in seine Überlegungen einbeziehen. Längst sind sie keine kleinen Gimmicks mehr, sondern leistungsfähige Computer, ohne deren Funktionsfähigkeit in manchen Organisationen das Chaos ausbricht oder die Arbeit stillsteht.

Smartphones und Tablets dienen der Datenerfassung, der Kommunikation, Unternehmen setzen sie teilweise zum Remote-Arbeiten ein, ermöglichen den entfernten Zugriff auf wichtige Daten, sind nötig für die Zwei-Faktor-Authentifizierung oder öffnen die Bürotür. In vielen Branchen nutzen Mitarbeiter Apps auf den Geräten, die komplette Arbeitsprozesse abbilden. Die Systeme übertragen diese dann teilweise automatisiert, beispielsweise an Abrechnungssysteme.

Gerade für kritische Infrastrukturen wie Strom- und Wasserversorgung, Gesundheitswesen oder den öffentlichen Verkehr ist digitale Souveränität von zentraler Bedeutung, da Ausfälle oder Abhängigkeiten von einzelnen Diensten unmittelbare Auswirkungen auf die Versorgungssicherheit und die öffentliche Ordnung haben können. Doch auch für andere Unternehmen – unabhängig von Größe und Branche – gilt: Wer bei mobilen Geräten die eigene digitale Handlungsfähigkeit nicht sichert, setzt sich einem erheblichen Risiko aus.

ALTERNATIVE ZUM GOOGLE-MONOPOL

Bei Smartphones zeigt sich schnell, wie groß die Abhängigkeit beispielsweise von den USA ist, denn mit iOS und Android gibt es nur zwei dominierende Systeme. Bei iPhones oder iPads ist es aktuell völlig unmöglich, eine US-unabhängige

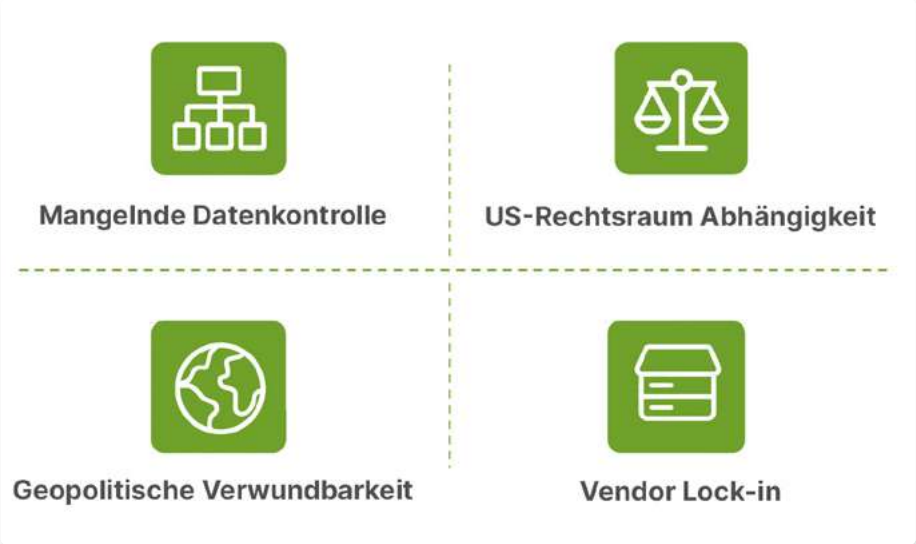


Abbildung 1: Risiken der mobilen Abhängigkeit von US-Diensten (Bild: Cortado Mobile Solutions GmbH)

Lösung zu finden. Anders bei Android: Hier gibt es zwar den beherrschenden US-Riesen Google, aber es gibt auch das Android Open Source Project (AOSP), eine quelloffene Alternative zum „Google Android".

Ein Beispiel für ein Betriebssystem, das auf AOSP basiert, ist /e/OS. Das Gesamtpaket von Google-Anwendungen und -Schnittstellen, das auf zertifizierten Android-Geräten vorinstalliert ist – etwa Google Play Store, Gmail, Google Maps oder YouTube –, fehlt auf diesen Geräten. Darüber hinaus gibt es noch einige andere Projekte wie GrapheneOS, CalyxOS oder iodéOS, die ähnliche Ansätze verfolgen.

Für den Einsatz solcher Google-unabhängigen Betriebssysteme sind kompatible Geräte erforderlich. Die jeweiligen Anbieter listen unterstützte Modelle auf ihren Webseiten auf. Auf der Liste von /e/OS-Anbieter Murena finden sich beispielsweise die nachhaltigen Fairphones aus den Niederlanden, aber auch verschiedene Google-Pixel-Modelle. Letzteres mag paradox erscheinen, hat aber technische Gründe: Pixel-Geräte eignen sich aufgrund ihrer offenen Architektur besonders gut für die Installation alternativer Betriebssysteme.

Wer andere Geräte einsetzen möchte, die nicht auf den Listen der Anbieter stehen, stößt derzeit oft auf Einschränkungen. Theoretisch könnte man zwar auch andere Android-Geräte rooten und Open Source darauf installieren, doch es gibt Einschränkungen. Nicht alle Androiden eignen sich für das Rooten oder Aufspielen von benutzerdefinierten Betriebssystemen. Daher empfiehlt es sich vor allem für Unternehmen, auf die geprüften Modelle zu setzen.

VERWALTUNG ERFORDERT EUROPÄISCHE LÖSUNGEN

Nach der Auswahl des Google-unabhängigen Betriebssystems und passender Geräte fehlt noch ein Mobile-Device-Management-(MDM)-System. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt MDM-Systeme bei allen Mobility-Projekten zwingend, um den Datenschutz zu gewährleisten. Sie sorgen für die sichere und nach der Datenschutzgrundverordnung (DSGVO) konforme Verwaltung der Geräte. Das BSI erklärt: „Mit Blick auf die Sicherheit ist die Kernfunktion des MDM-Systems die wirksame Durchsetzung definierter Sicherheitsrichtlinien und Konfigurationsparameter auf

Abbildung 2: Startbildschirm des Fairphones (Bild: Cortado Mobile Solutions GmbH)

den mobilen Endgeräten." Diese Empfehlung gilt grundsätzlich, egal ob Unternehmen mit iOS-Geräten, Google-fähigen oder entgoogelten Geräten arbeiten.

Ein Mobile Device Management verwaltet und kontrolliert mobile Endgeräte in einem Unternehmen. Dazu gehören die zentrale Einrichtung und das Ausrollen von Konfigurationen (E-Mail, WLAN und VPN), die Implementierung von Sicherheitsrichtlinien, die Bereitstellung von Anwendungen und Updates, die Verwaltung und der Schutz von Daten auf den Geräten sowie Remote Wipe und Remote Lock bei Geräteverlust.

Will man mobil digital souverän agieren, muss natürlich auch das MDM-System aus Europa oder aus Deutschland sein. Ein US-System oder eines aus einem Land außerhalb Europas widerspricht der digitalen Souveränität.

PRAKTISCHE HÜRDEN BEIM VERZICHT AUF GOOGLE-DIENSTE

Bei Geräten ohne Google sind neben den normalen MDM-Aufgaben primär zwei Bereiche für Unternehmen relevant: die Inbetriebnahme der Geräte ohne manuelles Einrichten und das Verteilen von Apps.

Nutzt man Google in Verbindung mit einer passenden MDM-Lösung, werden beim Zero-Touch-Enrollment von Android Enterprise die Geräte automatisch mit Einstellungen, Anwendungen und Richtlinien konfiguriert, wenn die Benutzer sie zum ersten Mal einschalten. Zur Identifikation der Geräte nutzt das System bei der Anmeldung Geräteinformationen und Konfigurationsprofile.

Bei Android ohne Google, also bei Open-Source-Lösungen, funktioniert das nicht. Derzeit gibt es keine Möglichkeit, die Geräte automatisch mit dem MDM zu verbinden. Das geht nur manuell. Zudem gibt es nur wenige Geräte, die ab Werk ohne Google gekauft werden können. Häufig müssen Unternehmen die Geräte erst „entgoogeln" und danach mit dem MDM verbinden. Anschließend erhalten sie automatisch den MDM-Payload mit den Konfigurationen. Der Unterschied zum Zero-Touch besteht darin: Das Gerät muss entgoogelt und manuell mit dem MDM verbunden werden. Deswegen übernehmen einige Google-unabhängige MDM-Anbieter für Kunden, die Geräte über sie beziehen, den gesamten Inbetriebnahmeprozess.

Die zweite Herausforderung besteht darin, Apps ohne den sonst üblichen Weg über den Google Play Store zu verteilen. Spezialisierte MDM-Anbieter lösen das, indem sie auf dem Gerät die Apps in Form signierter Android Package Kits (APK) einspielen. Dieser Weg wird auch genutzt, um Eigenentwicklungen von Unternehmen auf den Geräten zu verteilen.

Diese APKs lassen sich zentral verwalten und ohne Google-Dienste installieren. Einer datenschutzkonformen Nutzung der Apps steht damit nichts im Weg. Auch App-Updates können Unternehmen so zentral installieren und verwalten. Die Einrichtung von Exchange-Konten, VPNs und WLAN erfolgt über die Profile im MDM oder über die verwalteten Konfigurationen der gewünschten App.

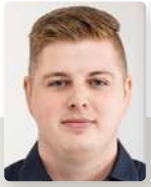
SCHRITTWEISE UMSETZUNG ALS REALISTISCHER WEG

Wer sein Unternehmen digital souverän aufstellen möchte, der findet schon heute Wege zur Realisierung. Wichtig dabei: eine schrittweise Umsetzung der Strategie. Die Umstellung sollte bei besonders sicherheitssensiblen Bereichen beginnen. Die Verantwortlichen müssen aber bedenken, dass ein Ersetzen von nicht-europäischen Diensten auch Funktionseinschränkungen mit sich bringen kann. Nicht alles wird genauso wie vorher funktionieren. Zudem können zusätzliche Kosten entstehen.

Trotz dieser Herausforderungen sollten sich Unternehmen mit dem Thema digitale Souveränität auseinandersetzen und vorsorgen. Eine vollständige digitale Unabhängigkeit ist derzeit jedoch nicht realistisch, aber Organisationen können bereits jetzt prüfen, was möglich ist. ■

HERAUSFORDERUNGEN BEI MOBILER DIGITALER SOUVERÄNITÄT

- *Es stehen nur ausgewählte Geräte zur Verfügung. Das bisher eingesetzte Gerät ist möglicherweise nicht dabei.*
- *Gewohnte Apps müssen durch andere Anwendungen ersetzt werden.*
- *Alternative Apps und Dienste können teurer sein.*
- *Schulungen für die Mitarbeiter sind nötig, wenn alternative Geräte und Apps eingesetzt werden.*
- *Umstellungen erzeugen bei einem Teil der Mitarbeiter Widerstand. Hier müssen Unternehmen Überzeugungsarbeit für das Thema digitale Souveränität leisten.*
- *Eine Umstellung erfordert einen erheblichen Arbeitsaufwand der IT.*



MICHAEL RÖDIGER
ist Geschäftsführer der
Cortado Mobile Solutions GmbH.

Sichere Identifikation im Cloud-Umfeld, schnellere Audits

DEZENTRALISIERTE IDENTITÄTEN: EINE NEUE ÄRA IM DIGITALEN IDENTITÄTSMANAGEMENT

Dezentralisierte Identitäten (DIDs) nutzen die Blockchain als Basis für Authentizität und Nachvollziehbarkeit. Sie erlauben es, sich unabhängig und sicher digital auszuweisen und gezielt zu entscheiden, welche Informationen preisgegeben werden. Mit der geplanten europäischen digitalen Identität greift die EU dieses Prinzip auf und will es bis 2027 etablieren.

Die digitale Identifikation bewegt sich im Spannungsfeld zwischen Sicherheit und Benutzerfreundlichkeit. Einerseits verlangen komplexe Sicherheitsmechanismen nach aufwendigen Verfahren, um die Authentizität und Privatsphäre der Nutzer zu gewährleisten. Andererseits führt kein Weg an elektronischen Identifikationsverfahren vorbei – sei es im Onlinehandel, beim Banking oder bei administrativen Prozessen und Fernzugriffen.

In der heutigen Welt geben Nutzer ihre Daten häufig an große Unternehmen oder Behörden weiter, zum Beispiel im Postident-Verfahren oder über einen Identitätsanbieter. Traditionell müssen sie hierfür Termine vereinbaren, bei denen Mitarbeiter sie über das Internet identifizieren und sämtliche ihrer personenbezogenen Daten begutachten, bevor sie etwa einen digitalen Vertrag unterzeichnen oder auf ihren Onlinebanking-Account zugreifen können. Dieses Vorgehen legt nicht nur zahlreiche personenbezogene Daten offen, sondern macht die Identität auch abhängig vom Prüfer.

Die dezentralisierte Identität, auch Self-Sovereign Identity (SSI) genannt, soll diesen Konflikt lösen. Das Konzept erlaubt es Nutzern, ihre personenbezogenen Daten in digitaler Form zu kontrollieren und darüber zu entscheiden, wer diese Angaben einsehen darf und zu welchem Zeitpunkt. Die Anwendung dezentraler Identitäten ermöglicht es, jederzeit und überall ohne die Einbindung einer weiteren Institution die eigenen Daten zu signieren und ausgewählte nachweisbare Informationen mit Dritten zu teilen.

BLOCKCHAIN-TECHNOLOGIE UNTERSTÜTZT SELEKTIVE DATENFREIGABE

Eine DID ist ein kryptografisches Konstrukt, das im Gegensatz zu traditionellen Identifikationsmethoden keine personenbezogenen Daten ver-

Bild: Vladislav - stock.adobe.com

wendet. Stattdessen wird mit der DID ein asymmetrisches Schlüsselpaar verknüpft, das die Verwaltung der in der Blockchain verankerten Identität ermöglicht. Die Blockchain wird hierbei als Datenbasis verwendet, um die DID nachverfolgbar abzulegen, ähnlich der Nachverfolgbarkeit von Kryptowährungen. Die Funktionsweise beruht darauf, dass der öffentliche Schlüssel für alle zugänglich ist und zur Überprüfung von Zertifikaten genutzt werden kann, die mit dem zugehörigen geheimen Schlüssel der Identität erstellt wurden.

Diese kryptografische Signatur ihrer Identitätsdaten ermöglicht es einer Person, ihre Identität zu bestätigen. Anders als bei der Überprüfung eines Personalausweises bietet eine DID den Vorteil, dass die Person selbst entscheiden kann, welche Daten sie teilen möchte. So kann beispielsweise nur der Name offengelegt werden, ohne zusätzliche Informationen wie Wohnort oder Körpermerkmale preiszugeben.

EU PLANT EUROPAWEITE DIGITALE BRIEFTASCHE BIS 2027

Die Europäische Union hat den Lösungsansatz bereits aufgegriffen: Gemäß der eIDAS-2.0-Verordnung haben sich alle teilnehmenden Länder dazu verpflichtet, bis 2027 allen Bürgerinnen und Bürgern sowie Organisationen eine interoperable Lösung für eine digitale Brieftasche zur Verfügung zu stellen. Diese EUDI-Wallets sollen EU-weit für den Zugang zu öffentlichen und privaten digitalen Diensten genutzt werden, um Online-Interaktionen nahtloser und effizienter zu gestalten. Die Umsetzung der digitalen Geldbörse befindet sich derzeit noch in der Entscheidungs- und Planungsphase.

Die Einführung der eIDAS 2.0 stellt Regierungsorganisationen und Unternehmen eine Schnittstelle bereit, über die sich die Bürger identifizieren können. Firmen, die diese Schnittstelle implementieren, können von einem vereinfachten Identifikationsprozess für ihre Kunden profitieren und somit einen Wettbewerbsvorteil erzielen.

DEZENTRALISIERTE IDENTITÄTEN UND CLOUD-TECHNOLOGIE

Parallel zur politischen Umsetzung durch die EU entstehen auch technische Lösungen für die Praxis. Dezentralisierte Identitätssysteme erweisen sich dabei als gute Ergänzung zur Cloud-Technologie. Sie integrieren sich nahtlos in Cloud-Dienste und ermöglichen sichere, benutzerfreundliche Identifikationsmethoden über verschiedene Plattformen hinweg. Das Ergebnis ist eine flexible und skalierbare Infrastruktur für moderne digitale Ökosysteme.

Ein wesentlicher Vorteil liegt in der Steigerung der Sicherheit. Die Funktionsweise einer DID erlaubt es, nur diejenigen Daten zu teilen, die notwendig sind. Neben der vollständigen Kontrolle über die eigene Identität und über die Freigabe dieser Daten erhöht sie die Sicherheit der Daten und unterstützt dennoch weiterhin bestehende Login-Technologien wie die Multi-Faktor-Authentifizierung und die biometrische Verifikation. Die Kombination von Identifikation und Authentifizierung steigert hierbei die Vertrauenswürdigkeit der Cloud-Nutzer. Die zugrunde liegende Blockchain-Technologie ermöglicht zudem eine einfache Nachverfolgung von Änderungen.

Weiter wird der Datenschutz durch Prinzipien wie Datenminimierung und Nutzerzustimmung gefördert. Eingebaute Datenschutzfunktionen und -kontrollen in Kombination mit der Einholung von Einwilligungen ermöglichen es den Nutzern, die Souveränität ihrer eigenen Daten jederzeit zu erhalten.

DIDs vereinfachen auch die Einhaltung gesetzlicher Vorschriften. Die globale Zugänglichkeit der Blockchain optimiert die Prozesse der Nachverfolgbarkeit. Die Schaffung einer einheitlichen, manipulationssicheren digitalen Identität, die über mehrere Institute hinweg zugänglich ist, gestaltet die Verifizierung in der digitalen Welt effizienter. Audit-Trails werden als integraler Bestandteil direkt verfügbar gemacht und vereinfachen somit Audit-Verfahren erheblich.

Zudem führt die Verwendung von dezentralen Identitäten zu einer wesentlichen Vereinfachung und Beschleunigung des Identifikationsprozesses. Das resultiert in einer besseren Nutzererfahrung, da die Anzahl der Hürden und Wartezeiten bei der Verifizierung reduziert wird. Übertragbare digitale Identitäten ermöglichen es den Nutzern darüber hinaus, eine einzige DID für verschiedene Dienste zu verwenden. Gleichzeitig können unbegrenzt neue DIDs erstellt und somit die Anonymität zwischen Anwendungen und Diensten gewährleistet werden.

FAZIT

Dezentralisierte Identitäten bieten sowohl für die geplante EU-weite Implementierung als auch für Unternehmensanwendungen erhebliche Vorteile. Sie stärken die Unabhängigkeit der Nutzer und erhöhen dadurch die Sicherheit. Unternehmen profitieren von der schnellen und einfachen Überprüfung notwendiger Daten sowie der klaren und sicheren Identifizierung von Usern. So lassen sich Mitarbeiter und Kunden problemlos einbinden, ohne dass sie physisch anwesend sein müssen. Mit der Blockchain-Technologie als Grundlage könnte dies das Vertrauen in die digitale Welt steigern und es Angreifern erschweren, Schaden anzurichten. ■

MARKUS LIMBACH
ist Partner Cyber Security & Resilience bei der KPMG AG. Er verfügt über mehr als 20 Jahre Erfahrung in der Durchführung von Beratungsprojekten in den Bereichen Informationssicherheit, Business- und Technology Resilience, Risikomanagement sowie Identitäts- und Zugriffsmanagement.

MARVIN KROSCHEL
ist Manager Cyber Security & Resilience bei der KPMG AG. Er verfügt über mehr als zehn Jahre Erfahrung in der Cybersicherheitsberatung, mit einem Schwerpunkt auf Identity and Access Management und Cloud-Transformationsprojekte und ist zertifizierter Azure Solutions Architect.

Strukturierte KI-Einführung verhindert Wildwuchs

WARUM UNTERNEHMEN IHRE KI-AGENTEN WIE MITARBEITER VERWALTEN SOLLTEN

KI-Agenten greifen auf Daten zu, erledigen Aufgaben selbstständig und treffen eigenmächtig Entscheidungen. Ohne klare Regeln entstehen Schatten-KI und ein unkontrollierter Agenten-Wildwuchs, ein ernst zu nehmendes Risiko für jedes Unternehmen. Cloud- und KI-Governance – in der Vergangenheit oft verpönt und gemieden – können hier Abhilfe schaffen, indem sie die Transparenz erhöhen und dabei helfen, Sicherheitslücken zu reduzieren. Somit bilden sie die Basis für den verantwortungsvollen Einsatz von KI im Unternehmensalltag.

In vielen Unternehmen beginnt die Reise in Richtung künstlicher Intelligenz (KI) nicht mit einer großen, strategisch geplanten Einführung, sondern schleichend. Mitarbeiter nutzen frei verfügbare Tools, um ihre Arbeit zu erleichtern oder Routineaufgaben schneller zu erledigen. Diese sogenannte Schatten-KI bleibt der IT-Abteilung meist verborgen, weil sie außerhalb der offiziellen Freigaben liegt. Die Vorteile für einzelne Anwender scheinen zunächst zu überwiegen, doch gleichzeitig steigt das Risiko, dass sensible Daten unkontrolliert in externe Systeme gelangen.

Schatten-KI ist damit häufig der erste Schritt in eine Dynamik, die Unternehmen später teuer zu stehen kommen kann, denn sobald offiziell freigegebene Plattformen wie Copilot, Copilot Studio oder SharePoint Agents hinzukommen, wächst die Zahl der eingesetzten digitalen Helfer rasant. Was als einzelnes Tool beginnt, entwickelt sich schnell zu einem unüberschaubaren Netz von autonomen Agenten.

GARTNER WARNT VOR „AGENT SPRAWL“

Mit der Einführung von generativer KI in Microsoft 365, der Power Platform oder vergleichbaren Umgebungen können Mitarbeiter ohne tiefes technisches Wissen eigene Agenten erstellen. Diese Agenten führen eigenständig Prozesse aus, verarbeiten Daten und interagieren mit Systemen. Sie entstehen mit wenigen Klicks und sind sofort produktiv nutzbar.

Genau diese niedrige Eintrittsschwelle führt zu einem Phänomen, das Gartner-Analysten als Agenten-Wildwuchs (Agent Sprawl) bezeichnen. Plötzlich existieren hunderte, manchmal tausende Agenten, die keiner zentralen Stelle bekannt sind. Manche laufen im Hintergrund weiter, obwohl das Projekt, für das sie entwickelt wurden, längst beendet ist. Andere wurden von Personen erstellt, die das Unternehmen bereits verlassen haben. Wieder andere greifen auf Datenquellen zu, die eigentlich streng kontrolliert sein sollten und stellen die Informationen einem Nutzerkreis zur Verfügung, der nicht immer grundsätzlich darauf Zugriff haben sollte.

Die Gefahr ist offensichtlich: Jeder dieser Agenten ist ein potenzielles Einfallstor. Ein unkontrolliert erstellter Agent kann Daten exfiltrieren, Sicherheitsrichtlinien umgehen oder schlicht fehlerhafte Ergebnisse liefern. Spätestens wenn von Microsoft propagierte „Pay-as-you-go“-Modelle eingesetzt werden und jede Interaktion Kosten verursacht, spüren Unternehmen die Folgen auch finanziell.

COMPLIANCE-VERSTÖßE DURCH UNKLARE VERANTWORTUNG

Agenten-Wildwuchs bleibt selten ohne Folgen. Besonders heikel ist der unkontrollierte Zugriff auf vertrauliche Daten. Wenn Agenten in Microsoft Teams, SharePoint oder anderen Systemen aktiv werden, tun sie das mit den Berechtigun-

Bild: Nasira Mal - stock.adobe.com

gen ihrer Ersteller. Beim Veröffentlichen eines Agenten erhalten somit unbedacht andere Personen die gleichen Zugriffsberechtigungen. Schon ein einzelner falsch konfigurierter Agent kann dazu führen, dass vertrauliche Dokumente in einem Chat erscheinen, für den sie nicht bestimmt waren.

Ein weiteres Risiko liegt in der unklaren Verantwortung. Wer prüft, ob ein Agent noch gebraucht wird? Wer trägt die Verantwortung, wenn ein automatisierter Prozess falsche Ergebnisse liefert? Wer entscheidet, ob die entstehenden Kosten im akzeptablen Verhältnis zum Geschäftsnutzen stehen? Ohne eindeutige Zuständigkeit bleiben solche Fragen unbeantwortet und die Sicherheitsverantwortlichen stehen vor einem kaum lösbaren Problem.

Regulatorische Anforderungen wie die Datenschutzgrundverordnung (DSGVO) verschärfen die Situation zusätzlich. Agenten, die unkontrolliert personenbezogene Daten verarbeiten, können zu massiven Compliance-Verstößen führen. Gleichzeitig ist es kaum möglich, eine saubere Nachvollziehbarkeit sicherzustellen, wenn es an Inventarisierung und Lifecycle-Management fehlt.

GOVERNANCE ALS ENABLER

Viele Unternehmen betrachten Governance zunächst als Bremsklotz. Regeln und Kontrollen werden mit Einschränkungen gleichgesetzt. Doch im Kontext von KI und Agenten ist das Gegenteil der Fall. Governance ist der Schlüssel, um Schatten-KI zu verhindern und Agenten-Wildwuchs in kontrollierte Bahnen zu lenken. Governance bedeutet hier nicht, Innovation zu blockieren – sie schafft vielmehr die Rahmenbedingungen, innerhalb derer Endanwender sicher experimentieren und produktiv mit KI arbeiten können. Ohne ein Mindestmaß an Regeln läuft jedes Projekt Gefahr, im Chaos zu enden. Mit Governance hingegen wird aus der unübersichtlichen Agentenflut ein handhabbares System, das klare Verantwortlichkeiten und nachvollziehbare Prozesse kennt.

BAUSTEINE FÜR WIRKSAME KONTROLLE

Eine hilfreiche Analogie ist die Personalverwaltung. Kein Unternehmen würde neue Mitarbeiter einstellen, ohne ihre Identität zu erfassen, Rollen und Berechtigungen zuzuweisen oder regelmäßige Reviews durchzuführen. Digitale Mitarbeiter in Form von KI-Agenten verdienen dieselbe Sorgfalt.

- **Onboarding:** Bevor ein Agent produktiv eingesetzt wird, braucht es eine Freigabe. Ähnlich wie ein neuer Mitarbeiter seine Vertragsunterlagen und Zugriffsrechte erhält, muss ein Agent einen definierten Erstellungsprozess durchlaufen. Dabei wird dokumentiert, welchen Zweck er erfüllt und welche Daten er benötigt.

- **Rollenwechsel:** Ändert sich der Einsatzzweck, benötigt auch der Agent ein Update. Neue Datenquellen oder veränderte Zugriffsrechte sollten nicht unbemerkt erfolgen, sondern wie bei einer Beförderung oder Rollenänderung überprüft und genehmigt werden.

- **Offboarding:** Sobald ein Projekt endet oder ein Agent nicht mehr benötigt wird, muss er sauber stillgelegt werden. Dazu gehören das Entfernen von Zugriffsrechten, die Archivierung relevanter Ergebnisse und die Dokumentation des Offboardings.

- **Leistungsbeurteilung:** Auch Agenten sollten regelmäßig überprüft werden. Statt Zielvereinbarungsgesprächen gibt es hier Risikobewertungen, Nutzungsstatistiken und Kostenanalysen. Ein Agent, der keine Mehrwerte bietet oder Sicherheitsrisiken birgt, sollte angepasst oder entfernt werden.

Diese systematische Sichtweise macht aus unkontrolliertem KI-Wildwuchs ein beherrschbares digitales Team, in dem jeder Agent einen Platz, eine Aufgabe und eine verantwortliche Person hat.

Damit Governance ihren positiven Effekt entfalten kann, braucht es konkrete Maßnahmen:

1. **Inventar aller Agenten** als zentrales Verzeichnis, das jederzeit Auskunft gibt

2. **Klare Verantwortlichkeiten** durch Zuweisung eines Verantwortlichen

3. **Lebenszyklus-Management** mit Regeln für Onboarding, Änderungen und Offboarding

4. **Risikobewertung und Monitoring** durch kontinuierliche Analysen und automatisierte Berichte

5. **Datenhygiene** als Basis für zuverlässige Ergebnisse: Veraltete oder redundante Inhalte müssen regelmäßig entfernt werden. Besonders auch bei generativer KI wie MS Copilot, welcher auf alle dem Mitarbeiter verfügbaren Informationen zugreift.

VON REAKTIV ZU PROAKTIV

Unternehmen, die Governance ernst nehmen, verlassen die reaktive Haltung. Statt erst einzugreifen, wenn Sicherheitsvorfälle oder Kostenexplosionen eintreten, können sie von Anfang an steuern. Das bedeutet, dass Innovation nicht gebremst, sondern beschleunigt wird.

Ein proaktiver Ansatz schafft Vertrauen sowohl bei Endanwendern, die sicher mit KI experimentieren können, als auch bei Führungskräften, die den geschäftlichen Nutzen im Blick haben. Wenn klar ist, dass Agenten kontrolliert, überprüft und bei Bedarf abgeschaltet werden, steigt die Akzeptanz im gesamten Unternehmen.

Schatten-KI und Agenten-Wildwuchs sind keine theoretischen Risiken. Sie entstehen unbemerkt und entwickeln sich schnell zu einem echten Problem für Sicherheit und Compliance. Wer die Einführung von KI-Agenten ohne Regeln angeht, läuft Gefahr, die Kontrolle zu verlieren.

Die gute Nachricht ist: Governance bietet einen klaren Ausweg. Sie verhindert nicht den Fortschritt, sondern ermöglicht ihn. Wenn Agenten wie Mitarbeiter behandelt werden, mit Inventar, Verantwortlichen, Lifecycle und Reviews, wird aus einer Bedrohung ein beherrschbares System. Unternehmen können so die Chancen von KI nutzen, ohne Sicherheits- oder Compliance-Risiken in Kauf zu nehmen. ■

MATTHIAS EINIG
ist Mitbegründer und CEO von Rencore.

Rechtliche Vorsorge bei Cybervorfällen

WENN ANGREIFER DEN VERTRAG TESTEN

Cyberangriffe stellen nicht nur die IT-Sicherheit auf die Probe, sondern auch bestehende Vertragswerke. Wer seine Verträge nicht krisenfest gestaltet, riskiert erhebliche wirtschaftliche Schäden. Eine strukturierte Prüfung der wichtigsten Vertragskomponenten kann Unternehmen im Ernstfall handlungsfähig halten.

Cyberangriffe sind längst kein Ausnahmefall mehr, sondern ein absehbares Unternehmensrisiko. Ransomware-Attacken oder andere Angriffe auf IT-Systeme und der Abfluss sensibler Daten haben unmittelbare rechtliche und wirtschaftliche Folgen. Sie betreffen nicht nur unternehmensinterne Prozesse, sondern stellen auch die bestehenden Vertragswerke auf die Probe.

So kann es etwa passieren, dass ein Software-as-a-Service-(SaaS)-Dienstleister die zugesagte Verfügbarkeit nicht mehr gewährleisten kann, dass ein IT-Provider seiner Unterstützungs- und Meldepflicht nicht nachkommt oder dass eine Cyberversicherung die Schadenregulierung verweigert, weil bestimmte vertragliche Anforderungen und Sorgfaltspflichten verletzt wurden. In all diesen Fällen zeigt sich, wie krisenfest Verträge tatsächlich ausgestaltet sind.

Wer auf solche Szenarien nicht vorbereitet ist, riskiert erhebliche Schäden und Kosten, für die gegebenenfalls weder Verursacher noch Versicherer aufkommen. Daher empfiehlt es sich, Verträge frühzeitig auf ihre Tauglichkeit im Ernstfall zu prüfen und gezielt abzusichern.

VERTRÄGE ALS TEIL DER CYBERABWEHR

Cyberangriffe lassen sich kaum vollständig verhindern. Unternehmen können und müssen jedoch Vorkehrungen treffen, um im Krisenfall handlungsfähig zu bleiben. Neben technischen und organisatorischen Sicherheitsmaßnahmen gehört dazu auch die rechtliche Vorsorge – insbesondere durch eine geeignete Vertragsgestaltung und ein gutes Vertragsmanagement.

Verträge sollten daraufhin überprüft werden, ob sie Risiken im Zusammenhang mit Cyberangriffen sachgerecht abbilden. Insbesondere gilt es, zugesagte Leistungen, Unterstützungspflichten und Haftungsregelungen zu prüfen. So kann es etwa nachteilig sein, Risiken aus Cyberangriffen pauschal von der Haftung auszunehmen oder zu enge oder weite Haftungsgrenzen zu vereinbaren.

Ein häufiges Problem ist die Unmöglichkeit, vertraglich zugesicherte Leistungen während oder nach einem Angriff zu erbringen – etwa vereinbarte Verfügbarkeiten bei SaaS-Produkten zu gewährleisten. Dienstleisterkonstel-

lationen werfen zudem Fragen zu gegenseitigen Unterstützungs- und Informationspflichten auf: Wer informiert wen, wann und welche Informationen müssen die Beteiligten bereitstellen? Die vertragliche Regelung dieser Pflichten ist oft unzureichend und beschränkt sich beispielsweise auf das für Auftragsverarbeitungsverträge erforderliche Mindestmaß.

Um Datenverluste oder andere Datenschutzvorfälle zu vermeiden beziehungsweise zu begrenzen, sollten Verträge konkrete Vorgaben zu Verschlüsselungs- und Backup-Maßnahmen, Zugriffsbeschränkungen sowie eindeutige Melde- und Unterstützungsleistungen enthalten. Letztere können Aufgaben von der Bereitstellung detaillierter Informationen bis hin zu technischen Supportleistungen umfassen.

Versicherungen, die Schäden aus Cyberangriffen abdecken sollen, enthalten darüber hinaus häufig bestimmte Pflichten, Verhaltensanforderungen (Obliegenheiten) und Ausschlussregelungen, die Unternehmen genau kennen und beachten müssen.

Daher sollten insbesondere:

- Hauptleistungspflichten klar und präzise geregelt sein,
- mögliche Verfügbarkeitseinschränkungen/Ausfallzeiten durch Cyberangriffe bei Verfügbarkeitsversprechen berücksichtigt werden,
- technische und organisatorische Maßnahmen implementiert und vertraglich festgehalten werden,
- Informations- und Unterstützungspflichten eindeutig beschrieben sein und
- Versicherungsbedingungen sorgfältig geprüft werden.

Damit werden Verträge zu einem elementaren Baustein der Cyberabwehr: Sie allein können Angriffe zwar nicht verhindern, können jedoch dabei unterstützen, deren Folgen kontrollierbarer zu machen und die Handlungsfähigkeit im Ernstfall zu sichern.

TYPISCHE RISIKOFELDER UND VERTRAGSLÜCKEN

Viele Vertragswerke gehen von einem störungsfreien Betrieb aus und berücksichtigen primär wartungsbedingte Ausfallzeiten. Sie beachten jedoch nicht in ausreichendem Maße die Möglichkeit, dass Cyberangriffe erhebliche, potenziell existenzbedrohende Konsequenzen haben können.

Leistungsversprechen

Nach einem erfolgreichen Cyberangriff mit erheblichen Schäden entsteht häufig Streit darüber, was die Parteien eigentlich ursprünglich hätten tun müssen und ob dies möglicherweise den Erfolg des Cyberangriffs oder dessen schwere Konsequenzen hätte verhindern können. Deshalb sind aussagekräftige Regelungen ratsam, welche Leistungen die Parteien (unabhängig von einem Cyberangriff) erwarten können, um im Ernstfall Klarheit hierüber zu haben.

Verfügbarkeit

Auch Verfügbarkeitszusagen, beispielsweise im Rahmen von SaaS-Verträgen, die im Ernstfall eines Cyberangriffs nicht eingehalten werden können, führen mitunter dazu, dass durch die (zeitweise) Nichtverfügbarkeit von Daten oder Diensten erhebliche Schäden bei den Kunden entstehen, die möglicherweise ersetzt werden müssen. Daher ist es sinnvoll, hier mögliche Cyberangriffe bei der Kalkulation von Verfügbarkeiten zu berücksichtigen und bei Bedarf sachgerechte Sonderregelungen zu treffen.

Datenschutz

Cyberangriffe betreffen regelmäßig auch personenbezogene Daten, sodass Unternehmen auch datenschutzrechtliche Vorgaben beachten müssen. Neben den gesetzlichen Anforderungen der Datenschutzgrundverordnung (DSGVO) – wie der Pflicht zur rechtzeitigen Meldung von Datenschutzverletzungen an Aufsichtsbehörden, betroffene Personen und/oder Auftraggeber – bestehen auch vertragliche Risiken, die Standardklauseln in IT- oder SaaS-Verträgen oft nicht ausreichend abbilden.

Diese Problematiken stellen sich zwar auch außerhalb des Anwendungsbereichs des Datenschutzrechts, sind hier jedoch besonders relevant. Neben dem Datenschutzrecht kommen hier auch zahlreiche weitere Pflichten aus dem Cybersicherheitsrecht in Betracht, zum Beispiel NIS-2 und DORA.

Zu beachten sind in diesem Zusammenhang besonders:

- **Meldepflichten:** Das Datenschutzrecht ist insbesondere bei den gesetzten Fristen und der Mitteilung von Datenschutzvorfällen zwar konkret, Details in Verträgen bleiben jedoch im Zusammenhang mit diesen Pflichten oft unzureichend. Hier sollte vertraglich möglichst klar geregelt sein, wer wann wen auf welchem Wege informiert, welche Informationen hierbei im Einzelnen bereitzustellen sind und in welcher Detailtiefe dies zu erfolgen hat.

- **Unterstützungspflichten:** Auch die Frage, inwieweit ein von einem Cyberangriff betroffener Vertragspartner bei der Behebung und Folgenbeseitigung unterstützen muss, bedarf klarer Regelungen. Dies kann neben der Bereitstellung von Informationen/Zugriffsmöglichkeiten auch aktive Sicherungs- und Forensikmaßnahmen umfassen.

- **Technische Maßnahmen:** Vor allem Backups, Verschlüsselungsmaßnahmen und Zugriffsbeschränkungen sollten nicht nur umgesetzt, sondern auch vertraglich verankert sein.

- **Verantwortlichkeiten:** Verträge sollten datenschutzrechtliche Verantwortlichkeiten unmissverständlich abbilden und auch dafür sorgen, dass die nötigen Regelungen entlang der gesamten Kette von Auftragsverarbeitern funktionieren.

Haftung

Bei Cyberrisiken ist es entscheidend, die Haftung differenziert zu betrachten:

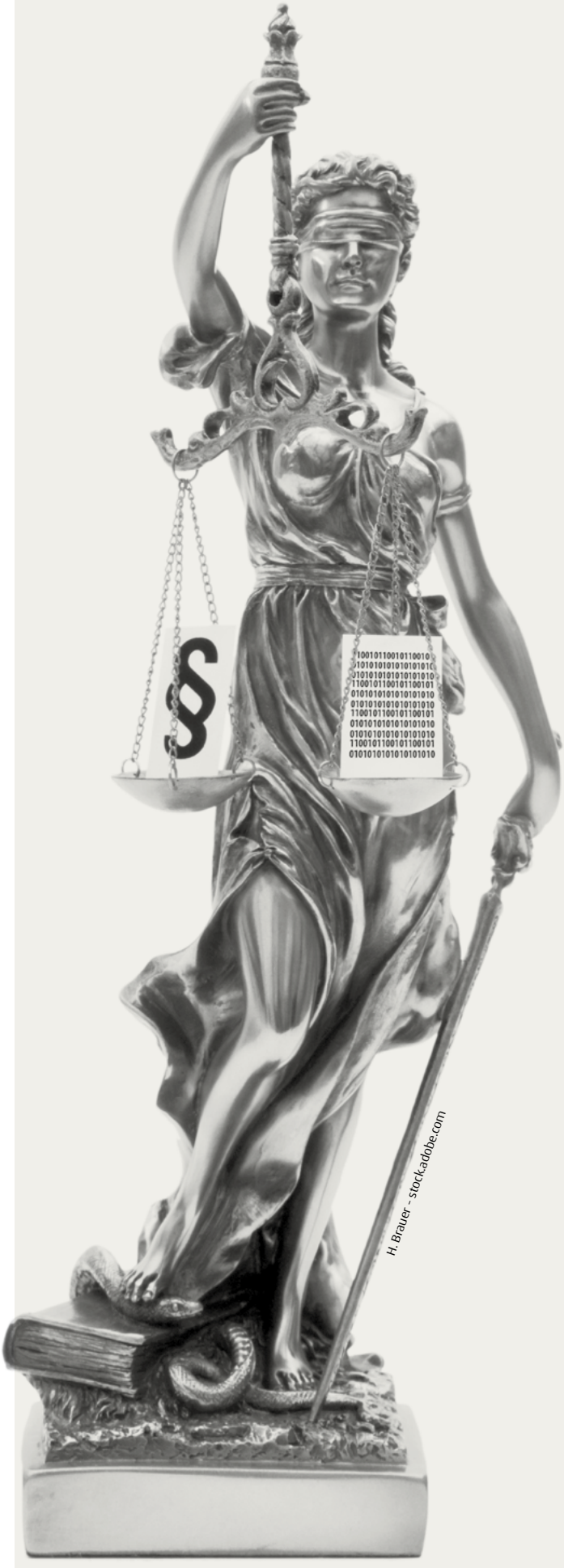
- **Schadensarten:** Bei der Verhandlung von Verträgen und insbesondere Haftungsklauseln sollten nicht nur unmittelbare Schäden berücksichtigt werden, sondern auch Folgeschäden von Cyberangriffen wie Betriebsunterbrechungen, entgangene Gewinne, Reputations- oder Drittschäden.

- **Haftungshöchstgrenzen:** Standardmäßige Limits erweisen sich häufig als nicht sachgerecht, da potenzielle Schäden schnell die vertraglich vereinbarte Summe um ein Vielfaches übersteigen können. Risikoangepasste Regelungen sind hier sinnvoll.

- **Pflichten und Obliegenheiten:** Der Umfang der Haftung kann davon abhängen, inwieweit der Vertragspartner vertraglich geregelte Pflichten und Obliegenheiten, etwa zur Implementierung von Sicherheitsmaßnahmen oder zur Erfüllung von Meldepflichten, einhält.

- **Schadensminderung:** Auch die erwartbaren Maßnahmen zur Schadensminderung sollten festgehalten werden.

Wichtig ist, dass bei Vertragsabschluss die Realitäten eines Cyberangriffs berücksichtigt und alle Pflichten und Obliegenheiten in diesem Licht sorgsam geprüft und beachtet werden, da nur so sachgerechte Regelungen getroffen werden können. Im Ernstfall kommt es vor allem darauf an, dass die Vertragsparteien ihre Pflichten kennen und befolgen, um Vertragsverletzungen und damit mögliche weitere Schäden zu vermeiden.



Cyberversicherung

Der Abschluss einer Cyberversicherung kann aufgrund der finanziellen Schäden durch einen Cyberangriff – darunter mögliche Umsatzeinbußen, Kosten für die Wiederherstellung von Systemen, Schadensersatzansprüche von Geschäftspartnern und Kunden sowie weitere Schäden – sinnvoll sein. Sie dient jedoch nur als Ergänzung und nicht als Ersatz sachgerechter technischer und organisatorischer Maßnahmen und entsprechender vertraglicher Regelungen.

CHECKLISTE: WORAUF VERTRÄGE VORBEREITET SEIN SOLLTEN

Verträge, die Risiken von Cyberangriffen nicht sachgerecht berücksichtigen, können die Parteien im Ernstfall schutzlos lassen oder unangemessen benachteiligen. Die folgende Checkliste bietet eine strukturierte Hilfestellung für die Vertragsgestaltung.

1. Hauptpflichten

Unklare Pflichten führen häufig dazu, dass die erwartete und die geleistete Leistung auseinanderfallen, was zu Streit und Beweisschwierigkeiten führen kann, wenn diese Differenz (mit-)ursächlich für einen Cyberangriff oder daraus resultierende Schäden ist.

Empfehlung: Verträge sollten (auch unabhängig von Cyberangriffen) möglichst klare Regelungen enthalten, welche Leistungen die Parteien einander schulden.

2. Verfügbarkeit und Downtimes

Verfügbarkeitszusagen gehen oft nur vom Regelfall aus und berücksichtigen mögliche Cyberangriffe nicht ausreichend.

Empfehlung: Eine vertragliche Differenzierung ist hier sachgerecht. Auch sollten Unternehmen den Krisenfall simulieren, um realistische Zusagen zur Verfügbarkeit machen zu können.

3. Haftungsregelungen

Pauschale Standardklauseln, die die Haftung für alle Fälle auf bestimmte Summen begrenzen, entsprechen den Risiken von Cyberangriffen häufig nicht.

Empfehlung: Haftungsregelungen sollten Cyberrisiken ausdrücklich berücksichtigen. Differenzierungen nach verschiedenen Schadenszenarien können sinnvoll sein.

4. Datenschutz und Meldepflichten

Cyberangriffe betreffen oft personenbezogene Daten. DSGVO-konforme schnelle Reaktionen und Meldungen sind erforderlich. Auch aus anderen Gesetzen sowie aus vertraglichen Regelungen können Meldepflichten bestehen.

Empfehlung: Pflichtenkataloge über die Meldung, Dokumentation und Unterstützung im Ernstfall sollten über den gesetzlichen Mindestinhalt hinaus konkret vereinbart werden.

5. Technische und organisatorische Maßnahmen

Die abstrakte Pflicht zur Ergreifung „angemessener" Maßnahmen ist ohne vertragliche Konkretisierung regelmäßig zu unbestimmt und erlaubt keine Angemessenheitsprüfung.

Empfehlung: Festlegung konkreter Mindeststandards und Nachweispflichten, um die Umsetzung überprüfbar zu machen.

6. Cyberversicherung

Versicherungsschutz ersetzt keine sorgfältige Vertragsgestaltung. Einschränkungen und Ausschlüsse gefährden den Versicherungsschutz.

Empfehlung: Policen und Deckungsgrenzen sollten sorgfältig geprüft und mit den Risiken ins Verhältnis gesetzt werden. Pflichten und Obliegenheiten aus dem Versicherungsvertrag sollten klar und bekannt sein und ihre Einhaltung dokumentiert werden.

Je nach Art der Versicherung kann eine Cyberversicherung verschiedene Felder abdecken, beispielsweise Kosten für

- die Deckung von Ausfällen, Eigenschäden und Haftpflichtschäden,
- den Wiederaufbau der IT-Infrastruktur,
- Rechtsberatung und Forensik,
- Ansprüche Dritter.

Zu beachten ist dabei, dass es mitunter Ausnahmeregelungen und Ausschlüsse gibt – sowohl hinsichtlich bestimmter Leistungsaspekte als auch der Höhe nach. Die Haftungssumme ist in der Regel auf einen festgelegten Betrag begrenzt.

Sowohl bei Vertragsabschluss als auch im Ernstfall müssen alle Pflichten und Obliegenheiten sorgsam geprüft und beachtet werden, da Verstöße zum teilweisen oder vollständigen Verlust des Versicherungsschutzes führen können.

Dazu gehören insbesondere:

- wahrheitsgemäße Angaben und sachgerechte Maßnahmen,
- die rechtzeitige Information und Einbindung bei Schadensfällen,
- eventuell auch die Bedingung, dass die Versicherung bei Abhilfe- und Informationsmaßnahmen ein Mitspracherecht bekommt.

EINKAUFS- UND VERTRAGSMANAGEMENT: RISIKEN FRÜHZEITIG BERÜCKSICHTIGEN

Neben der Prüfung und Anpassung von Verträgen sollten auch die Prozesse im Einkaufs- und Vertragsmanagement im eigenen Unternehmen geprüft werden. Ziel ist, dass relevante Aspekte im Zusammenhang mit Cyberangriffen und anderen sicherheits- oder datenschutzrelevanten Vorfällen ausreichend beachtet und abgebildet werden.

Bei der Auswahl und Beauftragung externer Dienstleister helfen Checklisten, Mindestanforderungen abzuprüfen. Außerdem bieten sich Standardklauseln oder Ergänzungsvereinbarungen an, um Risiken aus Cyberangriffen zu begegnen. Auch sollte ein klares Mapping von Pflichten und Obliegenheiten erfolgen, damit im Ernstfall nicht umfangreiche Vertragsdokumente geprüft werden müssen – deren Verfügbarkeit schlimmstenfalls sogar stark eingeschränkt sein kann.

Unternehmen sollten daher eine übersichtliche Zusammenfassung der Regelungen über verschiedene Verträge hinweg erstellen, um schnell handlungsfähig zu sein.

FAZIT: VERTRAGSWERKE FORTLAUFEND ANPASSEN

Wichtigste Maßnahmen gegen Cyberangriffe sind und bleiben technische und organisatorische Sicherheitsmaßnahmen sowie die Sensibilisierung von Beschäftigten. Parallel sollten Unternehmen jedoch unbedingt bestehende und neue Verträge daraufhin überprüfen, ob Pflichten und Obliegenheiten (insbesondere im Ernstfall) klar geregelt sind und ob allen Risiken, die mit Cyberangriffen einhergehen können, hinreichend Rechnung getragen wurde.

Dies sollte Hand in Hand gehen mit einer Betrachtung der entsprechenden Prozesse zur Erkennung und Behandlung von Cyberangriffen und anderen Vorfällen. Zudem müssen besonders etwaige Melde- und Informationspflichten gemäß der DSGVO eingehalten werden können.

Unternehmen sollten ihre Pflichten und Obliegenheiten kennen. Es lohnt sich also, klare Vereinbarungen zu treffen, einen Blick in (bestehende) Verträge zu werfen und diese speziell auf mögliche Risiken aus dem Kontext von Cyberangriffen zu überprüfen und bei Bedarf entsprechende (neue) Regelungen zu treffen. ■

RAPHAEL JÜNEMANN
ist Rechtsanwalt der Technologiekanzlei Schürmann Rosenthal Dreyer Rechtsanwälte und spezialisiert auf das Datenschutz- und IT-Recht. Den inhaltlichen Schwerpunkt seiner Tätigkeit bildet u. a. die Betreuung von Unternehmen und Behörden hinsichtlich der Umsetzung regulatorischer Anforderungen an die Datenverarbeitung.

www.srd-rechtsanwaelte.de

Online-Schulungen IT-Sicherheit 2025

Themen	Referenten
Einführung Notfallmanagement nach BSI-Standard 200-4	Niklas Bauer
KI im Kontext der Cybersecurity	Alexander Jaber
KI unter Kontrolle – ISO/IEC 42001 als Wegweiser für systematisches KI-Management	Hendrik Schlademann
KI-Verordnung – Geltungsbeginn am 2. Februar 2025: KI-Kompetenz und verbotene Praktiken	Alexander Forssman
Kick-Off zur KI-Verordnung – die KI-VO in aller Kürze	Alexander Forssman
Künstliche Intelligenz im Betrieb – Regulatory Mapping: (Daten-)Arbeitsrecht	Ralf Bruns, Kinga Möller
Praxisfall: Herausforderungen und Bewältigung eines Cyberangriffes – vom Angriff bis zur Abwicklung	Niklas Bauer
Quickwins für IT-Sicherheit: Sofortige Maßnahmen zur Risikoreduzierung	Alexander Jaber
ISO 27001 Foundation Kurs – PECB zertifiziert	Alexander Jaber
ISO 27001 Lead Auditor Kurs – PECB zertifiziert	Alexander Jaber
ISO/IEC 27001 Lead Implementer – PECB zertifiziert	Alexander Jaber

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

10 % Rabatt für <kes>+ Abonnenten

Der Weg zur erfolgreichen Umsetzung

INTEGRATION EINER SOFTWARE BILL OF MATERIALS IN DIE BACKEND-ENTWICKLUNG

Der Cyber Resilience Act der EU macht Software Bills of Materials ab 2027 verpflichtend. Unsere Autoren zeigen, wie mittelständische Unternehmen diese Transparenzanforderung in der Backend-Entwicklung umsetzen können.

Die moderne Softwareentwicklung ist durch hohe Komplexität, kurze Veröffentlichungszyklen und den intensiven Einsatz externer Softwarebibliotheken gekennzeichnet. In der Backend-Entwicklung spielen Frameworks, Open-Source-Komponenten und containerbasierte Technologien wie Docker oder Kubernetes eine zentrale Rolle. Diese Vielfalt an verfügbaren Softwaretechnologien trägt zwar stark zur Effizienz und Skalierbarkeit von Softwarelösungen bei, jedoch entstehen durch den Einsatz auch neue Herausforderungen. So erschwert beispielsweise die steigende Zahl externer Komponenten die Gewährleistung von Aktualität und Sicherheit sowie die Einhaltung von Lizenzbedingungen und die Risikobewertung.

Die Europäische Union hat nun die Sicherheitsanforderungen für Softwareunternehmen verschärft. Mit dem am 30. Dezember 2024 in Kraft getretenen Cyber Resilience Act (CRA) werden ab Dezember 2027 Software Bills of Materials (SBOMs) für alle betroffenen Unternehmen verpflichtend.[1]

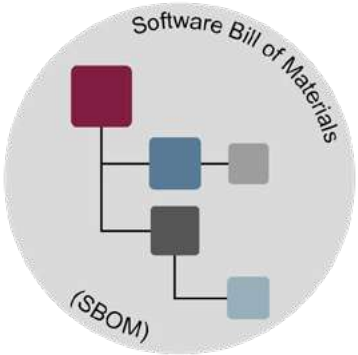


Abbildung 1: Software Bill of Materials (SBOM) (Bild: if(is))

Die Verantwortlichen für die Entwicklung stehen somit vor der komplexen Aufgabe, die Kontrolle über die eingesetzten Softwarekomponenten trotz steigender Komplexität zu behalten. In vielen Unternehmen fehlen etablierte Prozesse und Werkzeuge, um dieser Notwendigkeit und der damit verbundenen Verantwortung gerecht zu werden.

Das Risiko ist konkret: Softwareelemente oder Dienste mit veralteten Abhängigkeiten, sicherheitsrelevanten Schwachstellen oder fehlerhaften Lizenzen können in Softwareprojekte einfließen. Dies kann sich verschärfen, wenn die Software in kritischen Bereichen zum Einsatz kommt und die Dokumentation lückenhaft ist. Besonders ausgeprägt ist diese Problematik im Umfeld API-basierter Backend-Anwendungen, bei denen der Einsatz externer Komponenten und automatisierter Build-Prozesse sehr intensiv ist.

Moderne Backend-Anwendungen setzen massiv auf externe Softwarebibliotheken und Open-Source-Komponenten. Diese Abhängigkeit schafft neue Angriffsvektoren. Bei Supply-Chain-Angriffen missbrauchen Angreifer legitime Software-Updates vertrauenswürdiger Anbieter, um Kunden zu kompromittieren (siehe Abbildung 2).

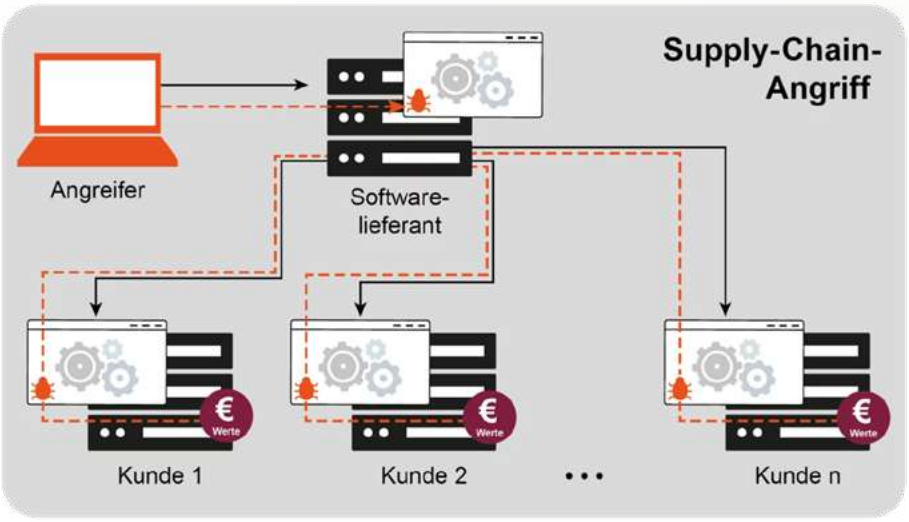


Abbildung 2: Supply-Chain-Angriff (Bild: if(is))

SBOM ALS TRANSPARENZWERKZEUG

Die Software-Lieferkette umfasst den gesamten Prozess von der Planung über die Entwicklung und Tests bis hin zur Auslieferung und Wartung einer Software. Da Unternehmen durch den Einsatz externer Komponenten ein gewisses Stück Kontrolle über ihre Software verlieren, birgt jeder Schritt potenzielle IT-Sicherheitsrisiken. Um diese Risiken beherrschbar zu machen, bietet die Software Bill of Materials ein zentrales Werkzeug.

Eine SBOM ist eine strukturierte Auflistung aller Softwarekomponenten, die konkret in einer Softwarelösung enthalten sind. Sie erfasst Informationen wie Herkunft, Version und weitere relevante Metadaten. In einer Software gibt es zwei Arten von Abhängigkeiten: jene, die explizit

Bild: Maxim - stock.adobe.com

anhand einer Syntax eingebunden werden und welche, die transitiv eingebunden werden. Diese werden in der Regel durch die explizit definierten Komponenten inkludiert.

Durch die Inklusion beider Arten entsteht eine transparente Übersicht über die Lage der eingebundenen Abhängigkeiten. Abbildung 3 verdeutlicht den systematischen Aufbau einer SBOM. Neben den Abhängigkeiten und Open-Source-Komponenten werden auch organisatorische Informationen wie „Author" und „Supplier-Name" dokumentiert [3]. Die Angabe der Versionsdefinition ermöglicht die präzise Identifikation, während Lizenzinformationen rechtliche Klarheit bringen. Eine solche umfassende Dokumentation ist besonders wichtig, wenn Sicherheitslücken auftreten und schnell geklärt werden muss, welche Komponenten betroffen sind.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterteilt SBOMs in verschiedene Kategorien.[2] Jede dieser Kategorien ist eine vollwertige Bill of Materials (BOM) mit einer anderen Detailtiefe. Dies kann für bestimmte Zwecke wichtig sein, da zu unterschiedlichen Zeitpunkten ein unterschiedlicher Grad an Informationen benötigt werden. Für die maschinenlesbare Darstellung haben sich Standards wie CycloneDX und SPDX etabliert, die jeweils feste Strukturen für die Informationsdarstellung definieren (siehe Abbildung 3).

PRAKTISCHE UMSETZUNG IN MITTELSTÄNDISCHEN UNTERNEHMEN

Doch wie lässt sich das in der Praxis umsetzen? Dazu entwickelten die Autoren ein Konzept am Beispiel eines mittelständischen Softwaredienstleisters mit etwa 200 Mitarbeitern, der sich auf digitale Lösungen für kleine und mittelständische Betriebe spezialisiert hat. Das Unternehmen führt kontinuierlich verschiedene Softwareprojekte durch – von webbasierten Verwaltungssystemen bis hin zu mobilen Anwendungen für die Auftragsverwaltung.

Aufgrund der heterogenen Kundenbasis mit unterschiedlichen Branchen und Anforderungen entstehen regelmäßig neue Entwicklungsprojekte mit diversen technischen und fachlichen Spezifikationen. Die Projekte umfassen sowohl Frontend- als auch Backend-Entwicklung und erfordern eine strukturierte Projektabwicklung sowie die sichere Integration verschiedener Softwarekomponenten.

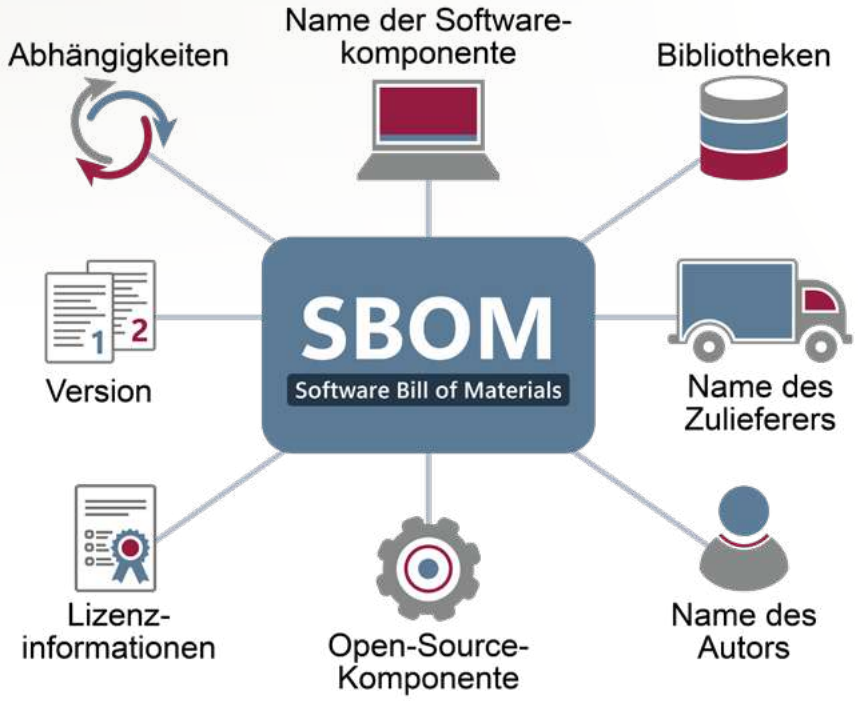


Abbildung 3: Struktur einer Software Bill of Materials (SBOM) mit den wesentlichen Komponenten und Abhängigkeiten (Bild: if(is))

HERAUSFORDERUNGEN IM ABHÄNGIGKEITS-MANAGEMENT

Das Abhängigkeitsmanagement des dargestellten Unternehmens macht die typischen Probleme mittelständischer Betriebe deutlich. Einige Teams haben bereits dynamische Prozesse etabliert, während andere noch immer einen reaktiven Ansatz praktizieren. Hier beginnt die Aktualisierung erst, wenn eine Sicherheitslücke öffentlich wird oder eine neue Version einer kritischen Komponente erscheint, und sie erfolgt ausschließlich manuell.

DAS PROBLEM DER FEHLENDEN AUTOMATISIERUNG

In der Praxis läuft die Aktualisierung von Software-Abhängigkeiten typischerweise so ab: Ein Entwickler erhält eine Meldung über eine Sicherheitslücke und führt eine manuelle Analyse durch. Dabei bewertet er die Änderungsrelevanz, prüft mögliche Kompatibilitätskonflikte und schätzt den Implementierungsaufwand ab. Erst dann fällt die Entscheidung, ob eine Aktualisierung durchgeführt wird. Dieser Prozess mag bei kritischen Sicherheitslücken mit hoher Priorität ablaufen, doch hier liegt das fundamentale Problem: Viele Schwachstellen bleiben völlig unbemerkt. Sie erhalten keine öffentliche Aufmerksamkeit, werden nicht automatisch erkannt und bleiben somit eine unkalkulierbare Bedrohung für die Systemsicherheit.

Die unstrukturierte Dokumentation von Entscheidungen verschärft das Problem zusätzlich. Wenn das Team entscheidet, eine Abhängigkeit nicht zu aktualisieren, hinterlässt es lediglich eine kurze Notiz in einem Kommunikationskanal. Detaillierte Begründungen, Risikobewertungen oder systematische Aufbereitungen für zukünftige Referenzen bleiben hingegen aus. Die Folge ist deutlich erkennbar: Unternehmen verlieren den Überblick über ihre tatsächlich verwendeten Abhängigkeiten und deren Zustand. Mit zunehmender Anzahl externer Softwarekomponenten wird das System nicht nur komplexer, sondern auch undurchsichtiger.

Die neuen Vorgaben der Europäischen Union durch den CRA stellen diese Praxis grundsätzlich infrage. Die Verordnung fordert eine kontinuierliche Aktualisierung von Software – ein Anspruch, den manuelle Prozesse strukturell

nicht erfüllen können. Besonders problematisch ist dabei, dass Sicherheitslücken dynamisch sind. Software wird niemals vollständig frei von Schwachstellen sein und das Risiko steigt exponentiell mit der Anzahl verwendeter Abhängigkeiten externer Software.

Die Folgen dieses reaktiven Vorgehens sind messbar: Längere Entwicklungszyklen, höhere Wartungskosten und vor allem ein erheblich gestiegenes IT-Sicherheitsrisiko prägen den Alltag. Was als ressourcenschonende, punktuelle Aktualisierung beginnt, entwickelt sich schnell zu einem kostspieligen Migrationsaufwand, wenn veraltete Abhängigkeiten schließlich doch aktualisiert werden müssen.

LÖSUNGSANSATZ: AUTOMATISIERTE SBOM-INTEGRATION

Die Lösung besteht in der Automatisierung des Abhängigkeitsmanagements durch die Integration einer SBOM. Aufgrund der hohen Anzahl unterschiedlicher Open-Source-Komponenten in einer Software ist eine manuelle Überprüfung nicht möglich. In diesem Zusammenhang bieten Software-Composition-Analysis-Tools eine effiziente Lösung. Sie prüfen alle Komponenten einschließlich transitiv eingebundener Abhängigkeiten automatisch und unabhängig auf IT-Sicherheitsprobleme und melden diese bei Bedarf an die verantwortlichen Entwickler.

Ein zukunftsfähiges Abhängigkeitsmanagement setzt auf kontinuierliche Überwachung und proaktive Verwaltung. Statt reaktiv auf Sicherheitslücken zu reagieren, werden Abhängigkeiten automatisch überwacht und aktualisiert. Dieser proaktive Prozess erlaubt es, potenzielle Risiken frühzeitig und kontinuierlich zu erkennen. So können Gegenmaßnahmen schneller ergriffen werden, um die Software sicherer zu machen. Darüber hinaus stellt dieser Ansatz einen entscheidenden Baustein zur Erfüllung regulatorischer Anforderungen dar.

SBOM-INTEGRATION: KONZEPTION UND IMPLEMENTIERUNG

Die Integration einer Software Bill of Materials in bestehende Entwicklungsprozesse erfordert eine strukturierte Herangehensweise, die technische und organisatorische Aspekte gleichermaßen berücksichtigt. Während die Notwendigkeit von SBOMs durch regulatorische Anforderungen wie den CRA immer deutlicher wird, zeigt sich in der Praxis oft eine Kluft zwischen Theorie und Umsetzung.

Rahmenbedingungen

Für die Umsetzung eines Projekts, das eine SBOM-Definition darstellt, sind verschiedene Voraussetzungen zu erfüllen, die für eine spätere Integration maßgeblich sind. Zunächst müssen alle Abhängigkeiten, welche inkludiert werden sollen, vollständig bekannt sein. Darüber hinaus ist sicherzustellen, dass diese Software-Bibliotheken für eine festgelegte Java-Version verfügbar sind, da Inkompatibilitäten andernfalls zu Problemen bei der Nutzung führen können. Ebenso ist ein konsistentes Schema für die Versionierung erforderlich, um die Nachvollziehbarkeit und Wartbarkeit zu gewährleisten. Zusätzlich muss die erzeugte BOM in einem unternehmensinternen Artefakt-Repository veröffentlicht werden, sodass sie zentral zur Verfügung steht. Schließlich sollte die Projektstruktur den Konventionen eines üblichen Entwicklungsprojektes folgen, um eine reibungslose Einbindung zu ermöglichen.

Zentrale SBOM-Definition

Der erste Schritt ist die Erstellung einer Software Bill of Materials in einem separaten Repository auf der genutzten Codeverwaltungsplattform. Da es sich um eine BOM handelt, die in der Entwicklung zum Einsatz kommen soll, muss eine Source-SBOM erstellt werden. Diese wird über eine Build-Konfiguration generiert und beinhaltet alle verwendeten Abhängigkeiten. Dadurch gibt es eine zentrale Referenz, auf die alle Projekte zugreifen können, ohne die Version manuell definieren und inkludieren zu müssen. So können Inkonsistenzen zwischen den Projekten vermieden werden. Darüber hinaus ist es möglich, andere Versionen zu nutzen, wenn dies erforderlich ist.

Die Grundlage einer effektiven SBOM-Implementierung bildet die zentrale Verwaltung aller Software-Abhängigkeiten. Anstatt Software-Bibliotheken dezentral in einzelnen Modulen zu definieren, wird ein zentraler Versionskatalog etabliert. Die Konfiguration erfolgt über spezielle Projektdateien, die sowohl den Versionskatalog als auch die Plattformkonfiguration und Veröffentlichungsschritte definieren. Alle definierten Abhängigkeiten können dann über einheitliche Referenzen in die eigentliche SBOM eingebunden werden. Diese zentrale Struktur gewährleistet Konsistenz und erleichtert die Wartung erheblich.

Automatisierte Aktualisierung und Dependency-Updates

Ein kritischer Punkt stellt die Automatisierung von Abhängigkeits-Updates dar. Die kontinuierliche Aktualisierung von Software-Abhängigkeiten

Bild: Bartek - stock.adobe.com

```
{
  "$schema": "https://docs.renovatebot.com/renovate-schema.json",
  "extends": [
    "config:recommended"
  ],
  "labels": [
    "Renovate"
  ],
  "rebaseWhen": "conflicted"
}
```

Abbildung 4: Beispielhafte Konfiguration für Renovate als Json-Datei (Bild: if(is))

ist eine zentrale Herausforderung moderner Entwicklung. Tools wie Renovate [4] können diesen Prozess automatisieren, müssen jedoch entsprechend konfiguriert werden. Die Kernaufgabe besteht darin, die Abhängigkeiten kontinuierlich zu analysieren und auf Aktualisierungen zu prüfen.

Sobald eine neue Version erkannt wird, erstellt das Tool automatisch einen Pull Request auf der Code-Verwaltungsplattform. Entwickler können diese Änderungen prüfen und freigeben, ohne manuell nach Updates zu suchen. Dies beschleunigt die Reaktion auf sicherheitsrelevante Schwachstellen erheblich. Nach der Einrichtung können Sicherheitspatches automatisch integriert werden, während größere Updates den bewährten Review-Prozess durchlaufen.

Diese Automatisierung ist für SBOM-Implementierungen besonders wertvoll, da sie sicherstellt, dass dokumentierte Abhängigkeiten nicht nur vollständig, sondern auch aktuell bleiben. Dies ist eine Grundvoraussetzung für regulatorische Compliance. Eine minimale Konfiguration demonstriert, wie unkompliziert sich dieser Prozess implementieren lässt (siehe Abbildung 4).

Die dargestellte Konfiguration aktiviert automatisch bewährte Regeln für Sicherheitsupdates, während das Labeling eine klare Nachverfolgbarkeit für Compliance-Zwecke gewährleistet. Durch die automatische Aktualisierung bleiben sowohl die tatsächlichen Abhängigkeiten als auch deren Dokumentation im SBOMs synchron. Je nach Tool lassen sich weitere Schritte konfigurieren, um beispielsweise die Freigabe von Updates zu automatisieren.

Zentrale Bereitstellung der BOM

Um eine breite Konsistenz zu erreichen, ist eine zentrale Bereitstellung von SBOM unerlässlich. Unternehmen veröffentlichen ihre SBOM in der Regel über zentrale Repository-Systeme, die bereits für die Verteilung anderer Software-Artefakte genutzt werden. Dies lässt sich über ein firmeninternes Repository lösen, das über eine Plattform wie Azure oder Alternativen bereitgestellt ist.

Dabei wird die SBOM wie ein reguläres Software-Paket behandelt und durchläuft dieselben Veröffentlichungsprozesse. Diese Integration in bestehende Infrastrukturen minimiert den zusätzlichen Aufwand und gewährleistet eine konsistente Handhabung. So können alle Teams auf dieselbe Grundlage zugreifen und erhalten eine solide und aktuelle Versionsdefinitionsbasis.

Die zentrale Verfügbarkeit ermöglicht es verschiedenen Stakeholdern, von Entwicklungsteams über Security-Verantwortliche bis hin zu Compliance-Teams auf die aktuellen SBOM-Informationen zuzugreifen. Diese Zentralisierung vereinfacht nicht nur die Qualitätssicherung, sondern ermöglicht auch eine skalierbare Umsetzung in größeren Organisationen. Dies schafft die notwendige Transparenz für fundierte Entscheidungen bezüglich Sicherheit, Lizenzkonformität und Abhängigkeitsmanagement.

FAZIT

Die Integration einer Software Bill of Materials in bestehende Entwicklungsprozesse ist machbar und bringt erheblichen Mehrwert: mehr Transparenz, höhere IT-Sicherheit, effizienteres Abhängigkeitsmanagement und bessere Compliance. Besonders der Einsatz automatisierter Tools reduziert den manuellen Aufwand und sorgt für zeitnahe Updates. So entstehen Freiräume für qualitätsfördernde Aufgaben wie Code-Reviews, Tests oder Architekturverbesserungen – ein klarer Beitrag zur Softwarequalität.

Ein weiterer Erfolgsfaktor ist die projektübergreifende Wiederverwendung. Sie gelingt nur mit einheitlichen Standards; andernfalls steigt der Anpassungsaufwand. Aus betriebswirtschaftlicher Sicht amortisieren sich die Implementierungskosten durch eingesparte Wartungszeit und eine gestärkte Compliance.

Insgesamt ist die SBOM-Integration weit mehr als ein Compliance-Thema: Sie ist eine Investition in eine nachhaltige, transparente und wartbare Software-Architektur. ■

STEFFEN WONNING
studiert an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Software Bill of Materials (SBOM)“.

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] *Europäische Union: Cyber Resilience Act (CRA), https://it-sicherheit.de/ratgeber/it-sicherheitsgesetze/cra/*

[2] *Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie BSI-TR-03183-2, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=6*

[3] *Scribe Security: What is a Software Bill of Materials (SBOM), https://scribesecurity.com/sbom/#definition-of-software-bill-of-materials*

[4] *Mend (Renovate): Renovate Documentation, https://docs.renovatebot.com/*

Besuchen Sie uns auf der it-sa 2025 Halle 7 Stand 106

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

VORSCHAU Ausgabe 6|25 DEZEMBER/ JANUAR

SCHWERPUNKT: Identity- und Access-Management

Digitale Identitäten sind längst zum Kern moderner Sicherheitsarchitekturen geworden. In einer Arbeitswelt, die von Cloud-Diensten, Homeoffice und mobilen Endgeräten geprägt ist, entscheidet das Management von Identitäten und Zugriffsrechten über Sicherheit, Compliance und Effizienz.

Das kommende Heft widmet sich den aktuellen Entwicklungen im Identity- und Access-Management:

- Zero Trust als strategischer Rahmen für Vertrauen ohne Vorschuss
- Moderne Authentifizierungs- und Autorisierungsverfahren von Passkeys bis Biometrie
- Die praktische Umsetzung von Single-Sign-on-Lösungen im Unternehmensalltag

Darüber hinaus ist vorgesehen, auch Themen wie Identity Governance – als Instrument für die regelkonforme Vergabe von Rechten – sowie cloudbasierte IAM-Plattformen in den Blick zu nehmen, die mit Skalierbarkeit und Flexibilität für komplexe Infrastrukturen werben.

Erscheinungstermin: 3. Dezember 2025

IN UNSEREM VERLAG ERSCHEINEN AUßERDEM NOCH FOLGENDE ZEITSCHRIFTEN

IT-SICHERHEIT
Management und Technik

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

Chefredaktion:
Sebastian Frank (S.F.)
(verantwortlich für den redaktionellen Teil)
E-Mail: s.frank@kes.de

Online-Redaktion:
Jessica Herz (Leitung Online)
E-Mail: herz@datakontext.com
Lisa Bieder
Konstantin Falke
Silvia Klüglich
Janek Mazac
Philip Meyer
Chiara Schönbrunn

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
E-Mail: torid.kehmeier@datakontext.com

Hersteller:
DATAKONTEXT GmbH
Augustinusstraße 11 A, 50226 Frechen

Kontakt und Informationen zum Thema Produktsicherheitsverordnung:
Dieter Schulz
Tel.: +49 2234 98949-99
E-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)

© DATAKONTEXT
Mit Namen gekennzeichnete Beiträge stellen nicht unbedingt die Meinung der Redaktion oder des Verlages dar. Für unverlangt eingeschickte Manuskripte übernehmen wir keine Haftung. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Verfasser alle Rechte, einschließlich der weiteren Vervielfältigung zu gewerblichen Zwecken. Die Zeitschrift und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

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: ©Gorodenkoff, AdobeStock & ConSense GmbH

Fotos: Firmenbilder; NürnbergMesse/Thomas Geiger, NürnbergMesse/Frank Boxler; ConSense GmbH; F24; if(is); ChatGPT Image; (Arsyifa, Bartek, Deemerwha studio, Digital Vision Lab, Fazla, fotografiedk, Gorodenkoff, H. Brauer, ImageFlow, Intelligent Horizons, Jah_CK, Johannes, KamStudio, Kunchan, Malambo C/peopleimages.com, Maxim, MD NAZMUL, Nasira Mai, Papisut, qunoo, Vera, Vladislav) - stock.adobe.com

31. Jahrgang 2025 · ISSN: 1868-5757

<kes>+

Die Zeitschrift für
Informations-Sicherheit

Mehr wissen mit <kes>+

Sichern Sie sich Ihren Wissensvorsprung in der Informationssicherheit!

- Fachzeitschrift <kes> inkl. Specials 6x jährlich per Post und digital.
- Zugang zu aktuellen Online-Fachartikeln und Studien sowie zu dem kompletten Online-Archiv.
- Exklusiver Zugriff auf über zwanzig neue Online-Premium-Artikel pro Monat sowie auf aktuelle Videos und Webinaraufzeichnungen.
- 10 % Rabatt auf DATAKONTEXT-Online-Schulungen im Bereich Informationssicherheit.
- nur 199,– € im Jahr
  (inkl. Mwst. und Versand)

Jetzt 30 Tage kostenfrei testen:
www.kes-informationssicherheit.de

<kes>

DATAKONTEXT

Wir erreichen Verantwortliche für die IT-Sicherheit

- Newsletter
- Content-Marketing
- Webinare & Webkonferenzen

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

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