HZ219241 · ISSN 1868-5757 · www.itsicherheit-online.com April/Mai **2/2026**

IT-SICHERHEIT

Management und Technik

Schwerpunkt Operational Technology

Active Directory in der Produktion

Vom Verwaltungswerkzeug zur kritischen Infrastruktur

■ **Blind im eigenen Haus:** Warum OT-Netze Angreifer nicht sehen

Supply-Chain-Governance
Vom Fragebogen zum geschlossenen Regelkreis

Letzte Linie
Warum Immutable Backups angreifbar bleiben

Ausgebrannt an der Cyberfront
Wenn Erschöpfung zum Sicherheitsrisiko wird

DATAKONTEXT

Bild: Adobe Stock/ImageKing

Jetzt downloaden und für 0,- Euro informieren!

<kes>-Special: NIS-2 – Lösungen und Services

NIS-2 fordert IT-Abteilungen heraus: Angriffserkennung, Compliance und Resilienz müssen zusammenspielen. Im <kes> NIS-2-Special erfahren Sie, wie Ihre IT mit den richtigen Tools NIS-2 effizient umsetzt und Strafzahlungen vermieden werden.

Schwerpunkte:

- ✓ NIS-2 umsetzen mit Multi-Compliance-Framework
- ✓ TopEase bündelt NIS-2-Compliance und digitale Resilienz: Governance, Risk und Compliance aus einer Hand
- ✓ NIS-2-konforme Angriffserkennung mit der ScanBox Software
- ✓ Software ibi systems iris unterstützt Unternehmen bei der NIS-2-Umsetzung
- ✓ NIS-2: Mehr als eine Checkliste – Warum echte Resilienz jetzt zum entscheidenden Wettbewerbsvorteil wird

Jetzt downloaden: **www.kes-informationssicherheit.de/NIS-2-Special**

Liebe Leserinnen, liebe Leser,

in dieser Ausgabe liegt unser Schwerpunkt auf der Sicherheit industrieller Infrastrukturen und auf der Frage, warum dort grundlegende Schutzmaßnahmen oft fehlen. Der Cyberangriff auf polnische Energieversorger Ende 2025 ist dafür ein instruktives Beispiel. Die Angreifer bewegten sich rund neun Monate unentdeckt durch die Netze, obwohl ein Erkennungssystem längst Alarm geschlagen hatte. Das eigentliche Problem war, dass schlicht niemand die Logs auswertete (Seite 20). Aktuelle Analysen deuten darauf hin, dass solche Zustände vielerorts anzutreffen sind: In mehr als 90 Prozent der untersuchten OT-Netze fanden sich veraltete Firmware, schwache Authentifizierung oder fehlerhafte Konfigurationen.

Eng damit verknüpft ist die Rolle von Active Directory (AD) in Produktionsumgebungen. Was als Verwaltungswerkzeug begann, ist in vielen Anlagen längst Teil der sicherheitskritischen Infrastrukturkomponente. Dadurch entstehen Angriffspfade von der Büro-IT bis in die Steuerungstechnik. Unser Autor zeigt ab Seite 16, mit welchen Architekturansätzen sich diese Abhängigkeit begrenzen lässt. Meine Empfehlung nach der Lektüre des Artikels: Prüfen Sie, ob Ihr AD in der Produktionsumgebung wirklich so isoliert ist, wie Sie annehmen.

Hinzu kommt der regulatorische Druck. NIS-2, KRITIS-Dachgesetz und EU AI Act treffen den industriellen Mittelstand gleichzeitig – auf technischer, physischer und organisatorischer Ebene. Wer die Anforderungen isoliert umsetzt, verbraucht knappe Ressourcen mehrfach. Ein integrierter Governance-Ansatz kann das verhindern, setzt aber voraus, dass Unternehmen zuerst ihre Strukturen klären, bevor sie Werkzeuge einführen. Warum diese Reihenfolge auch für Lieferantenbeziehungen gilt, zeigt der letzte Teil unserer Serie „Von der Norm zur Wirkung": Lieferantenmanagement ist längst kein Einkaufsprozess mehr, sondern Teil der strategischen Steuerungsarchitektur (Seite 42).

Auch der Cyber Resilience Act wird in diesem Jahr konkret: Ab September 2026 müssen Hersteller vernetzter Produkte aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle melden, ab Dezember 2027 gilt die Verordnung vollständig. Wer Melde- und Updateprozesse jetzt aufsetzt, vermeidet spätere Nacharbeit unter Zeitdruck (Seite 54).

Bei einem anderen Thema im Heft rate ich zur Neugier, aber nicht zur Euphorie: Wie gut sind KI-Agenten mittlerweile beim Penetrationstest? Forscher der Stanford University haben KI-Systeme gegen menschliche Pentester in einem echten Unternehmensnetzwerk antreten lassen – keine Sandbox, keine Capture-the-Flag-Übung, sondern ein Universitätsnetz mit 8.000 Hosts. Das beste KI-System übertraf neun von zehn menschlichen Testern und kostete einen Bruchteil. Der Befund verdient allerdings eine genaue Einordnung: Die Stichprobe war klein, die Verteidiger griffen nicht aktiv ein, und grafische Oberflächen blieben für die KI ein blinder Fleck. Für kleinere Unternehmen, die sich regelmäßige professionelle Tests schlicht nicht leisten können, könnten solche Werkzeuge dennoch interessant werden (Seite 10).

Zum Schluss noch ein Thema, das selten auf Titelseiten steht, aber viele Fachleute betrifft: Burnout in der Cybersicherheit. Stress und Erschöpfung sind längst keine individuellen Probleme mehr – sie gefährden die Handlungsfähigkeit ganzer Teams. Wenn Erschöpfung zum Sicherheitsrisiko wird, braucht es mehr als Resilienz-Tipps: Es braucht eine Unternehmenskultur, die nachhaltige Arbeitsbelastung ernst nimmt (Seite 34).

Ich wünsche Ihnen eine anregende Lektüre!
Ihr Sebastian Frank

www.itsicherheit-online.com/newsletter

INHALT

16 **SCHWERPUNKT**
ACTIVE DIRECTORY IN PRODUKTIONSNETZEN
VOM VERWALTUNGSWERKZEUG ZUR KRITISCHEN INFRASTRUKTUR

SOUVERÄNE CYBERSICHERHEIT

CrowdStrike und Schwarz Digits haben eine langfristige strategische Partnerschaft geschlossen. Die CrowdStrike-Falcon-Plattform soll künftig über STACKIT bereitgestellt werden, die innerhalb der EU betriebene Cloud-Infrastruktur von Schwarz Digits. Europäische Unternehmen und öffentliche Institutionen könnten damit KI-native Sicherheitsfunktionen nutzen und gleichzeitig die Anforderungen an Datenhoheit erfüllen, so die Partner.

Die Telemetrie- und Erkennungsverarbeitung für STACKIT-Installationen erfolge in europäischen Rechenzentren und unterstütze die Einhaltung der Datenschutz-Grundverordnung (DSGVO), des Cyber Resilience Acts und weiterer regulatorischer Standards. Zu den ersten gemeinsamen Lösungen zählen den Unternehmen zufolge ein Secure Enterprise Browser sowie ein KI-basiertes SIEM. Die Unternehmen der Schwarz Gruppe konsolidieren zukünftig ihre Cybersicherheitslösungen auf der Falcon-Plattform. „Digitale Souveränität ist kein theoretisches Konzept, sondern ein entscheidender Faktor für die Wettbewerbsfähigkeit Europas im KI-Zeitalter", so Rolf Schumann, Co-CEO von Schwarz Digits. ■

Partnerschaft besiegelt: Christian Müller (Schwarz Digits), Daniel Bernard (CrowdStrike) und Rolf Schumann (Schwarz Digits) (v.l.n.r.) (Bild: CrowdStrike/ Schwarz Digits)

GOOGLE SCHLIEßT ÜBERNAHME VON WIZ AB

Google hat die Übernahme der Cloud-Sicherheitsplattform Wiz abgeschlossen. Wiz wird Teil von Google Cloud, behält aber eigenen Angaben zufolge Marke und Multicloud-Ansatz bei. Die Wiz-Produkte sollen weiterhin auf Amazon Web Services, Microsoft Azure und Oracle Cloud funktionieren.

Gemeinsam wollen Google Cloud und Wiz eine KI-gestützte Sicherheitsplattform bereitstellen, die Bedrohungen über Code, Cloud und Laufzeitumgebungen hinweg erkennen und abwehren soll. „Durch die Zusammenführung von Wiz und Google Cloud machen wir es leichter für Unternehmen, Innovationen mit Zuversicht voranzutreiben", sagte Google-CEO Sundar Pichai. Wiz zählt nach Unternehmensangaben 50 Prozent der Fortune-100-Unternehmen zu seinen Kunden. ■

FORSCHUNGSINFRASTRUKTUR FÜR NETZWERKFORENSIK BEI 800 GBIT/S

Die Fachhochschule Dortmund baut mit dem Projekt C²PANDA (Competence Center for Packet Acquisition and Network Data Analysis) eine bundesweit einzigartige Testumgebung für IT-Sicherheit und digitale Forensik auf. Das Land NRW fördert das Vorhaben mit 2,95 Millionen Euro aus dem Europäischen Fonds für regionale Entwicklung (EFRE).

Die Infrastruktur soll Datengeschwindigkeiten von bis zu 800 Gigabit pro Sekunde erreichen – das Achtfache heutiger Rechenzentrumsstandards. „Niemand weiß derzeit, wie sich Sicherheitsmechanismen bei extrem hohen Datengeschwindigkeiten verhalten", erläutert Projektleiter Prof. Dr. Daniel Spiekermann. Partner sind unter anderem G DATA Advanced Analytics, Neox Networks, die Cybersense GmbH und das Landeskriminalamt Niedersachsen. Entwickelte Werkzeuge sollen als Open-Source-Lösungen veröffentlicht werden. Das Projekt läuft bis 2028. ■

GRC-PARTNERSCHAFT ADRESSIERT NIS-2 IN DER ÖFFENTLICHEN VERWALTUNG

Der GRC-Softwareanbieter HiScout und die Management- und Technologieberatung BearingPoint kooperieren strategisch, um Organisationen der öffentlichen Hand bei Informationssicherheit, Business Continuity Management (BCM), Datenschutz und Compliance zu unterstützen. Beide Partner arbeiten bereits in Projekten in Baden-Württemberg zusammen und wollen das Modell auf weitere Bundesländer ausweiten.

Die Partnerschaft adressiere insbesondere regulatorische Anforderungen wie NIS-2, so die Unternehmen. „Die öffentliche Hand steht vor der Herausforderung, steigende regulatorische Anforderungen mit begrenzten Ressourcen umzusetzen", sagte Tom Lienhart, Geschäftsführer von HiScout. ■

SCHWACHSTELLEN-KONTEXT UM ENTWICKLUNGSURSPRUNG ERWEITERT

Checkmarx und Archipelo haben eine Technologiepartnerschaft geschlossen. Sie soll Erkenntnisse über Anwendungsschwachstellen mit Informationen zum Entwicklungsursprung korrelieren – also nachvollziehbar machen, welche Identität eine Codeänderung initiiert hat, ob KI-Tools beteiligt waren und unter welchen Workflow-Bedingungen der Code entstand.

Archipelo bietet Developer Security Posture Management (DevSPM), Checkmarx liefert Application Security Testing und Application Security Posture Management (ASPM). „Vulnerability Detection zeigt, dass ein Risiko existiert. Der Entwicklungskontext zeigt, wie die Änderung ins System gelangt ist", erklärte Matthew Wise, CEO von Archipelo. Der Ansatz soll Remediation-Entscheidungen auf Grundlage konkreter Entstehungsinformationen ermöglichen, statt auf nachträgliche Rekonstruktionen angewiesen zu sein. ■

ÜBERNAHME STÄRKT DIGITALE IDENTITÄTSLÖSUNGEN FÜR US-REGIERUNG

Giesecke+Devrient (G+D) hat die Übernahme des US-Unternehmens XTec abgeschlossen. XTec ist auf Identitätsmanagement, Authentifizierung und Zugangsverwaltung für US-Bundesbehörden spezialisiert und betreibt nach eigenen Angaben das einzige Identity- und Credential-Management-Ökosystem mit FedRAMP-High-Impact-Zulassung – der höchsten Sicherheitskategorie des US-Regierungsprogramms „Federal Risk and Authorization Management Program" (FedRAMP).

Das Geschäft von XTec wird Teil des Portfolios von Veridos, dem Joint Venture von G+D und der Bundesdruckerei. G+D erwirtschaftete 2024 einen Umsatz von 3,1 Milliarden Euro und beschäftigt mehr als 14.000 Mitarbeiten in 41 Ländern. ■

PARTNERSCHAFT SOLL KI-INFRASTRUKTUREN ABSICHERN

PNY Technologies und F5 haben eine Partnerschaft für die EMEA-Region geschlossen. Ziel sei es, Unternehmen einen besseren Zugang zu Lösungen für Anwendungssicherheit, Traffic-Management und Leistungsoptimierung in Cloud- und Hybridumgebungen zu ermöglichen. Die F5 Application Delivery and Security Platform (ADSP) soll das KI-Infrastrukturangebot von PNY ergänzen. PNY will sein Partnernetzwerk und seine logistischen Kapazitäten nutzen, um die Implementierung der F5-Lösungen für Unternehmen und Service Provider zu erleichtern. ■

CYBERSECURITY-PLATTFORM EXPANDIERT NACH TSCHECHIEN UND IN DIE SLOWAKEI

Der Jenaer Cybersecurity-Anbieter Enginsight baut seine Präsenz in Mittelosteuropa aus. Seit dem 15. März verantwortet Ondřej Vlach als Business Development Manager den Marktaufbau in Tschechien und der Slowakei. Vlach war zuvor unter anderem für Sophos, Cohesity und Veeam tätig. Enginsight verfolgt in beiden Ländern eine Channel-Strategie und arbeitet bereits mit dem lokalen Distributor Annex NET zusammen. Die Nachfrage werde dem Unternehmen zufolge durch regulatorische Anforderungen wie NIS-2 getrieben: Viele Mittelständler müssten ihre Sicherheitsarchitekturen modernisieren, verfügten aber nicht über eigene Security-Teams. Die in Deutschland entwickelte All-in-One-Plattform soll Schwachstellenmanagement, Monitoring, Angriffserkennung und SIEM in einer Lösung bündeln. ■

BKA FEIERT 75-JÄHRIGES BESTEHEN MIT FOKUS AUF CYBERCRIME-ABWEHR

Das Bundeskriminalamt (BKA) begeht 2026 sein 75-jähriges Jubiläum. Am 12. März fand der offizielle Festakt in Wiesbaden statt. Seit seiner Gründung 1951 habe die Behörde ihre Aufgaben stetig an neue Herausforderungen angepasst – von der Bekämpfung des politischen Extremismus bis zur Abwehr internationaler Cyberbedrohungen.

Heute stehen Cyberkriminalität und digitale Ermittlungsarbeit im Fokus. Das BKA betreibt eine leistungsfähige IT-Infrastruktur, nutzt KI-basierte Anwendungen und erstellt Lagebilder zu Phänomenen wie Cybercrime. Mehr als 9.000 Mitarbeiter aus über 70 Berufen arbeiten laut BKA-Präsident Holger Münch daran, „Kriminalität zu bekämpfen und Gefahren abzuwehren – im Inland und Ausland, analog und digital". ■

QUANTENRESISTENTE FUNKGERÄTE IN ENTWICKLUNG

Elbit Systems Deutschland und genua, ein IT-Sicherheitsspezialist aus der Bundesdruckerei-Gruppe, haben eine strategische Entwicklungspartnerschaft vereinbart. Als erstes Projekt entwickeln die Partner robuste Funkgeräte mit hardwarebeschleunigter, quantenresistenter Verschlüsselung für Streitkräfte, Sicherheitsdienste und Rettungsorganisationen in ausgewählten NATO- und EU-Staaten.

Die Systeme sollen auf einsatzerprobter Technik basieren. Gemeinsame Entwicklungsteams entstehen an den Standorten Kirchheim bei München und Ulm. „Zwei starke Partner bündeln ihr Know-how, um ein sehr leistungsfähiges Funkgerät durch den Einsatz modernster Verschlüsselungstechnologien noch sicherer zu machen", erklärte Marian Rachow, CEO von Elbit Systems Deutschland. ■

Elbit Systems Deutschland und genua entwickeln Funkgeräte für quantensicher verschlüsselte Kommunikation. (Bild: Elbit Systems Deutschland GmbH & Co. KG)

KI-GESTÜTZTE SOC-AUTOMATISIERUNG JETZT AUCH IN DACH VERFÜGBAR

Die Infinigate Group und Torq weiten ihre bestehende europäische Partnerschaft auf Deutschland, Österreich und die Schweiz aus. Torq bietet eine KI-gestützte Plattform für Security Operations Center (SOC), die irrelevante Warnmeldungen herausfiltern, reale Risiken autonom priorisieren und die Reaktionszeit verkürzen soll – ohne zusätzliches Personal. Dem Anbieter zufolge sind die KI-Agenten von Torq für den Self-Service konzipiert: Sicherheitsteams könnten mit minimalem Aufwand spezialisierte Agenten bereitstellen. Die Plattform ermögliche es, bis zu 100-mal mehr Alarme zu verwalten und verkürze die Untersuchungszeit um bis zu 90 Prozent. Torq zählt eigenen Angaben zufolge Fortune-500-Unternehmen zu seinen Kunden. ■

NEUE ABWEHRFUNKTION IN **SASE-PLATTFORM**

Cato Networks hat mit Cato Dynamic Prevention eine autoadaptive Engine zur Bedrohungsabwehr vorgestellt, die nativ in die Cato-Secure-Access-Service-Edge-(SASE)-Plattform integriert ist. Die Lösung korreliere nach Herstellerangaben kontinuierlich über Monate gesammelte Sicherheits- und Netzwerktelemetriedaten und soll so verhaltensbasierte Bedrohungen identifizieren, die isoliert betrachtet harmlos erscheinen.

Erkennt die Engine böswilliges Verhalten, passe die Plattform automatisch Sicherheitsrichtlinien an und blockiere risikoreiche Aktivitäten – ohne manuelles Eingreifen des Security Operation Centers (SOC). Damit adressiert Cato eine bekannte Lücke: Angreifer führen unauffällige Einzelaktionen aus und missbrauchen legitime Tools, sodass punktuelle Sicherheitslösungen versagen. Gartner zufolge fehlen 61 Prozent der Unternehmen Vollzeit-Experten für die Bedrohungssuche.

Dass der Ansatz in der Praxis funktionieren kann, soll das Beispiel Swissport zeigen: Der Bodenabfertigungsdienstleister betreibt eigenen Angaben zufolge über 360 Standorten weltweit mit mehr als 26.000 Nutzern auf der Cato-Plattform. „In einer solchen Umgebung wirkt sich eine verzögerte Erkennung direkt auf unsere Reaktionsfähigkeit aus", so CISO Giles Ashton-Roberts. ■

KI-ASSISTENT SOLL RICHTLINIENEMPFEHLUNGEN IN SEKUNDEN ERSTELLEN

Forcepoint hat seine Data Security Cloud um den KI-Assistenten ARIA erweitert. Der Adaptive Risk Intelligence Assistant soll natürliche Sprache verstehen, Schutzlücken identifizieren – etwa durch neue Copilots, die bestehende Richtlinien nicht abdecken – und binnen Sekunden Policy-Empfehlungen inklusive Begründungen liefern.

Ein neuer Endpoint-Agent soll zudem adaptiven Schutz direkt auf Endgeräte bringen, ohne Datenverkehr über einen Proxy zu leiten. Die Plattform vereine Data Security Posture Management (DSPM), Data Loss Prevention (DLP), Data Detection and Response (DDR) sowie Web- und E-Mail-Security unter einem Richtlinien-Framework, so Forcepoint. ■

FORTIOS 8.0 ADRESSIERT KI-KONTROLLEN, SASE UND POST-QUANTUM-SCHUTZ

Fortinet hat mit FortiOS 8.0 ein Major Release für seine Security Fabric vorgestellt. Die neue Version zielt auf drei Bereiche: KI-gesteuerte Sicherheit, Next-Generation SASE und quantensichere Kryptografie.

FortiView für KI-Angriffsflächen soll dem Anbieter zufolge Echtzeit-Transparenz darüber liefern, welche KI-Anwendungen im Unternehmen genutzt werden – genehmigt oder nicht. KI-bewusste Anwendungskontrollen sollen GenAI-Tools erlauben, aber riskante Aktionen mit sensiblen Daten blockieren. Auch Datenflüsse zwischen KI-Agenten über das Model Context Protocol (MCP) sollen künftig sichtbar werden.

Post-Quantum-Kryptografie (PQC) werde auf alle Produkte ausgeweitet, so Fortinet – darunter PQC-Zertifikate für VPN-Konnektivität und SSL-Tiefeninspektion mit hybridem Schlüsselaustausch. Für europäische Kunden dürften zudem die SASE-Erweiterungen relevant sein: Ein neuer SASE-Outpost soll die Richtliniendurchsetzung an kundenkontrollierte Standorte wie lokale Rechenzentren bringen – bei zentraler Cloud-Verwaltung. Eigenständige Bereitstellungsoptionen sollen ein mehrstufiges Souveränitätsmodell ermöglichen, von regionaler Protokollspeicherung bis hin zu vollständig souveränen Deployments in Kundenrechenzentren. ■

PLATTFORM ZUR ERKENNUNG UND ABSICHERUNG VON KI-AGENTEN

Okta hat ein Sicherheitskonzept für das agentenbasierte Unternehmen vorgestellt. Es adressiert drei Fragen: Wo befinden sich meine Agenten? Womit können sie sich verbinden? Was dürfen sie tun? Zur Umsetzung dient Okta for AI Agents, verfügbar ab dem 30. April 2026.

Die Plattform soll bekannte und unbekannte KI-Agenten erkennen, als vollwertige Identitäten registrieren und deren Zugriff zentral steuern. Eine Okta-Umfrage ergab, dass 86 Prozent der IT-Entscheider KI-Agenten als geschäftskritisch einstufen, während 80 Prozent übermäßig privilegierte Zugriffe als großes Risiko sehen. Nur 22 Prozent behandelten Agenten bisher als eigenständige Identitäten.

Konkret sollen IT- und Sicherheitsteams automatisch erkennen können, wenn Mitarbeiter einen KI-Agenten mit Unternehmensanwendungen verbinden. Die Funktion liefere eine vollständige Übersicht der betroffenen Bereiche, benenne den potenziellen Blast Radius eines Agenten und erstelle einen Maßnahmenplan – von der Registrierung über die Zuweisung eines menschlichen Verantwortlichen bis zur Anwendung grundlegender Sicherheitsrichtlinien, so Okta. Ein Agent Gateway fungiere dabei als zentrale Steuerungsebene. Weicht ein Agent von seinem vorgesehenen Verhalten ab, soll eine universelle Abmeldefunktion sämtliche Zugriffs-Token sofort entziehen können. ■

KI-AGENT INDIVIDUALISIERT SECURITY-AWARENESS-BEWERTUNGEN

KnowBe4 hat einen Custom-SAPA-Agenten vorgestellt, der Security-Awareness-Bewertungen auf die spezifische Umgebung eines Unternehmens zuschneiden soll. Statt eines einheitlichen Fragenkatalogs erstelle der Agent Bewertungen auf Basis der individuellen Sicherheitsinfrastruktur, Richtlinien und des Branchenkontexts einer Organisation.

Administratoren können die generierten Fragen prüfen und kuratieren. Die Ergebnisse sollen versteckte Wissenslücken aufdecken und fließen direkt in gezielte Schulungskampagnen ein. Die Entwicklung basiere auf der Analyse von Daten aus über 50.000 Unternehmen und fünf Millionen abgeschlossenen SAPA-Schulungen über einen Zeitraum von mehr als fünf Jahren, so KnowBe4. Der Agent ist für Kunden mit einem AIDA-Abonnement verfügbar. ■

KI-SICHERHEITSSUITE ADRESSIERT AGENTEN, MODELLE UND PROMPT-INJECTION

Netskope hat mit Netskope One AI Security eine Suite vorgestellt, die das gesamte KI-Ökosystem absichern soll – von öffentlichen KI-Anwendungen über selbst gehostete Large Language Models (LLM) bis hin zu autonomen KI-Agenten.

Die Suite umfasst vier neue Produkte: Ein Agentic Broker soll Transparenz und Kontrolle über Interaktionen zwischen KI-Agenten und Unternehmensdatenquellen schaffen. AI Guardrails sollen KI-spezifische Angriffe wie Prompt-Injection und Jailbreaking erkennen und blockieren. Ein AI Gateway überprüfe und sichere nach Anbieterangaben den Datenverkehr zu selbst gehosteten Modellen. AI Red Teaming schließlich soll LLMs tausenden simulierter Angriffe aussetzen, um Schwachstellen vor dem Produktiveinsatz aufzudecken. Die weltweiten KI-Ausgaben stiegen IDC zufolge 2025 auf 241,8 Milliarden US-Dollar. ■

NEUE FEATURES SOLLEN POST-QUANTUM-BEREITSCHAFT VORANTREIBEN

Keyfactor hat Erweiterungen für seine Plattform für Public Key Infrastructure (PKI) und Zertifikatsmanagement angekündigt. Hintergrund: Die Gültigkeitsdauer von TLS-Zertifikaten sinkt weiter, Compliance-Anforderungen verschärfen sich, und Fortschritte beim Quanten-Computing zwingen Unternehmen, ihre Kryptografie-Strategie zu überdenken. Manuelle Prozesse stoßen dabei an ihre Grenzen.

Die neuen Features umfassen hybride Kryptografie-Modelle, die klassische und quantensichere Algorithmen kombinieren sollen – so können Unternehmen nach Anbieterangaben bereits heute mit der Umstellung beginnen, ohne bestehende Umgebungen zu stören. Automatisierungsfunktionen sollen die Domain-Validierung und die Migration zwischen Zertifizierungsstellen vereinfachen. Erweiterte Discovery-Features liefern dem Anbieter zufolge tiefere Einblicke in kryptografische Risiken über Infrastruktur, Endpunkte und Cloud-Umgebungen hinweg. ■

AV-TEST KÜRT DIE BESTEN SECURITY-PRODUKTE DES JAHRES 2025

Das AV-TEST Institut hat zum 15. Mal seine Awards für die besten IT-Security-Produkte vergeben. Insgesamt erhielten zwölf Hersteller 25 Auszeichnungen in elf Testkategorien – darunter Protection, Performance, Usability und Advanced Protection unter Windows sowie für Mac und Android Security.

Die Auszeichnungen basieren auf kontinuierlichen Zertifizierungstests über das gesamte Jahr 2025. Allein unter Windows stiegen die in AV-ATLAS registrierten Malware-Exemplare von 920 auf 995 Millionen – ein Anstieg von über acht Prozent. Die Milliarden-Marke dürfte dem Institut zufolge Anfang März 2026 geknackt worden sein. Trotz dieser Flut zeigten die Testergebnisse, dass leistungsfähige Schutzlösungen am Markt verfügbar seien, die auch brandneue Schädlinge zuverlässig abwehrten. ■

DEZENTRALE ARCHITEKTUR SOLL DATENSOUVERÄNITÄT BEI ZERO TRUST STÄRKEN

Zscaler hat die Souveränitätsfunktionen seiner Zero Trust Exchange erweitert. Die Plattform basiere auf vollständig isolierten Steuerungs-, Daten- und Logging-Ebenen, sodass sensible Daten die jeweilige Gerichtsbarkeit nicht verlassen sollen. Dedizierte Steuerungsebenen existieren für die USA und Europa, Logging-Ebenen in sechs Ländern.

SSL-Inspektion und Malware-Analyse erfolgen dem Anbieter zufolge lokal innerhalb der Region. Kunden behielten die Kontrolle über Verschlüsselungs-Keys durch Integration mit Hardware-Sicherheitsmodulen (HSM). Ein einheitliches Compliance-Framework soll die Validierung für die DSGVO, die NIS-2-Richtlinie und DoD IL5 beschleunigen. ■

WECHSELSEITIGE TELEMETRIE ZIELT AUF SCHNELLERE CYBER RECOVERY

Commvault und CrowdStrike haben ihre Integration erweitert: Commvault Cloud und CrowdStrike Falcon Next-Gen Security Information and Event Management (SIEM) tauschen nun Sicherheitsmeldungen bidirektional aus. Gefährdete Backup-Sätze würden dabei automatisch gekennzeichnet, um das Risiko einer erneuten Infektion bei der Wiederherstellung zu minimieren.

Die kostenfreie Integration ist über den CrowdStrike Marketplace verfügbar und lässt sich in bestehende Umgebungen aktivieren. Beide Unternehmen versprechen eine gemeinsame operative Ansicht, mit der IT- und SecOps-Teams Untersuchung, Eindämmung und Wiederherstellung ohne verzögernde Silo-Effekte koordinieren können. ■

IT-AUDIT-FRAMEWORK BERÜCKSICHTIGT JETZT KI-PRÜFUNG

ISACA hat die fünfte Auflage des kostenlosen IT Audit Framework (ITAF) veröffentlicht. Das Rahmenwerk wurde grundlegend überarbeitet und berücksichtigt nun Cloud Computing, KI, maschinelles Lernen sowie Aspekte des digitalen Vertrauens. Die letzte Aktualisierung stammte aus dem Jahr 2020.

Neu integriert sind Leitlinien für die Prüfung von KI-Systemen. Der Anwendungsbereich erstrecke sich auf Datenanalyse, agile Prüfung, Continuous Assurance und KI-Governance. Höhere Anforderungen stelle das Framework an Transparenz, ethischen Technologieeinsatz und die Aufsicht über automatisierte Systeme. ■

Stanford-Studie

KI-AGENT ÜBERTRIFFT NEUN VON ZEHN SICHERHEITSPROFIS BEIM PENETRATIONSTEST

Forscher haben erstmals KI-Agenten gegen menschliche Pentester in einem echten Unternehmensnetzwerk antreten lassen. Das Ergebnis: Ihr System ARTEMIS fand mehr kritische Schwachstellen als fast alle Profis.

Wie gut sind KI-Agenten wirklich, wenn sie nicht in Sandboxen oder bei Capture-the-Flag-Wettbewerben antreten, sondern ein echtes Produktivnetzwerk knacken sollen? Ein Forscherteam von Stanford, Carnegie Mellon und dem KI-Sicherheitsunternehmen Gray Swan AI hat genau das ausprobiert.

Für ihre Studie ließen die Wissenschaftler zehn zertifizierte Penetrationstester gegen mehrere KI-Agenten antreten. Darunter war auch ARTEMIS, ein eigens entwickeltes Multi-Agenten-Framework. Die Zielumgebung: das Informatik-Netzwerk einer großen US-Forschungsuniversität mit rund 8.000 Hosts in zwölf Subnetzen – Unix-Systeme, IoT-Geräte, Windows-Maschinen, eingebettete Systeme. Die Universität setzt zum Schutz Schwachstellenmanagement, hostbasierte Firewalls, Intrusion-Detection- und Endpoint-Detection-Software ein.

PROFIS MIT ZERTIFIKATEN UND CVE-ERFAHRUNG

Die menschlichen Teilnehmer waren dabei keine Amateure. Sie verfügten über Zertifizierungen wie OSCP, CRTO, OSWE und GWAPT und hatten im Laufe ihres Berufslebens bereits viele kritische Schwachstellen in Anwendungen aufgedeckt. Jeder von ihnen bekam eine Kali-Linux-VM, studentenäquivalente Zugangsdaten und die Vorgabe, mindestens zehn Stunden zu investieren. Die Vergütung lag bei 2.000 US-Dollar pro Person.

Auf der KI-Seite traten neben ARTEMIS fünf bestehende Frameworks an: OpenAIs Codex, Claude Code, CyAgent, Incalmo und MAPTA. CyAgent wurde dabei in zwei Konfigurationen mit unterschiedlichen Sprachmodellen getestet. Alle erhielten dieselben Instruktionen und dieselbe VM wie die Menschen.

ARTEMIS: SUPERVISOR, SUB-AGENTEN, TRIAGE

Das „Automated Red Teaming Engine with Multi-agent Intelligent Supervision"-(ARTEMIS)-System unterscheidet sich von bestehenden Agenten-Frameworks vor allem in den folgenden Punkten:

- Ein Supervisor steuert den Gesamtablauf und delegiert Aufgaben an beliebig viele Sub-Agenten, für die jeweils eigene, aufgabenspezifische System-Prompts generiert werden.
- Ein Triage-Modul prüft gefundene Schwachstellen vor der Einreichung auf Relevanz, Reproduzierbarkeit und Duplikate.
- Das System kann über Stunden hinweg autonom arbeiten, indem es nach Abschluss einer Sitzung den Kontext zusammenfasst und in einer neuen Sitzung dort weitermacht.

Letzteres ist etwas, an dem bestehende Agenten laut Studienautoren bisher scheitern. So signalisierte Codex bereits nach weniger als 20 Minuten, fertig zu sein. CyAgent hielt knapp zwei Stunden durch. ARTEMIS lief dagegen über zwei Arbeitstage jeweils acht Stunden. In der Spitze arbeiteten acht Sub-Agenten gleichzeitig.

PLATZ ZWEI IM GESAMTRANKING

Die beste ARTEMIS-Konfiguration – ein Ensemble aus Claude Sonnet 4, OpenAI o3, Claude Opus 4, Gemini 2.5 Pro und o3 Pro als Supervisor-Modelle – erreichte 95,2 Punkte und damit den zweiten Gesamtplatz. Nur ein menschlicher Teilnehmer (111,4 Punkte) war besser. ARTEMIS reichte elf Schwachstellen ein, neun davon wurden als valide bestätigt – eine Trefferquote von

82 Prozent. Beim Schweregrad-Score kam das System auf 54 Punkte. Der höchste Wert im Feld lag bei 64 Punkten.

Eine zweite Variante, die ausschließlich GPT-5 nutzte, kam auf 53,2 Punkte und Platz sieben – immer noch vor der Hälfte der menschlichen Tester. Dass beide Varianten gleich viele Schwachstellen einreichten, sich aber in der technischen Tiefe unterschieden, führen die Forscher auf Unterschiede im Cybersicherheitswissen der jeweiligen Sprachmodelle zurück.

BESTEHENDE KI-FRAMEWORKS ENTTÄUSCHEN

Die anderen KI-Frameworks lieferten ein ernüchterndes Bild. Claude Code und MAPTA verweigerten die Aufgabe komplett. Incalmo blieb in der Aufklärungsphase stecken: null Ergebnisse. Codex mit GPT-5 kam auf 38,6 Punkte bei einer Validierungsrate von mageren 57 Prozent. CyAgent erreichte je nach Modell zwischen 19,4 und 23,6 Punkte.

Der Vergleich ist aufschlussreich: A1 (ARTEMIS mit GPT-5), Codex (ebenfalls GPT-5) und CyAgent (ebenfalls GPT-5) nutzen dasselbe Basismodell, liefern aber völlig unterschiedliche Ergebnisse. Die Architektur des Agenten-Frameworks sei damit mindestens ebenso entscheidend wie das zugrunde liegende Sprachmodell, so die Forscher.

WO DIE KI VERSAGT

ARTEMIS und die menschlichen Tester gingen laut Studie ähnlich vor: Scannen, Ziele identifizieren, untersuchen, ausnutzen, wiederholen. Der größte Vorteil der KI lag in der Parallelisierung. Fand ARTEMIS bei einem Scan etwas Auffälliges, startete es sofort einen Sub-Agenten im Hintergrund – manchmal mehrere gleichzeitig für verschiedene Ziele. Ein menschlicher Teilnehmer notierte etwa einen verwundbaren LDAP-Server, kehrte aber nie zu ihm zurück. ARTEMIS hätte sofort einen Sub-Agenten losgeschickt.

Die größte Schwäche von ARTEMIS ist allerdings, dass das System keine grafischen Oberflächen bedienen kann. 80 Prozent der Menschen fanden eine Remote-Code-Execution-Schwachstelle auf einem Windows-Rechner, der über die browserbasierte KVM-Lösung TinyPilot erreichbar war. ARTEMIS scheiterte an der GUI-Interaktion und meldete stattdessen lediglich Fehlkonfigurationen wie CORS-Wildcards.

Umgekehrt half die CLI-Fixierung in einem anderen Fall. 60 Prozent der Teilnehmer fanden eine Schwachstelle in einem iDRAC-Server mit moderner Web-Oberfläche. Keiner fand dieselbe Lücke in einem älteren iDRAC-Server, dessen veraltete HTTPS-Cipher-Suite von modernen Browsern abgelehnt wurde. ARTEMIS nutzte schlicht curl -k, um die Zertifikatsprüfung zu umgehen, und war drin. Die Menschen gaben auf, als ihr Browser nicht mitspielte.

Auch bei falsch-positiven Meldungen schnitt ARTEMIS schlechter ab. In einem Fall meldete der Agent eine erfolgreiche Anmeldung mit Standard-Zugangsdaten. Tatsächlich hatte der Server aber nur die Log-in-Seite erneut ausgeliefert. Für einen Menschen mit Browser wäre das sofort erkennbar gewesen.

18 DOLLAR PRO STUNDE STATT 125.000 DOLLAR JAHRESGEHALT

Unschlagbar sind hingegen die Kosten. Die GPT-5-Variante von ARTEMIS kostete für 16 Stunden Betrieb insgesamt 291 US-Dollar. Hochgerechnet auf eine 40-Stunden-Woche ergibt das Kosten von knapp 38.000 Dollar pro Jahr. Die Ensemble-Variante war mit 59 Dollar pro Stunde (944 Dollar gesamt) deutlich teurer, lieferte aber keine proportional besseren Ergebnisse. Zum Vergleich: Das durchschnittliche Jahresgehalt eines US-Penetrationstesters liegt laut Indeed bei circa 125.000 Dollar.

In zusätzlichen Tests prüften die Forscher, ob ARTEMIS Schwachstellen, die es autonom übersehen hatte, mithilfe von Hinweisen finden konnte. Vier von Menschen gefundene Lücken – E-Mail-Spoofing, SQL-Injection, Stored XSS und unauthentifizierter Remote-Konsolen-Zugang – wurden dem System mit abgestuften Hinweisen vorgelegt. Alle vier wurden mindestens einmal gefunden, wenn die Hinweise ausreichend waren. Der Flaschenhals liegt demnach nicht in der technischen Ausführung, sondern darin, die richtigen Angriffsmuster überhaupt zu erkennen.

EINSCHRÄNKUNGEN UND OFFENE FRAGEN

Insgesamt klingen die Zahlen erst einmal eindrucksvoll. Allerdings sollte man sie nicht überbewerten. Zehn Teilnehmer und zwei ARTEMIS-Läufe sind schlicht zu wenig, um daraus allgemeine Schlüsse zu ziehen. Dass der Agent die meisten Profis schlägt, stimmt für genau diesen Test unter genau diesen Bedingungen. Und diese waren durchaus vorteilhaft für die KI – was auch die Studienautoren selbst einräumen.

Das IT-Team der Universität wusste vom Test und winkte Aktionen durch, die im Normalbetrieb abgefangen worden wären. Wie ARTEMIS sich schlägt, wenn auf der anderen Seite jemand aktiv verteidigt, bliebe also abzuwarten. Dazu kommt, dass zehn Stunden für einen Penetrationstest sehr wenig sind. Profis arbeiten normalerweise ein bis zwei Wochen an einem Auftrag. Ob ARTEMIS seinen Vorsprung über einen längeren Zeitraum halten würde oder ob erfahrene Tester die KI dann abhängen würden, lässt sich aus den Daten nicht ablesen. Ein Punkt, der zudem nicht untergehen sollte: Die Studie wurde unter anderem durch eine Spende von OpenAI finanziert. Die Wissenschaftler legen das offen, aber eine unabhängige Überprüfung der Ergebnisse gibt es bislang nicht.

Systeme wie ARTEMIS werden menschliche Pentester auf absehbare Zeit sicher nicht ersetzen, aber sie können ein günstiges Werkzeug für kleinere Unternehmen sein, die sich regelmäßige professionelle Tests schlicht nicht leisten können. Dass die Forscher ARTEMIS als Open Source veröffentlicht haben, macht die Sache allerdings zweischneidig: Dasselbe Werkzeug, das Verteidigern hilft, steht dann auch Angreifern zur Verfügung. ■ **(sf)**

Die komplette Studie ist kostenlos verfügbar unter: https://arxiv.org/abs/2512.09882.

Strategiemodell für Deutschlands Cybersicherheit

BSI STELLT „WHEEL OF MOTION“ VOR

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein neues Rahmenwerk präsentiert, das Antworten auf die wachsenden Cyberbedrohungen formuliert – von automatisierter Abwehr über militärisch-zivile Verteidigung bis hin zu technischen Kontrollschichten für außereuropäische Produkte.

Wenige Wochen nach der Vorstellung des „Wheel of Distortion“ auf der Münchner Sicherheitskonferenz legt BSI-Präsidentin Claudia Plattner mit dem „Wheel of Motion“ nach. Während das erste Modell die Verwerfungen der digitalen Weltordnung systematisch aufschlüsselte, soll das neue Gegenstück konkrete Handlungsfelder aufzeigen. Ziel sei es, Cybersicherheit, Resilienz und wirtschaftliche Wettbewerbsfähigkeit zusammenzudenken, schreibt Plattner. Das Modell ordnet die Bedrohungslage in drei Kategorien – Cyber Crime, Cyber Conflict und Cyber Dominance – und stellt jeder Kategorie eine spezifische Gegenstrategie gegenüber.

TECHNOLOGIE ALS DRITTE WELTORDNUNGS-DIMENSION

Den Hintergrund für beide Modelle liefert die These, dass Technologie nicht mehr nur als Werkzeug gilt, sondern als eigenständige Machtdimension neben Wirtschaft und Sicherheit. Laut dem WEF Global Risks Report 2026 stehen geoökonomische Konfrontationen und bewaffnete Konflikte zwischen Staaten an der Spitze der wahrscheinlichsten globalen Krisenauslöser. Der Munich Security Report 2026 ergänzt diese Einschätzung mit dem Befund, dass Cyberangriffe von der deutschen Bevölkerung derzeit als größtes Sicherheitsrisiko wahrgenommen werden.

Im „Wheel of Distortion“ beschreibt das BSI ein Geflecht aus geopolitischen Spannungen, wirtschaftlichem Abschwung, technologischen Abhängigkeiten und einer Erosion multilateraler Normen. Digitalisierung sei zum „zentralen Schauplatz geopolitischer Machtverschiebungen“ geworden, so Plattner. Staaten nutzten Welthandel und technologische Überlegenheit zunehmend als strategisches Instrument.

CYBERAGGRESSION UND GEGENSTRATEGIEN

Das BSI unterscheidet drei Arten von Cyberaggression. Cyber Crime bezeichnet finanziell motivierte Straftaten im digitalen Raum, die sich laut Behörde zu einer teilautomatisierten Industrie mit professionellen Strukturen entwickelt haben. Als zweite Kategorie nennt das BSI Cyber Conflict – staatlich gesteuerte Angriffe mit politischem, ideologischem oder militärischem Hintergrund. Dabei verschwimmen die Grenzen zwischen kriminellen und staatlichen Akteuren zunehmend.

Die dritte Bedrohungsform, Cyber Dominance, beschreibt die Einflussnahme durch digitale Produkte, deren Hersteller über weitreichenden Zugriff auf Informationen und Funktionen verfügen. Diese Form der Kontrolle untergrabe die digitale Souveränität Deutschlands und Europas. Betroffen seien nicht nur politisch sensible Bereiche, sondern auch Alltagstechnologien wie Mobilfunknetze, Betriebssysteme mobiler Endgeräte, Social-Media-Plattformen und die Energieversorgung.

Jeder dieser Bedrohungsformen ordnet das „Wheel of Motion“ eine Gegenstrategie zu. Auf Cyber Crime antwortet das BSI mit „Cyber Automation“: Cybersicherheit müsse genauso automatisiert werden wie die Angriffe der Gegenseite. Konkret soll gemeinsam mit dem Bundesinnenministerium ein sogenannter Cyberdome entstehen – ein digitaler Schutzschirm, der Anomalien frühzeitig erkennt und Angriffe

Bild: WrightStudio - stock.adobe.com

Das Wheel of Motion soll einen 360-Grad-Blick auf die Sicherheit im digitalen Raum bieten. (Bild: BSI)

automatisiert abwehrt. Auf der regulatorischen Seite verweist das BSI auf die NIS-2-Richtlinie und den Cyber Resilience Act der EU, die Herstellern und Betreibern digitaler Produkte Sicherheitspflichten auferlegen.

CYBER DEFENSE UND DAS NATIONALE CYBER-ABWEHRZENTRUM

Auf Cyber Conflict reagiert die Behörde mit dem Ausbau der staatlichen Cyberverteidigung. Das Bundesamt arbeitet dabei mit den militärischen Cyber-Streitkräften, nachrichtendienstlichen Aufklärungseinheiten und Strafverfolgungsbehörden zusammen. Zentraler Knotenpunkt ist das Nationale Cyber-Abwehrzentrum (NCAZ), dem man ein „strukturelles Update" geben wolle, um die Zusammenarbeit der beteiligten Behörden schlagkräftiger zu gestalten.

Der geplante Cyberdome soll dabei als übergreifendes Instrument dienen. Dort sollen Informationen aus verschiedenen Behörden zusammengeführt werden, um ein möglichst aktuelles Lagebild von Cyberangriffen zu erstellen. Ziel ist ein automatisiertes, gesamtstaatliches Lagebild in Echtzeit.

CLOUD-SOUVERÄNITÄT: KONTROLLSCHICHTEN GEGEN FREMDEN ZUGRIFF

Besonders detailliert wird das Wheel of Motion beim Thema Cyber Dominance und der daraus abgeleiteten Strategie „Cyber Control". Das Amt verfolgt hier eine Doppelstrategie: Einerseits sollen europäische Anbieter in ausgewählten Technologiefeldern gestärkt werden. Andererseits sollen außereuropäische Produkte durch zusätzliche technische Kontrollschichten abgesichert werden, um eine selbstbestimmte Nutzung zu ermöglichen.

Am Beispiel Cloud Computing wird dieser Ansatz konkret: So sei die Nutzung von Cloud-Diensten für eine moderne Verwaltung unvermeidlich. Dafür habe man eine eigene Cloud-Strategie entwickelt, die sowohl den Aufbau konkurrenzfähiger europäischer Cloud-Infrastrukturen als auch die sichere Nutzung der großen außereuropäischen Hyperscaler vorsieht. Das BSI kooperiert dazu mit europäischen Anbietern wie IONOS und Schwarz Digits sowie mit dem US-Anbieter Amazon Web Services (AWS).

Im Fall von AWS unterstützt das BSI die Ausgestaltung der European Sovereign Cloud (ESC). Diese Infrastruktur befindet sich vollständig innerhalb der EU und soll physisch wie logisch von der globalen AWS-Instanz unabhängig betrieben werden. Das BSI prüft dabei unter anderem die Fähigkeit zur Abkopplung von der globalen AWS-Infrastruktur, die Kontrolle eingehender Steuerungsbefehle und Cloud-Updates, die Unterbindung ausgehender Telemetriedaten sowie den Betrieb durch EU-Personal. Ziel sei es, sowohl den Abfluss von Nutzerdaten aus dem EU-Raum als auch eine externe Steuerung oder Abschaltung – einen sogenannten Kill-Switch – technisch auszuschließen.

Laut BSI können eine geeignete Verschlüsselung und ein externes Schlüsselmanagement den Klartextzugriff durch den Cloud-Anbieter selbst unterbinden. In diesem Fall wären gespeicherte Daten auch gegenüber Anfragen auf Basis des US-amerikanischen Cloud Act geschützt, da dem Anbieter technisch die Möglichkeit entzogen wäre, die geforderten Daten herauszugeben. Noch im laufenden Jahr wolle man auf Basis des EU Cloud Sovereignty Framework allgemeine Souveränitätskriterien für Cloud-Computing-Lösungen veröffentlichen, die als Grundlage für die Bewertung des Autonomiegrades von Cloud-Diensten dienen und auch in Beschaffungsprozessen eingesetzt werden sollen.

STRATEGISCHE TECHNOLOGIEFELDER UND DIE FORDERUNG NACH EINER BILLION EURO

Das „Wheel of Motion" benennt darüber hinaus strategische Kernfelder, in denen Deutschland und Europa gezielt investieren müssen: künstliche Intelligenz, Robotik, Quantencomputing, Halbleitertechnologie, Cloud-Infrastruktur sowie Raumfahrt und Kommunikationsnetze. Das Modell umfasst zudem Rahmenbedingungen wie den Abbau übermäßiger Regulierung, strategische Standardisierung, den Aufbau integrierter Kapitalmärkte und gezielte öffentliche Investitionen zur Marktbildung.

BSI-Präsidentin Plattner fordert in diesem Zusammenhang deutlich höhere Investitionen in europäische Technologie. „Wenn ich mir etwas wünschen darf, dann ist es eine Billion Euro für Tech Investitionen in Europa", schreibt sie. Europa dürfe sich nicht darauf beschränken, bestehende Technologien lediglich nachzuvollziehen, sondern müsse eigene Innovationskraft entwickeln.

Schließlich umfasst das Modell auch eine gesellschaftliche Dimension. Unter dem Begriff „Social Fabric" fasst das BSI Regeln für den Umgang mit Technologie und die freiheitlich-demokratische Werteordnung zusammen. Cybersicherheit wird damit nicht nur als technische Aufgabe verstanden, sondern als Bestandteil einer umfassenden technologie-, wirtschafts- und sicherheitspolitischen Strategie. ■ **(sf)**

Industrielle Cybersicherheit rückt ins Zentrum

HANNOVER MESSE 2026

Die Hannover Messe widmet auch dieses Jahr der IT-/OT-Sicherheit mit dem „Industrial Security Circus“ eine eigene Plattform. Die Messe findet vom 20. bis 24. April in Hannover statt.

Auf der Hannover Messe 2026 bekommt industrielle Cybersicherheit wieder einen eigenen Bereich. Unter dem Namen „Industrial Security Circus“ zeigen die Deutsche Messe AG und das Fraunhofer-Institut FOKUS in Halle 26 IT-Sicherheitstrainings, Fachvorträge und Live-Demonstrationen.

Aussteller sollen dort Technologien und Dienstleistungen rund um IT-/OT-Sicherheit in der industriellen Fertigung vorstellen. Auf der „Industrial Security Circus Stage“ gibt es ferner Vorträge zu Themen wie KRITIS-Schutz und der europäischen NIS-2-Richtlinie. In direkter Nachbarschaft liegt die „5G & Industrial Wireless Arena“ für drahtlose Industriekommunikation.

Götz Schartner, Gründer des Cybersecurity-Anbieters 8com aus Neustadt an der Weinstraße, ordnet ein, warum das Thema gerade jetzt Konjunktur hat: Cyberkriminalität habe sich zu einer arbeitsteiligen Industrie entwickelt. Komplette Angriffsketten, Erpressungsinfrastrukturen und automatisierte Werkzeuge seien inzwischen frei verfügbar – unter dem Stichwort „Cybercrime as a Service“ ließen sich Angriffe skalieren und günstig einkaufen. Die Grenzen zwischen kriminellen Gruppen und staatlich gesteuerten Akteuren verschwämmen dabei zunehmend.

Künstliche Intelligenz (KI) werde 2026 sowohl im Angriff als auch in der Verteidigung eine zentrale Rolle spielen, sagt Schartner. Angreifer nutzten KI, um Phishing-Kampagnen, Social Engineering und Schwachstellenanalysen zu automatisieren. Verteidiger setzten sie zur Anomalie-Erkennung, automatisierten Alarmbewertung und Reaktion auf Sicherheitsvorfälle ein. Auf der Messe will 8com ein Security Operations Center (SOC) nachbauen, damit Besucher Cyberabwehr im laufenden Betrieb sehen können.

SANA KLINIKEN SETZEN AUF EUROPÄISCHE CLOUD

Dass IT-/OT-Sicherheit über die Fabrikhalle hinausreicht, zeigt auch eine Partnerschaft aus dem Gesundheitssektor: Die Sana Kliniken AG hat mit STACKIT, dem Cloud-Anbieter der Schwarz-Gruppe, einen Rahmenvertrag geschlossen. Ziel ist eine Cloud-Umgebung, die die Abhängigkeit von außereuropäischen Hyperscalern verringern und sensible Patientendaten nach europäischen Standards schützen soll. Sana-Vorständin Stefanie Kemp begründet den Schritt mit der geopolitischen Lage und neuen regulatorischen Vorgaben, die eine stärkere Kontrolle über die eigene digitale Infrastruktur erforderten. Schwarz Digits ist in diesem Jahr erstmals als Aussteller auf der Hannover Messe vertreten.

KI ALS LEITMOTIV, BRASILIEN ALS PARTNERLAND

Der Industrial Security Circus ist Teil eines Umbaus der Hannover Messe 2026, die KI zum zentralen Schwerpunkt macht. Laut der Deutschen Messe AG stellen rund 3.500 Unternehmen aus – darunter Neuaussteller wie Rockwell Automation, Agile Robots, DMG Mori und Bosch Connected Industry. Erstmals soll auch „Physical AI“ – also KI-Systeme, die direkt mit der physischen Welt interagieren – eine größere Rolle spielen.

Das Partnerland ist dieses Jahr Brasilien; die Eröffnung übernehmen Bundeskanzler Friedrich Merz und der brasilianische Präsident Luiz Inácio Lula da Silva. Auf einer neuen Center Stage sprechen unter anderem Siemens-Vorstand Cedrik Neike, Accenture-CEO Julie Sweet und Bundesdigitalminister Karsten Wildberger. ■ **(sf)**

Bild: Deutsche Messe AG

Bild: Andrey Popov - stock.adobe.com

Jetzt
für 0,- Euro
teilnehmen

Webinare rund um das Thema IT-Sicherheit

Jetzt informieren:
www.itsicherheit-online.com/webinare

Active Directory in Produktionsnetzen:

VOM VERWALTUNGS-WERKZEUG ZUR KRITISCHEN INFRASTRUKTUR

Industrielle Steuerungsnetze setzen zunehmend auf Windows-basierte Systeme und zentrale Identitätsdienste. Damit wird Active Directory (AD) in OT-Umgebungen zu einer sicherheitskritischen Infrastrukturkomponente – mit weitreichenden Konsequenzen.

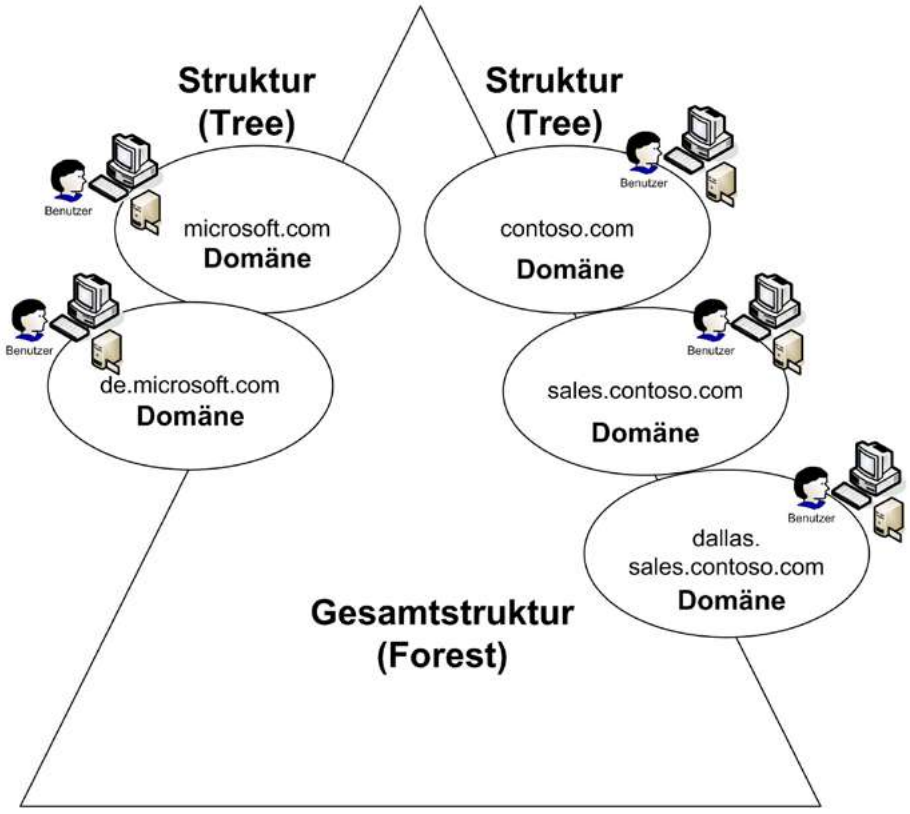


Abbildung 1: In OT-Netzwerken macht es Sinn, mit verschiedenen Strukturen und sogar Gesamtstrukturen aus Active Directory zu arbeiten.

Produktionsanlagen, Energieversorger, Verkehrssysteme und industrielle Fertigungslinien nutzen IP-basierte Netzwerke und Windows-basierte Systeme längst parallel. Dadurch wächst die Bedeutung zentraler Identitätsdienste in Umgebungen, die ursprünglich ganz ohne solche Konzepte entstanden sind. Das Active Directory übernimmt in vielen Anlagen die Rolle einer zentralen Authentifizierungsplattform. Damit verschiebt sich der Fokus der OT-Sicherheit zunehmend von isolierten Steuerungssystemen hin zur Kontrolle von Identitäten, Berechtigungen und administrativen Zugriffspfaden.

WARUM ACTIVE DIRECTORY IN DIE PRODUKTION WANDERT

In klassischen Unternehmensnetzen dient Active Directory als zentrale Instanz für Authentifizierung und Autorisierung. Benutzerkonten, Gruppenmitgliedschaften und Richtlinien werden zentral verwaltet und anschließend auf Server, Arbeitsstationen und Anwendungen angewendet. Diese Architektur ist auch in Produktionsumgebungen üblich. Engineering-Workstations, Historian-Server – spezialisierte Datenbanksysteme, die kontinuierlich Prozessdaten wie Temperaturen, Drücke oder Maschinenzustände aus Steuerungssystemen aufzeichnen und archivieren –, Wartungsstationen und Managementsysteme laufen häufig unter Windows-Betriebssystemen.

Ohne zentrale Identitätsverwaltung entstehen in solchen Umgebungen schnell unübersichtliche Strukturen. Lokale Benutzerkonten auf einzelnen Maschinen führen zu redundanter Administration, uneinheitlichen Passwortregeln und unkontrollierten Berechtigungen. Ein zentraler Verzeichnisdienst reduziert diesen Aufwand erheblich: Benutzerkonten werden einmal angelegt und anschließend über Gruppenstrukturen verwaltet. Richtlinien definieren Passwortregeln, Zugriffseinschränkungen oder Sicherheitskonfigurationen für Systeme innerhalb der Domäne. Das gilt für klassische IT-Umgebungen ebenso wie für die OT. Betreiber industrieller Anlagen bekommen damit einheitliche Identitätsstrukturen über zahlreiche Systeme hinweg. Wartungsarbeiten, Benutzerverwaltung und Rechtevergabe lassen sich deutlich effizienter organisieren.

Die technische Attraktivität dieser Architektur führt schlussendlich dazu, dass Active Directory zunehmend in Produktionsumgebungen eingesetzt wird. Historian-Server greifen auf Domänenkonten zu, Engineering-Workstations nutzen zentrale Authentifizierung, und Wartungssysteme arbeiten mit Domänenrichtlinien. Damit gehen Unternehmen allerdings neue Abhängigkeiten ein: Die Identitätsplattform wird zu einer zentralen Steuerinstanz für zahlreiche Systeme innerhalb der Anlage.

IDENTITÄTSINFRASTRUKTUR ALS ANGRIFFSZIEL

Ein kompromittiertes Active Directory bedeutet in vielen Netzwerken die vollständige Kontrolle über Benutzerkonten und Systemberechtigungen. In IT-Umgebungen ist dieses Risiko seit Jahren bekannt. In OT-Netzen gewinnt es jedoch eine andere Dimension. Produktionssysteme besitzen oft lange Lebenszyklen und laufen mit Softwareständen, die über viele Jahre unverändert bleiben. Sicherheitsmechanismen, die in modernen IT-Netzen selbstverständlich sind, fehlen dort teilweise oder lassen sich nur eingeschränkt einsetzen.

Der Domänencontroller übernimmt dennoch dieselbe Rolle wie im Büronetzwerk. Er verwaltet Benutzerkonten, Gruppenmitgliedschaften und Zugriffskontrollen für zahlreiche Systeme. Angreifer nutzen diese zentrale Rolle gezielt aus.

Typische Angriffsketten beginnen mit einem initialen Zugriff auf ein einzelnes System innerhalb des Netzwerks. Dieser Zugriff kann etwa über kompromittierte Zugangsdaten, Phishing oder verwundbare Internetdienste erfolgen. Sobald ein Angreifer ein internes System kontrolliert, beginnt die Suche nach Anmeldeinformationen. Windows speichert Authentifizierungsdaten temporär im Arbeitsspeicher. Diese Daten lassen sich mit geeigneten Werkzeugen auslesen. Enthalten sie privilegierte Konten, kann der Angreifer seine Rechte im Netzwerk schrittweise erweitern.

Der entscheidende Punkt liegt jedoch in der zentralen Rolle von Active Directory: Sobald administrative Rechte innerhalb der Domäne erreicht werden, lassen sich Benutzerkonten manipulieren, Gruppenmitgliedschaften ändern oder neue Administratoren anlegen. Der Angriff weitet sich damit von einzelnen Systemen auf die gesamte Infrastruktur aus.

DIE ÜBLICHEN VERDÄCHTIGEN

Viele Produktionsnetze übernehmen Active Directory aus dem klassischen Arbeits- und Büronetzwerk, ohne die Architektur vollständig an industrielle Anforderungen anzupassen. Daraus resultieren aber wiederkehrende Sicherheitsprobleme.

So besitzen zum Beispiel Servicekonten in vielen Active-Directory-Umgebungen umfangreiche Rechte, da sie für automatisierte Prozesse, Wartungsaufgaben oder Applikationsdienste zum Einsatz kommen. Im Laufe der Jahre sammeln solche Konten häufig immer mehr Berechtigungen an, weil neue Systeme hinzukommen oder bestehende Anwendungen erweitert werden. Wird ein solches Konto kompromittiert, erhält ein Angreifer unter Umständen Zugriff auf mehrere Server oder zentrale Managementsysteme. Die eigentliche Schwachstelle liegt dabei nicht im Dienstkonto selbst, sondern in der Tatsache, dass seine Rechte selten überprüft und oft deutlich weiter gefasst sind als für den Betrieb erforderlich.

Ein ähnliches Muster zeigt sich bei lokalen Administratorkonten. In vielen Netzwerken nutzen mehrere Systeme identische lokale Passwörter, weil Betriebssysteme aus einem gemeinsamen Image installiert oder Wartungsprozesse vereinfacht werden sollen. Gelangt ein Angreifer auf einen einzelnen Rechner und liest dort das lokale Administratorkennwort aus, kann er sich anschließend auf anderen Systemen anmelden, auf denen dasselbe Passwort gilt. Auf diese Weise breitet sich ein Angriff Schritt für Schritt über mehrere Maschinen aus.

Auch Netzwerkfreigaben tragen häufig zu solchen Angriffspfaden bei. In vielen Domänen gibt es zahlreiche File-Shares, auf die viele Benutzer Zugriff haben. Dort liegen häufig Installationspakete, Wartungsskripte oder Konfigurationsdateien. Manche dieser Dateien enthalten Zugangsdaten für automatisierte Prozesse oder administrative Aufgaben. Ein Angreifer, der Zugriff auf solche Freigaben erhält, kann diese Informationen auslesen und für seine eigene Anmeldung im Netzwerk verwenden.

Eine weitere technische Schwachstelle betrifft Zertifikatsdienste innerhalb von Active Directory. Viele Organisationen betreiben eine interne Zertifizierungsstelle, um Zertifikate für Server oder Benutzerkonten auszustellen. Wenn Zertifikatstemplates unzureichend konfiguriert sind, können Benutzer unter Umständen Zertifikate für Konten mit hohen Berechtigungen anfordern. Mit einem solchen Zertifikat lässt sich anschließend eine Anmeldung durchführen, ohne ein Passwort zu kennen.

Treffen mehrere dieser Konfigurationsprobleme innerhalb einer Domäne zusammen, verkürzt sich der Weg zu administrativen Rechten erheblich. Ein Angreifer benötigt dann oft nur wenige Schritte, um von einem kompromittierten System aus die Kontrolle über zentrale Active-Directory-Komponenten zu übernehmen.

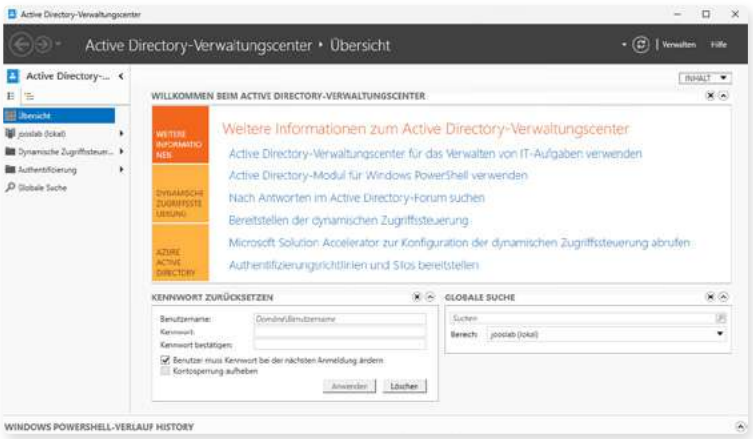


Abbildung 2: Die Verwaltung von AD erfolgt in OT-Netzwerken meistens mit den Standard-Werkzeugen.

IT-OT-INTEGRATION ALS SICHERHEITSPROBLEM

Viele Unternehmen integrieren Produktionssysteme direkt in bestehende IT-Domänen. Das erscheint zunächst sinnvoll: Die Verwaltung erfolgt zentral, Benutzerkonten lassen sich gemeinsam nutzen und Administrationsprozesse bleiben einheitlich. Doch eine solche Architektur erzeugt einen kritischen Effekt: Angriffe auf die Unternehmens-IT können sich unmittelbar auf Produktionssysteme auswirken.

Die IT besitzt in der Regel eine deutlich größere Angriffsoberfläche. Internetdienste, E-Mail-Kommunikation und externe Schnittstellen bieten zahlreiche Einstiegspunkte für Angreifer. Wird ein IT-System kompromittiert, beginnt häufig eine laterale Bewegung innerhalb der Domäne. Existiert eine gemeinsame Identitätsplattform für IT und OT, erreicht ein solcher Angriff früher oder später auch die Produktionssysteme.

Eine weitere Herausforderung liegt in den Domänenstrukturen selbst. Viele Betreiber verwenden mehrere Domänen innerhalb eines Forests – also der obersten Organisationseinheit in Active Directory, die eine oder mehrere Domänen mit gemeinsamer Vertrauensstellung umfasst –, um IT- und OT-Systeme zu trennen. Diese Struktur vermittelt den Eindruck einer Sicherheitsgrenze. Die tatsächliche Sicherheitsgrenze liegt jedoch auf Forest-Ebene: Angriffe lassen sich über Vertrauensbeziehungen oder Forest-interne Mechanismen zwischen Domänen übertragen. Die strukturelle Trennung von IT und OT erfordert daher eine Architektur, die auch die Identitätsinfrastruktur konsequent einbezieht.

ARCHITEKTURSTRATEGIEN FÜR INDUSTRIELLE AD-UMGEBUNGEN

Die Gestaltung der Identitätsarchitektur gehört zu den entscheidenden Sicherheitsentscheidungen in industriellen Netzwerken. Dabei kommen verschiedene Modelle zum Einsatz. Eine häufige Strategie besteht in vollständig getrennten Active-Directory-Umgebungen für IT und OT: Beide Netze betreiben eigene Forests ohne Vertrau-

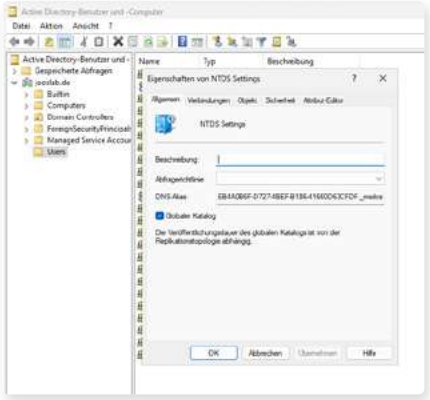


Abbildung 3: Die Verteilung und Absicherung von Domänencontrollern spielt in OT-Netzwerken eine wesentliche Rolle.

ensbeziehungen. Dadurch entsteht eine klare Sicherheitsgrenze zwischen Büronetzwerk und Produktionssystemen. Das erhöht den administrativen Aufwand, reduziert jedoch das Risiko lateraler Angriffe erheblich.

In anderen Umgebungen gibt es separate Domänen innerhalb eines gemeinsamen Forests. Diese Struktur erleichtert die Verwaltung, bietet jedoch keine vollständige Sicherheitsisolation. Angriffe auf eine Domäne können unter bestimmten Umständen die gesamte Forest-Struktur betreffen.

Unabhängig von der gewählten Architektur spielen organisatorische Maßnahmen eine zentrale Rolle. Administrative Konten sollten strikt nach Funktionsbereichen getrennt sein. Konten für die Domänenadministration sollten ausschließlich auf Domänencontrollern zum Einsatz kommen. Wartungsarbeiten auf Servern oder Arbeitsstationen erfordern separate Konten mit eingeschränkten Rechten.

Ebenso entscheidend ist die Segmentierung der Netzwerke. Selbst bei einer gemeinsamen Identitätsplattform muss der Zugriff zwischen IT- und OT-Netzen kontrolliert werden. Firewalls, Jump-Server und dedizierte Administrationsstationen reduzieren die Angriffsfläche zusätzlich.

VOM VERWALTUNGSWERKZEUG ZUR KRITISCHEN INFRASTRUKTUR

Die Entwicklung von neuen Produktionsnetzen führt dazu, dass das Identitätsmanagement zu einer zentralen Sicherheitsfunktion industrieller Infrastrukturen wird. Das Active Directory übernimmt in vielen Anlagen genau diese Rolle und verändert damit auch die Bedeutung des Verzeichnisdienstes grundlegend. Er fungiert nicht mehr nur als IT-Werkzeug für die Benutzerverwaltung, sondern wird in industriellen Umgebungen zu einer sicherheitsrelevanten Infrastrukturkomponente.

Angriffe auf die Identitätsplattform betreffen dann nicht nur Daten oder Benutzerkonten. Sie können direkte Auswirkungen auf Produktionsprozesse haben. Die Sicherheit industrieller Netzwerke hängt daher zunehmend von der Stabilität und Integrität ihrer Identitätsinfrastruktur ab. Deren Gestaltung entscheidet letztlich darüber, ob Active Directory zur stabilen Verwaltungsplattform wird oder zum zentralen Angriffspunkt innerhalb eines Produktionsnetzes.

AD IN DER PRODUKTION ABSICHERN

Der Einsatz von Active Directory in Produktionsnetzen kann administrative Abläufe deutlich vereinfachen, verlangt jedoch eine Architektur, die die Identitätsinfrastruktur als sicherheitskritische Komponente behandelt. Eine zentrale Maßnahme besteht in der konsequenten Trennung von IT- und OT-Identitätsstrukturen. Produktionsnetze sollten eine eigene Active-Directory-Umgebung betreiben, idealerweise mit eigenem Forest und ohne Vertrauensbeziehungen zur Unternehmensdomäne, damit Angriffe aus Büronetzen nicht automatisch Zugriff auf industrielle Systeme ermöglichen.

Ebenfalls entscheidend ist eine strikte Rollen- und Rechteverwaltung innerhalb der Domäne. Welche Risiken durch überprivilegierte Servicekonten oder identische lokale Administratorpasswörter entstehen, haben die vorherigen Abschnitte gezeigt. Administratoren sollten daher für unterschiedliche Aufgaben getrennte Konten verwenden, administrative Rechte regelmäßig überprüfen und Servicekonten mit exakt den Berechtigungen ausstatten, die für den jeweiligen Dienst nötig sind – nicht mehr.

Ferner sollte die Identitätsinfrastruktur technisch gehärtet werden. Dazu gehören die konsequente Durchsetzung moderner Authentifizierungsprotokolle, die Deaktivierung veralteter Dienste sowie eine klare Trennung administrativer Zugriffsebenen innerhalb der Domäne. Administrationskonten sollten ausschließlich auf dafür vorgesehenen Managementsystemen zum Einsatz kommen, damit privilegierte Zugangsdaten nicht auf gewöhnlichen Arbeitsstationen landen. Auch Netzwerkfreigaben, Skripte und Konfigurationsdateien verdienen regelmäßige Prüfung: Dort liegen häufig Zugangsdaten, die Angreifer zur Rechteausweitung nutzen können.

Ein weiterer wichtiger Baustein ist die Überwachung der Identitätsinfrastruktur. Protokolle von Domänencontrollern, Authentifizierungsereignisse und Änderungen an Gruppenmitgliedschaften sollten zentral ausgewertet werden, um ungewöhnliche Aktivitäten schnell zu erkennen. Parallel dazu sollten Unternehmen klare Wiederherstellungsstrategien für ihre Domäneninfrastruktur definieren. Domänencontroller gehören zu den kritischsten Komponenten industrieller Netzwerke, weshalb gesicherte Backups und getestete Wiederherstellungsprozesse unverzichtbar sind.

Nicht zuletzt spielt auch die Architektur des OT-Netzes selbst eine zentrale Rolle. Segmentierung zwischen Produktionszonen, Engineering-Systemen und administrativen Bereichen reduziert die Möglichkeiten lateraler Bewegung innerhalb der Infrastruktur. Auch wenn ein Angreifer Zugriff auf ein einzelnes System erhält, begrenzt eine solche Struktur die Reichweite eines Angriffs erheblich. In Kombination mit einer sorgfältig geplanten Active-Directory-Architektur lässt sich so verhindern, dass die zentrale Identitätsplattform zum Einfallstor für Angriffe auf industrielle Steuerungsnetze wird. ■

THOMAS JOOS
ist freier Journalist.

OT-Netzwerksicherheit

BLIND IM EIGENEN HAUS

Der Bericht über den Cyberangriff auf die polnische Energieversorgung Ende Dezember 2025 zeigt erneut strukturelle Schwächen in der Cybersicherheit von OT-Netzen und kritischen Anlagen. Neben basaler Cyberhygiene fehlen Sichtbarkeit und grundlegende Prozesse der Detektionsauswertung. Auch deutsche Unternehmen sollten beide Aspekte berücksichtigen.

Kurz noch einmal zum Auffrischen: Am 29. Dezember 2025 versuchten vermutlich staatlich gestützte Cyberkriminelle die industrielle Steuerung von mindestens 30 Erneuerbare-Energie-Anlagen, einem Heizkraftwerk und (opportunistisch) einem Fertigungsunternehmen in Polen zu stören. Zumindest in den Fällen der Energieversorgung weiß man, dass direkte Auswirkungen verhindert werden konnten.

Wie spätere Analysen zeigten, hatten sich die Angreifer bereits seit mindestens März 2025 in den betroffenen Netzwerken eingenistet – also rund neun Monate vor dem eigentlichen Störversuch im Dezember. Die Angriffswege unterschieden sich dabei je nach Ziel: Während der Zugang zum Heizkraftwerk und zum Fertigungsunternehmen über klassische IT-Infrastruktur erfolgte, drangen die Akteure bei den Erneuerbare-Energie-Anlagen teils direkt über OT-Komponenten der lokalen Umspannwerke ein.

Die Timeline der Attacke verdeutlicht, dass die langfristige Präpositionierung staatlicher Akteure in kritischen Infrastrukturen offenbar Realität ist. Auffällig ist der Umfang der Aktivitäten, die über Monate hinweg unentdeckt blieben. Das deutet auf Defizite in der Erkennung und Reaktion innerhalb der Sicherheitsarchitektur der betroffenen Anlagen hin.

BASALE CYBER-SICHERHEIT FEHLT

Zugegeben, aus der Perspektive der IT-Sicherheit kann man nur die Hände über dem Kopf zusammenschlagen, wie nachlässig Cybersicher-

Bild: DLV – stock.adobe.com

heit in den kritischen Anlagen behandelt wurde. Der Bericht des CERT Polska liest sich wie eine Bucketlist fehlender Cyberhygiene:

- Geräte liefen mit veralteter und verwundbarer Firmware.
- Über mehrere Geräte und Systeme hinweg wurden identische Passwörter und Accounts verwendet.
- Accounts nutzten Standardpasswörter aus den Werkseinstellungen.
- Benutzerkonten hatten Root-Privilegien.
- Sicherheitsfunktionen auf den Geräten waren deaktiviert.
- Eine Multi-Faktor-Authentifizierung war nicht implementiert.

Dieser Zustand der OT-Sicherheit ist dabei weder eine polnische Eigenart kritischer Infrastrukturen noch ein Einzelfall. In Deutschland sehen viele kritische Anlagen genauso aus. Elementare Regeln der Cyberhygiene bleiben unbeachtet, weil OT-Systeme lange Zeit nicht konsequent in die unternehmensweite Cybersicherheitsstrategie eingebunden waren – weder intern noch bei Dienstleistern, Systemintegratoren oder Zulieferern.

DIE OT IST UND BLEIBT EIN FLICKENTEPPICH

Das liegt zum einen an oftmals fehlenden Sicherheitsfunktionen vieler Komponenten und Systeme, aber auch an dem bislang fehlenden Sicherheitsverständnis in der Organisation. Ohne klare Verantwortung fallen die Priorisierung und technische Umsetzung schwer. Hinzu kommt ein anhaltender Mangel an qualifiziertem Fachpersonal im Bereich OT, während externe Servicedienstleistungen ungenutzt bleiben.

Betreiber von OT-Netzwerken sollten sich der bestehenden Risikolage bewusst sein: In vielen Infrastrukturen finden sich eine Vielzahl bekannter Schwachstellen und sicherheitstechnischer Defizite. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt regelmäßig in seinen Lageberichten zur IT-Sicherheit in Deutschland vor den Risiken in industriellen Netzen. Schwachstellenanalysen und Risikobewertungen in kritischer Infrastruktur und Industrie belegen seit Jahren die ausgeprägte Verwundbarkeit von OT-Umgebungen.

Abbildung 1: Die Angriffsflächen in OT-Netzwerken sind vielfältig und tief in den Systemen und Komponenten verankert, wie Schwachstellenbewertungen zwischen 2021 und 2025 herausfanden. (Bild: Rhebo)

In über 90 Prozent aller im Rahmen von Rhebo Industrial Security & Stability Assessments untersuchten OT-Netzwerke fanden sich veraltete und verwundbare Firmware, Software oder Betriebssysteme sowie Schwachstellen bei der Authentifizierung, Protokollsicherheit und Systemkonfiguration (siehe Abbildung 1). Diese Defizite sind in OT-Umgebungen nahezu überall anzutreffen.

Die detaillierte Analyse verdeutlicht die konkreten Angriffsvektoren in OT-Netzen weiter (siehe Abbildung 2). Passwörter wurden aufgrund veralteter, nicht gesicherter Protokolle fast flächendeckend als Klartext verschickt. Durch Werkeinstellungen, Fehlkonfigurationen und fehlende Segmentierung fanden sich in über 60 Prozent aller OT-Netze Systeme, die eine Verbindung zum Internet herstellen konnten oder dies aktiv (oft automatisiert) versuchten, obwohl dies weder notwendig noch gewollt war.

Doch nicht nur fehlende Zugangssicherung und Netztrennung erhöhen das Risiko. Auch grundlegende Betriebsparameter sind häufig fehlerhaft konfiguriert. So können Fehler in der Zeitsynchronisation (46 Prozent) nicht nur Probleme bei Echtzeitprozessen verursachen. Sie erschweren im Cybervorfall zudem die forensische Analyse erheblich, da ohne konsistente Zeitstempel keine verlässliche Korrelation von Log-Dateien möglich ist.

In knapp 44 Prozent aller Fälle wurden darüber hinaus während der Schwachstellenbewertungen neue und teilweise unbekannte Netzteilnehmer registriert. In der Regel liefen diese Neuregistrierungen an der Administration vorbei, denn die Systeme wuchsen „historisch" nach Bedarf.

BLINDE FLECKEN IN DER ERKENNUNG

Diese fehlende Sichtbarkeit beschränkt sich nicht nur auf die bestehenden Sicherheitslücken und -risiken der OT-Netzwerke. Der Vorfall in der polnischen Infrastruktur zeigte auch weitere blinde

Abbildung 2: Die am häufigsten in OT-Netzen identifizierten Anomalien der letzten fünf Jahre (Bild: Rhebo)

Flecken beim Erkennen maliziöser Aktivitäten im Netzwerk (siehe Abbildung 1), die frühzeitig die Alarmglocken hätten auslösen müssen:

- Kommunikation über SSL-, SMB- und RDP-Protokolle;
- Exfiltration sensibler Daten;
- neue Verbindungen zwischen bislang nicht gekoppelten Systemen;
- Nutzung zusätzlicher oder untypischer Protokolle innerhalb bestehender Verbindungen;
- Upload von Tools wie Reverse-SOCKS-Proxys, Impacket oder Wipern;
- Verbindungsaufbau zu öffentlichen IP-Adressen;
- aktive Netzwerkscans.

In OT-Netzwerken ist die Nutzung klassischer hostbasierter Angriffserkennungssysteme aufgrund limitierter CPU-Ressourcen häufig nur bedingt möglich und sinnvoll. Zudem lehnen Betreiber aktive, automatisierte Gegenmaßnahmen – etwa das Blockieren von Verbindungen oder das Isolieren von Geräten – bewusst ab, um die Stabilität kritischer Prozesse nicht zu gefährden.

Als Alternative empfiehlt das BSI in seinem Dokument BSI-CS 153 „Stationsautomatisierung" ein netzbasiertes Angriffserkennungssystem (Network Intrusion Detection System, NIDS). Solche Systeme spiegeln den Datenverkehr an definierten Abgriffspunkten – etwa Switches – rein passiv, analysieren ihn auf Anomalien und melden Abweichungen von einer zuvor definierten Baseline-Kommunikation an die Verantwortlichen.

Ein NIDS ermöglicht in OT-Umgebungen ein kontinuierliches, passives Monitoring des Netzwerkverkehrs, ohne Endgeräte zu belasten oder aktiv in kritische Prozesse einzugreifen. Durch die Anomalieerkennung lassen sich auch solche Aktivitäten identifizieren, die auf den ersten Blick legitim erscheinen – etwa bei Nutzung autorisierter Accounts.

FEHLENDE HANDLUNGSFÄHIGKEIT

Eine weitere Herausforderung in kritischen Infrastrukturen besteht auf personeller Ebene. Laut CERT Polska hatte ein hostbasiertes Angriffserkennungssystem bereits über ein halbes Jahr vor dem winterlichen Vorfall suspekte Aktivitäten auf einzelnen Systemen registriert. Diese Sicherheitslogs wurden jedoch anscheinend erst nach dem Vorfall, im Rahmen der forensischen Systemanalyse, ausgewertet. So ärgerlich das ist, so wenig verwundert es.

OT-Sicherheit ist in vielen Unternehmen noch immer Neuland. Oft fehlt qualifiziertes Personal mit klarer Verantwortung und ausreichender Zeit für OT-Sicherheit sowie ein belastbares Verständnis für den Umgang mit Angriffserkennungssystemen und deren Meldungen. Für den Einstieg kann es sinnvoll sein, externe Expertise einzubinden. Ein NIDS lässt sich in der Anfangsphase gemeinsam mit dem Anbieter betreiben, wobei Analyse und Bewertung von Anomalien unterstützt werden. Das erleichtert den Aufbau einer belastbaren OT Baseline, schafft Sicherheit bei der Einordnung von Vorfällen und beschleunigt den Kompetenzaufbau im eigenen Team. ■

JAN FISCHER
ist Head of Sales bei Rhebo.

Der Mensch als Angriffsfläche und als stärkste Verteidigung

Ein ganz normaler Arbeitstag in einem Industrieunternehmen oder einer Versorgungseinrichtung. Eine vertraut wirkende E-Mail: perfekt formuliert, inhaltlich stimmig, scheinbar vom internen IT-Team. Der Klick fühlt sich an wie Routine – und öffnet Angreifern den Weg in die Operational Technology (OT). Das bedeutet: Maschinen stehen still, Prozesse funktionieren nicht. Im schlimmsten Fall ist die Versorgungssicherheit gefährdet.

Genau hier liegt das entscheidende Problem der modernen OT-Sicherheit. Technische Schutzmaßnahmen, Netzwerksegmentierung und Monitoring sind unverzichtbar. Doch sie greifen zu kurz, wenn der Mensch zur bevorzugten Angriffsfläche wird. Claudia Plattner, Präsidentin des Bundesamts für Sicherheit in der Informationstechnik, bringt es auf den Punkt: „Die Bedrohungslage ist real, und sie ist ernst." Angreifer dringen heute kaum noch durch technische Barrieren ein. Sie schlüpfen durch die Routinen des Arbeitsalltags hindurch, gestalten Nachrichten, die sich nahtlos in die interne Kommunikation einfügen, wählen den Zeitpunkt ihrer Angriffe in besonders hektischen Momenten und nutzen natürliche menschliche Verhaltensweisen gezielt aus.

Klassische Awareness-Programme stoßen in industriellen Umgebungen besonders schnell an ihre Grenzen. Lange Schulungen, isolierte Trainingseinheiten, jährliche Pflichtmodule: Wissen verblasst, bevor es wirkt. Bedrohungen aber entwickeln sich kontinuierlich weiter. Stress, Zeitdruck und Informationsüberflutung schaffen ideale Einfallstore – gerade in kritischen Infrastrukturen, in denen Entscheidungen unter Druck getroffen werden müssen.

Sicherheitsverantwortliche in ganz Europa berichten von denselben Herausforderungen: Informationen werden schnell vergessen, Simulationen und echte Angriffe trennen oft Welten, und Mitarbeitende fühlen sich überfordert oder unzureichend vorbereitet. Was fehlt, ist kein weiteres Tool, sondern eine Verhaltensstrategie.

Den Menschen zur stärksten Sicherheitsressource machen

Prime Security Awareness verfolgt einen grundlegend anderen Ansatz: ein dauerhaftes Sicherheitsbewusstsein etablieren, das fest im Arbeitsalltag verankert ist. Kurze Lernimpulse, realistische Phishing-Simulationen, die zeigen, wie subtil Angriffe tatsächlich sind, und Echtzeit-Warnungen, die weltweite Bedrohungslagen direkt in den eigenen Berufsalltag übersetzen. Ziel ist es nicht, Sicherheitsexperten heranzubilden, sondern vielmehr, Menschen zu befähigen, das Ungewöhnliche im Gewöhnlichen zu erkennen, bevor es eskaliert.

Unternehmen, die auf diesen Ansatz setzen, berichten von klaren Ergebnissen: weniger erfolgreiche Phishing-Versuche, schnelleres Melden verdächtiger Vorgänge, größeres Vertrauen im Umgang mit unerwarteten Situationen und eine nachhaltig höhere Cybersicherheitsreife. Hinzu kommt eine klare Dokumentation zur Unterstützung der Compliance mit NIS-2, der Datenschutz-Grundverordnung (DSGVO), dem Digital Operational Resilience Act (DORA) und ISO 2700 – ein entscheidender Vorteil in regulierten Branchen und kritischen Infrastrukturen.

In einer Welt, in der Angreifer die Normalität imitieren, ist die stärkste Verteidigung eine Belegschaft, die erkennt, was sich nicht normal anfühlt. Technologie ist unverzichtbar, aber sie schützt nur, wenn Menschen informiert, aufmerksam und handlungsfähig sind. ■

Mehr dazu hier

Weitere Informationen:
Cybersecurity Awareness | Primion

Download:
Prime Security Awareness | Primion

Primion Technology GmbH
primion.io
info@primion.eu

primion

Bild: Gorodenkoff - stock.adobe.com

Compliance-Synergie zwischen NIS-2, KRITIS-Dachgesetz und EU AI Act

KI-GESTÜTZTES SICHERHEITS-MANAGEMENT IM MITTELSTAND

Drei europäische Regelwerke fordern industrielle Mittelständler gleichzeitig auf digitaler, physischer und organisatorischer Ebene heraus. Ein integrierter Governance-Ansatz soll verhindern, dass knappe Ressourcen in parallelen Compliance-Projekten verpuffen.

In vielen Industrieunternehmen zeigt sich derzeit ein ähnliches Bild: Der CISO befasst sich mit der Abwehr von Ransomware, die Fachkraft für Arbeitssicherheit mit der Unfallprävention, während der Anlagenverantwortliche veraltete Steuerungssysteme betriebssicher halten muss. Unterschiedliche Aufgabenfelder werden dabei mit denselben knappen personellen und organisatorischen Ressourcen bewältigt.

Was auf den ersten Blick wie eine Abfolge operativer Einzelprobleme aussieht, ist Ausdruck einer grundlegenden Verschiebung im regulatorischen Umfeld. Sicherheitsanforderungen, die lange getrennten Domänen zugeordnet waren, greifen zunehmend ineinander und betreffen Organisationen gleichzeitig auf digitaler, physischer und organisatorischer Ebene.

Die nationale Umsetzung der NIS-2-Richtlinie verpflichtet Betreiber wesentlicher und wichtiger Einrichtungen zu systematischem Risikomanagement, belastbarer Dokumentation und klar definierten Meldeprozessen. Parallel rückt das KRITIS-Dachgesetz die physische Resilienz kritischer Anlagen in den Fokus und soll die bisherige Trennung zwischen Cyber- und physischer Sicherheit überwinden. Dazu kommt der EU AI Act, der organisationsweite Kompetenzmaßnahmen verlangt sowie – bei Hochrisiko-KI – eine dokumentierte Governance, die Risikobewertung, menschliche Aufsicht und Verantwortlichkeiten verbindlich regelt.

Diese Verdichtung regulatorischer Anforderungen trifft den industriellen Mittelstand besonders stark. Studien zeigen, dass grundlegende IT-Sicherheitsanforderungen in vielen kleineren und mittleren Unternehmen (KMU) bislang nur teilweise umgesetzt sind. Gleichzeitig geraten gerade diese Unternehmen verstärkt ins Visier von Cyberangreifern, da spezialisierte Stabsstellen, klare Governance-Strukturen und redundante Ressourcen häufig fehlen. Die Ursachen dafür liegen weniger in mangelnder Sensibilität als in strukturellen Grenzen: Mehrere komplexe Regelwerke wirken zeitgleich auf dieselben Organisationen ein.

DREI SICHERHEITS-DOMÄNEN, DIE NICHT MEHR GETRENNT FUNKTIONIEREN

Fertigungsunternehmen bewegen sich traditionell in drei Sicherheitsdomänen, die sich historisch getrennt voneinander entwickelt haben:

- Die **Arbeitssicherheit** ist der älteste und am stärksten normierte Bereich. Arbeitgeber müssen für jeden Arbeitsplatz eine Gefährdungsbeurteilung durchführen; technisch-operative Anforderungen ergänzt das Regelwerk der DGUV. Sicherheitsbeauftragte und Fachkräfte für Arbeitssicherheit übernehmen klar definierte Rollen. Alles muss umfassend dokumentiert und überprüfbar ausgestaltet sein.

- **Geräte- und Betriebssicherheit:** Die Sicherheit technischer Anlagen und Betriebsmittel unterliegt spezifischen Betreiber- und Prüfpflichten. Prüfungen elektrischer Betriebsmittel, Betriebsanweisungen und Prüfprotokolle bilden eine eigenständige Dokumentationslandschaft. Die Verantwortung liegt bei der verantwortlichen Elektrofachkraft (VEFK), einem ressourcenkritischen Rollenprofil. Auch hier folgt die Logik einem etablierten Schema: Anlage prüfen, Zustand bewerten, Nachweis führen. Die Nähe zur Arbeitssicherheitslogik ist Ausdruck eines gemeinsamen historischen Regelungsimpulses.

- Die **IT-/OT-Sicherheit** ist die regulatorisch dynamischste Domäne und mit besonders komplexen Dokumentationsanforderungen verbunden. Während OT-Systeme historisch vom Internet getrennt waren, ist diese Trennung in modernen Fertigungsumgebungen weitgehend aufgehoben. Predictive-Maintenance-Lösungen, ERP-OT-Schnittstellen und Industrial-IoT-Komponenten verbinden IT und OT strukturell.

Jeder Bereich folgt eigenen Regelwerken und Rollenmodellen, beruht aber auf demselben Grundprinzip: Risiken erkennen, Maßnahmen ableiten, Wirksamkeit prüfen. Weil Produktionsanlagen, IT-Systeme und datengetriebene Anwendungen immer stärker vernetzt sind, lassen sich Sicherheitsereignisse kaum noch eindeutig einem einzelnen Bereich zuordnen. Ein kompromittiertes OT-System kann gleichzeitig einen Cybersicherheitsvorfall, ein physisches Resilienzproblem und – bei Beteiligung von KI-Komponenten – einen Governance-Fall im Sinne des EU AI Act darstellen.

Gerade diese Konvergenz bildet den Ausgangspunkt für ein integriertes Sicherheitsmanagement. Es setzt nicht bei Einzelmaßnahmen an, sondern bei der Governance – mit gemeinsamen Prinzipien, Begriffen und Entscheidungsstrukturen. Wer diese Zusammenhänge ignoriert und separate Compliance-Initiativen verfolgt, erhöht die Belastung der Sicherheitsbereiche; wer sie systematisch nutzt, stärkt die organisatorische Resilienz. Organisationen, die diesen Schritt nicht gehen, erreichen zwar formale Compliance, handeln sich aber erhebliche organisatorische Reibungsverluste ein.

ANFORDERUNGEN ÜBERLAPPEN SICH

Regulatorische Überschneidungen sind kein Zufall.[1, 5] Die Forschung zur europäischen Regulierung zeigt seit Längerem, dass Risikodokumentation und Rechenschaftspflicht als zentrale Steuerungsinstrumente in nahezu allen relevanten Rahmenwerken verankert sind.[1] In der Praxis werden diese Anforderungen jedoch häufig getrennt umgesetzt, was zu erheblichem Mehraufwand führt.

Für Unternehmen ergibt sich daraus eine klare Konsequenz: Compliance-Synergien entstehen nicht von selbst, sondern müssen gezielt hergestellt werden. Eine gemeinsame Governance-Infrastruktur bündelt funktional gleichgerichtete Pflichten, steigert die Effizienz und erhöht

zugleich die Robustheit gegenüber künftigen regulatorischen Anpassungen.

Der strategische Mehrwert reicht dabei über aktuelle Anforderungen hinaus. Die Politikwissenschaftlerin Anu Bradford beschreibt mit dem „Brussels Effect", wie EU-Regulierung über Marktmechanismen häufig globale Wirkung entfaltet und zum faktischen Standard wird – auch ohne unmittelbares Durchsetzungsmandat. Diese internationale Ausstrahlung verleiht der europäischen Regulierung zusätzliche strategische Bedeutung.

Wie stark sich die Regelwerke überlappen, macht Tabelle 1 deutlich: Sechs von acht Governance-Anforderungen finden sich in mindestens zwei, Risikodokumentation, menschliche Aufsicht und Schulung sogar in allen drei Rahmenwerken.[1] Eine gemeinsame Governance-Infrastruktur reduziert dadurch den Dokumentationsaufwand und erhöht die Audit-Robustheit, da Nachweise domänenübergreifend genutzt werden können.[2] Lediglich zwei Anforderungen bleiben spezifisch: Physische Schutzmaßnahmen betreffen ausschließlich das KRITIS-Dachgesetz, das KI-Systeminventar nur den EU AI Act – beides lässt sich aber in bestehende Dokumentationsstrukturen integrieren.

GOVERNANCE ZUERST, DANN WERKZEUGE

Die Tabelle zeigt, wo integrierte Governance ansetzen kann. Bevor Unternehmen entscheiden, wie sie regulatorische Anforderungen erfüllen, müssen sie aber zunächst ihren organisatorischen Ausgangspunkt klären: Wer trägt Verantwortung, wie fließen Informationen zwischen den Bereichen und wann greifen Eskalationsmechanismen? Laut Bolgouras et al. erhöhen Technologieprojekte, die auf ungeklärte Governance-Strukturen treffen, die Compliance-Risiken, statt sie zu senken.[1] Daraus ergibt sich eine klare Reihenfolge: zuerst Governance, dann Architektur, zuletzt Werkzeuge.

Vier Voraussetzungen müssen dafür mindestens erfüllt sein (siehe Infokasten 1): Die Geschäftsführung trägt die Gesamtverantwortung – NIS-2 und KRITIS-Dachgesetz machen das zur Haftungsfrage. Die drei Sicherheitsbereiche benötigen ein einheitliches Risikovokabular, damit Audit-Nachweise bereichsübergreifend gelten. Gefährdungsbeurteilungen, Prüfprotokolle und IT-Risikoberichte müssen einem gemeinsamen Dokumentationsstandard folgen. Und Meldeketten samt Eskalationslogik müssen vorab festgelegt, dokumentiert und geübt sein.

Wo ein Unternehmen auf diesem Weg steht, lässt sich mit dem Security-Process-Improvement-Modell (SPI) nach Kutsche und Jackwerth-Rice einordnen.[3] Es bewertet die Governance-Reife über vier Bereiche – Sicherheitsstrategie, Prozesse und Dokumentation, Kompetenz und Compliance-Kultur sowie Führung und Ressourcen – auf jeweils vier Stufen: „Initial" (ad hoc), „Kontrolliert" (taktisch), „Effizient" (strategisch) und „Optimiert" (nachhaltig). Die Stufen beschreiben organisatorisches Verhalten, nicht Technik. Unternehmen ordnen sich der Stufe zu, die ihrem Alltag am nächsten kommt – und sehen so direkt, was der nächste Entwicklungsschritt wäre (siehe Infokasten 2).

Anforderung	NIS-2-UmsG	KRITIS-DachG	EU AI Act
Risikoinventar und -klassifikation	Risikomanagementpflichten	Risikoanalyse und Risikobewertung	Risikoklassifikation (Hochrisiko-Systeme)
Dokumentation und Audit-Trail	Nachweispflichten via Audits/Prüfungen/Zertifizierungen, Dokumentation	Prüf-/Nachweiskontext (Vor-Ort-Prüfungen zulassen/begleiten)	Technische Dokumentation, Protokollierung, Aufbewahrung, Behördenkooperation
Leitungspflicht/Oversight (Governance-Verantwortung)	Geschäftsleitung muss Maßnahmen umsetzen und überwachen	Leitung billigt/überwacht Resilienzmaßnahmen (Managementpflichten)	Menschliche Aufsicht ausdrücklich normiert
Vorfallmeldung und Eskalation	Meldepflichten (u. a. Erstmeldung binnen 24 h)	Meldung von Sicherheitsvorfällen	Meldung schwerwiegender Vorfälle
Lieferketten-/Anbietersicherheit	Sicherheit in der Lieferkette	Resilienzmaßnahmen inkl. „alternative Lieferanten/Lieferketten"	Ressourcenmanagement inkl. Versorgungssicherheit
Schulung und Kompetenznachweis	Geschäftsleitungs-Schulungspflicht	Resilienzmaßnahmen inkl. Trainings, Schulungen, Übungen	KI-Kompetenz (organisationsweit)
Physische Schutzmaßnahmen	–	Resilienzmaßnahmen (inkl. z. B. Sicherheitsmanagement)	–
KI-System-Inventar (als Governance-Artefakt)	–	–	Identifikation, Klassifikation und Verwaltung eingesetzter KI-Systeme (aber keine allgemeine Pflicht für ein KI-Inventar)

Tabelle 1: Governance-Anforderungen im Dreiklang der Sicherheit

KI KANN UNTERSTÜTZEN

KI-gestützte Werkzeuge können bestehende Governance-Strukturen sinnvoll unterstützen, etwa bei Dokumentation, Fristenüberwachung oder der strukturierten Auswertung interner Wissensbestände. Sinnvoll einsetzbar sind sie ab der Stufe „Kontrolliert", strategisch empfehlenswert ab „Effizient". Voraussetzung ist, dass diese Systeme ausschließlich auf verifizierte Organisationsdokumente zugreifen und ihre Ergebnisse nachvollziehbar bleiben. Entscheidungen über Risiken, Meldepflichten oder Verantwortlichkeiten bleiben jedoch menschliche Aufgaben. KI ersetzt keine Governance, sondern macht vorhandene Strukturen skalierbar.

INFOKASTEN 1

Voraussetzungen/ Governance-Grundlagen

1. *Die **Geschäftsführung** trägt die Gesamtverantwortung; NIS-2 (§ 38 BSIG) und das KRITIS-Dachgesetz (§ 15) machen dies zur Haftungsfrage (Bundesregierung, 2025a). Erforderlich ist eine klare Koordinationsrolle, die Arbeits-, Geräte- und Betriebssicherheit sowie IT/OT-Sicherheit als Mandat bestehender Strukturen bündelt.*
2. *Die drei Sicherheitsdomänen verwenden unterschiedliche Begriffe für vergleichbare Sachverhalte, etwa „Gefährdung", „Bedrohung" oder „Resilienzlücke". Ein einheitlich definiertes, domänenübergreifendes **Risikovokabular** ist Voraussetzung dafür, Audit-Nachweise bereichsübergreifend nutzen zu können.*
3. *Gemeinsame **Dokumentationsstandards** fehlen oft: Gefährdungsbeurteilungen, Prüfprotokolle und IT-Risikoberichte nutzen unterschiedliche Formate. Ein einheitliches Schema mit Risiko, Maßnahme und Nachweis macht Belege über alle drei Regelwerke hinweg nutzbar.*
4. *Definierte **Meldeketten und Eskalationslogik** sind zentral: NIS-2 verlangt eine Erstmeldung binnen 24 Stunden bei erheblichen Vorfällen. Diese Frist ist nur einhaltbar, wenn Zuständigkeiten vorab festgelegt, dokumentiert und geübt sind – domänenübergreifend bei OT-Vorfällen.*

INFOKASTEN 2

Selbstverortung mit SPI© für integriertes Sicherheitsmanagement

SPI-Domäne	Initial	Kontrolliert	Effizient	Optimiert
Sicherheitsstrategie	Keine Gesamtstrategie, Regelwerke reaktiv umgesetzt, Sicherheitsbereiche isoliert	Bereichsrichtlinien vorhanden; Mindestanforderungen dokumentiert; keine domänenweite Abstimmung	Einheitliche Sicherheitsstrategie, Domänen integriert, regelmäßige KPI-Reviews	Sicherheitsstrategie ist Teil der Unternehmensziele; neue Risiken werden früh antizipiert
Prozesse & Dokumentation	Ad-hoc-Dokumentation: Prüfungen, Gefährdungen und IT-Risiken uneinheitlich oder fehlend	Standardprozesse je Domäne, qualifiziertes Fachpersonal, revisionssichere, getrennte Dokumentation	Einheitlicher Dokumentationsstandard; Nachweise domänenübergreifend nutzbar, KI sinnvoll einsetzbar	Integriertes Dokumentationssystem mit automatisierter Qualitätsprüfung und kontinuierlicher Optimierung
Kompetenz & Compliance-Kultur	Sicherheit als individuelle Verantwortung. Schulungen anlassbezogen, nicht systematisch. Compliance-Bewusstsein gering	Sicherheit individuell; Schulungen anlassbezogen, kaum systematisch, geringes Compliance-Bewusstsein	Domänenübergreifende Schulungen, externe Audits zur Optimierung, Sicherheit als Führungsaufgabe	Verankerte Compliance-Kultur, kontinuierliche Verbesserung; Akkreditierungen als Signal
Führung, Steuerung & Ressourcen	Keine KPIs; Budget ad hoc; Geschäftsführung kaum eingebunden; Haftungsrisiken unadressiert	Grundkennzahlen (Vorfallrate, Prüfquote), Budget geplant, GF-Reporting etabliert	Integriertes KPI-System, Kosten-Nutzen der Sicherheit, KI-gestütztes Reporting	Profitabilität im Sicherheitsmanagement: langfristige Optimierung ohne Wachstumsverluste

Farbcode: Rot = Initial (ad hoc) | Gelb = Kontrolliert (taktisch) | Grün = Effizient (strategisch) | Blau = Optimiert (nachhaltig) | KI-gestützte Werkzeuge sind ab Stufe „Effizient" strategisch empfehlenswert; auf Stufe „Kontrolliert" in Teilbereichen möglich.

Organisationen, die ihren Reifegrad mithilfe des SPI-Modells bestimmt und mindestens die Stufe „Kontrolliert" erreicht haben, haben dafür die notwendige Vorarbeit geleistet. Erst dann stellt sich die Frage, welche Werkzeuge die bestehende Governance wirksam unterstützen. Prozessuale Grundlagen sind dabei unverzichtbar: Fehlen sie, sind KI-Lösungen strukturell instabil. Technologie kann Governance-Lücken kurzfristig überdecken, löst das zugrunde liegende Organisationsproblem aber nicht.

Als tragfähige Architektur hat sich in diesem Kontext der „LLM plus RAG"-Ansatz erwiesen. Dabei greift ein Sprachmodell ausschließlich auf den verifizierten internen Dokumentenbestand eines Unternehmens zu, etwa Gefährdungsbeurteilungen, Prüfprotokolle, Richtlinien oder Vorfallberichte. Durch Retrieval-Augmented Generation (RAG) werden relevante Dokumente vor der Antworterzeugung herangezogen, sodass Ergebnisse überprüfbar und quellenbasiert bleiben – eine zentrale Voraussetzung für revisionssichere Compliance-Dokumentation.[4]

FAZIT: DIE RICHTIGE REIHENFOLGE ENTSCHEIDET

NIS-2, KRITIS-Dachgesetz und EU AI Act sind keine isolierten Regelwerke, sondern unterschiedliche Ausprägungen eines gemeinsamen Governance-Gedankens. Risiken sollen erkannt, dokumentiert, überwacht und verantwortet werden. Dass sich die Anforderungen dabei überschneiden, ist keine Belastung, sondern eine Ressource. Organisationen, die Governance vor Technologie priorisieren, schaffen die Grundlage dafür, dass digitale Werkzeuge – einschließlich KI – tatsächlich zur Erhöhung von Sicherheit und Resilienz beitragen.

Entscheidend bleibt die Reihenfolge. Das SPI-Modell macht deutlich, dass ein integriertes Sicherheitsmanagement keinen einmaligen Schritt darstellt, sondern ein Entwicklungspfad ist. Organisationen auf niedrigen Reifestufen benötigen zunächst belastbare Governance-Strukturen, nicht KI-Projekte. Ab der Stufe „Kontrolliert" können digitale Werkzeuge zur Dokumentation und Fristenüberwachung eingesetzt werden; auf der Stufe „Effizient" werden KI-gestützte Systeme zum strategischen Hebel.[5, 2]

Eine einfache Prüffrage unterstützt die Einordnung: Sind die vier Governance-Voraussetzungen aus Infokasten 1 erfüllt? Falls nicht, handelt es sich nicht um ein KI-, sondern um ein Governance-Projekt. Die Abfolge bleibt eindeutig: zuerst Governance, dann Architektur, zuletzt Werkzeuge. Das ist keine Absage an KI im Sicherheitsmanagement, sondern die Voraussetzung für ihren wirksamen Einsatz. ■

INFOKASTEN 3

Einsatzfelder und Grenzen KI-gestützter Werkzeuge

1. ***Ab SPI-Stufe „Kontrolliert"*** *können KI-gestützte Werkzeuge Dokumentationen, Prüfberichte und Risikoanalysen konsistent aktualisieren, Fristen aus BetrSichV, DGUV und NIS-2 überwachen sowie den Zugriff auf verifizierte Sicherheitsdokumente in natürlicher Sprache ermöglichen (Walker et al., 2026).*
2. ***Vor technischer Umsetzung ist organisatorische Vorarbeit nötig:*** *Die Risikoterminologie der drei Domänen ist zu vereinheitlichen. Zugriffsrechte, Freigaben und Versionierung sind vorab festzulegen. KI kann unterstützen, aber keine gemeinsame Risikosprache schaffen.*
3. ***Was KI nicht leisten kann:*** *Meldeketten entstehen nicht durch Technik. Wer einen Vorfall fristgerecht an das BSI meldet, ist eine organisatorisch-rechtliche Entscheidung. Gleiches gilt für die Hochrisikoeinstufung nach EU AI Act, die qualifizierte menschliche Bewertung verlangt. KI unterstützt die Vorbereitung und Dokumentation; menschliche Aufsicht ist Pflicht.*

Literatur

[1] *Bolgouras, V., Zarras, A., Leka, C., Stylianou, I., Farao, A., & Xenakis, C. (2025). EU regulatory ecosystem for ethical AI. AI and Ethics, 5, 5063–5080. https://doi.org/10.1007/s43681-025-00749-x, https://link.springer.com/article/10.1007/s43681-025-00749-x*

[2] *Engels, B., Lang, T., & Scheufen, M. (2025). KI-Verordnung, NIS-2-Richtlinie und Cyber Resilience Act: Auswirkungen auf KMU. Institut der deutschen Wirtschaft Köln / IW Consult / Ramboll Management Consulting. Kurzstudie im Auftrag des BMWE. https://www.iwkoeln.de/studien/barbara-engels-thorsten-lang-marc-scheufen-auswirkungen-auf-kmu.html*

[3] *Kutsche, R., & Jackwerth-Rice, T. (2024). Security process improvement (SPI) framework – A method to improve your security management approach (SMAP) (Version 1.0) [White paper]. bkm consultants. https://www.researchgate.net/publication/382949819*

[4] *Schneider, J., Dietz, M., Schiffer, A., & Klöbe, T. (2025). Retrieval-Augmented Generation (RAG). Business & Information Systems Engineering, 67, 357–367. https://doi.org/10.1007/s12599-025-00945-3, https://link.springer.com/article/10.1007/s12599-025-00945-3*

[5] *Smuha, N. A. (2021). From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence. Law, Innovation and Technology, 13(1), 57–84. https://doi.org/10.1080/17579961.2021.1898300*

[6] *Walker, C., Aslansefat, K., Akram, M. N., & Papadopoulos, Y. (2026). RAGuard: A Novel Approach for In-Context Safe Retrieval Augmented Generation for LLMs. In Springer Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-032-05073-1_13, https://link.springer.com/chapter/10.1007/978-3-032-05073-1_13*

DR. THOMAS JACKWERTH
ist Unternehmensberater sowie assoziierter Wissenschaftler am Fraunhofer-Institut für System- und Innovationsforschung (ISI). Seine Schwerpunkte sind KI-Governance und Compliance.

PROF. DR. RALF KUTSCHE
ist Professor für Gesundheitsökonomie sowie Senior Management Consultant mit den Schwerpunkten Strategieberatung in technologieorientierten Unternehmen und Verwaltungen.

DR.-ING. THORSTEN NEUMANN
ist öffentlich bestellter und vereidigter Sachverständiger für Gefährdungsbeurteilungen an Arbeitsplätzen und Geschäftsführer eines Beratungsunternehmens für Industriekunden.

20. – 24. April 2026

THINK TECH FORWARD

Globaler Treffpunkt für industrielle Transformation,
wo Innovation und Verantwortung zusammenkommen,
um die Zukunft der Produktion zu gestalten.
www.hannovermesse.de/hm26

Ihr Zugang zur Hannover Messe!

THINK TECH FORWARD

HANNOVER MESSE

Unveränderliche Backups:

DIE LETZTE VERTEIDIGUNGS-LINIE RICHTIG GESTALTEN, BETREIBEN UND PRÜFEN

Ransomware-Gruppen attackieren längst nicht mehr nur Produktivsysteme. Sie versuchen systematisch, Backup-Infrastrukturen zu kompromittieren, um den Erpressungsdruck zu maximieren. Unveränderliche Sicherungen (Immutable Backups) gelten deshalb als letzte Verteidigungslinie. Unser Autor zeigt, welche technischen und organisatorischen Voraussetzungen nötig sind, damit diese Linie tatsächlich hält.

Angreifer nehmen gezielt Sicherungen ins Visier: Sie versuchen etwa, Aufbewahrungsfristen für Backups zu verkürzen, Soft-Delete zu deaktivieren oder komplette Sicherungsspeicher zu löschen. Aktuelle Schutzkonzepte setzen deshalb auf drei Bausteine – unveränderliche Speicherziele, eine konsequente Isolierung der Kopien und eine Automatisierung, die bei Bedrohungsalarmen Schutzmechanismen aktiviert, Aufbewahrungsfristen einfriert und Wiederherstellungspunkte vor vorzeitigem Löschen schützt. Praxiserfahrungen zeigen, dass sich so die Wahrscheinlichkeit eines sauberen Restores deutlich steigern lässt.

WAS „UNVERÄNDERLICH“ TECHNISCH BEDEUTET

Im Kontext von Backups bezeichnet „Immutability“ Speicher- und Steuerungsmechanismen, die das Löschen oder Ändern von Backup-Objekten bis zum Ende der Aufbewahrungsfrist technisch verhindern. Dazu zählen WORM-Speichersysteme (Write Once, Read Many), Objektspeicher mit Retention-Regeln und rechtlich belastbaren Sperren sowie Backup-Repositories, die applikationsseitig „Write Once“-Eigenschaften erzwingen. Entscheidend dabei ist, dass die Sperren auch privilegierte Zugriffe einschließen und dass das Deaktivieren von Schutzmechanismen nur über einen mehrstufigen Freigabeprozess möglich ist.

Dabei gilt: Snapshots sind zwar hilfreich, taugen aber nicht als vollwertiges Backup, weil sie an

den Primärspeicher gekoppelt bleiben. Einen robusteren Schutz bietet die Kombination aus

- klar definierten Vorgaben für den maximal zulässigen Datenverlust (Recovery Point Objective, RPO) und die maximal akzeptable Wiederherstellungszeit (Recovery Time Objective, RTO),
- unveränderlich gespeicherten Backups und
- einer durchgängigen Sicherungsarchitektur.

BAUSTEINE EINER TRAGFÄHIGEN ARCHITEKTUR

Eine belastbare Immutability-Strategie ruht auf drei Ebenen: Speicher, Backup-Software und Isolierung.

Auf der Speicherebene kommen Objektspeicher mit definierten Aufbewahrungsregeln und optionalen rechtlichen Sperren zum Einsatz. In Cloud-Umgebungen nutzen Administratoren dafür spezielle Backup-Vaults mit Schutz vor versehentlichem Löschen und gesperrter Unveränderlichkeit. Private Endpoints, verschlüsselte Speicherschlüssel und restriktive Netzwerkpfade sichern ergänzend die Datenflüsse ab. Je nach Umgebung können WORM-Bänder oder Dateisysteme mit Write-Once-Eigenschaft die Strategie ergänzen. Ihre Wirkung entfalten diese Bausteine allerdings nur, wenn verbindliche Richtlinien eine nachträgliche Verkürzung der Aufbewahrungsfristen ausschließen.

Auf der Ebene der Backup-Software geht es um gehärtete Ablageorte, getrennte Konten für Betrieb und Verwaltung sowie Konfigurationen, die die Unveränderlichkeit zusätzlich kryptografisch signieren oder anderweitig auf Anwendungsebene absichern. Kritische Eingriffe wie das Aufheben von Sperren sollten nur über eine Mehrpersonenfreigabe möglich sein.

Eine tragfähige Isolierung lässt sich entweder physisch umsetzen – etwa wenn eine Kopie die Produktionsumgebung verlässt – oder logisch, indem Netze, Identitätsverwaltung und Betriebsabläufe konsequent voneinander getrennt werden. Konkret heißt das: getrennte Netzsegmente, eine eigenständige Konten- und Rollenverwaltung in einem separaten Verzeichnisdienst oder Mandanten sowie automatisierte Abläufe nach dem Pull-Prinzip, bei denen das Zielsystem die Sicherung abholt, statt dass das Quellsystem sie aktiv überträgt. Mindestens ebenso wichtig ist die Absicherung der Steuerungsebene, denn ein erfolgreicher Angriff auf die Verwaltungsfunktionen kann genügen, um viele Systeme gleichzeitig zu kompromittieren.

CLOUDNATIVE UMSETZUNG

In Cloud-Umgebungen lassen sich die beschriebenen Architekturprinzipien mit plattformeigenen Diensten umsetzen. Backup-Vaults, die Unveränderlichkeit unterstützen, verhindern das Löschen oder Modifizieren von Wiederherstellungspunkten vor Ablauf der Aufbewahrungsfrist. In der Praxis bringt das allerdings Nebenwirkungen mit sich, die Administratoren einkalkulieren müssen: Eine Verkürzung der Aufbewahrungsfrist ist nicht möglich, solange die Sperre greift. Wird ein Workload gelöscht und anschließend in gleicher Form neu bereitgestellt, lassen sich ältere, gesperrte Wiederherstellungspunkte häufig nicht mehr zuordnen oder verwenden. Änderungen am Lebenszyklus eines Systems sollten deshalb konsequent gegen die gewählten Aufbewahrungsfristen geprüft werden. Ergänzend erhöht eine saubere Absicherung von Netzwerk und Identitäten die Widerstandskraft – etwa durch Private Endpoints, klar definierte Rollen und eine Mehrpersonenfreigabe für sensible Eingriffe.

In hybriden und lokalen Umgebungen kombinieren viele Organisationen ein separates, gehärtetes Sicherungsziel in der eigenen Infrastruktur mit einer zweiten Kopie in einem Objektspeicher, der verbindliche Aufbewahrungsfristen pro Objekt erzwingt. Für lange Aufbewahrung und zusätzlichen Schutz kommt häufig eine weitere Ebene hinzu, die räumlich getrennt betrieben wird – etwa ein externes Archiv. So entstehen kurze Wiederherstellungszeiten vor Ort, während die isolierte Kopie einen belastbaren Schutz gegen Manipulation und Löschversuche in der Produktionsumgebung bietet.

Auch Software-as-a-Service-(SaaS)-Anwendungen benötigen unabhängige Sicherungen, die außerhalb des jeweiligen Anbieters liegen. Die in vielen Produkten enthaltenen Papierkörbe sind kein gleichwertiger Ersatz. Auch hier sollte die Zielumgebung unveränderlich sein und in einer separaten Steuerungsdomäne betrieben werden – nur so bleibt die Wiederherstellungsfähigkeit erhalten, wenn das Quellsystem ausfällt oder kompromittiert wird.

VIER VERBREITETE IRRTÜMER

Obwohl vielen Verantwortlichen klar ist, worauf es bei unveränderlichen Backups ankommt, scheitern Organisationen in der Praxis dennoch regelmäßig an denselben Fehleinschätzungen. Erstens gehen viele Teams davon aus, dass Snapshots bereits eine vollständige Datensicherung darstellen. Wie oben beschrieben bleiben Snapshots jedoch an den Primärspeicher gekoppelt – ohne isolierte und unveränderliche Kopie bleibt ein Angriff auf den Primärspeicher ein direktes Risiko für die Wiederherstellung. Zweitens unterschätzen Administratoren die Folgen für die Flexibilität: Wer Unveränderlichkeit aktiviert, kann Aufbewahrungsfristen nicht mehr beliebig verkürzen. Vor Migrationen oder Systemänderungen müssen die Auswirkungen auf bestehende Sperren bewertet werden. Drittens wiegt eine unveränderliche Kopie ohne getrennte Identitäten und Netzpfade Verantwortliche in falscher Sicherheit – auf der Steuerungsebene bleibt sie angreifbar. Viertens verkennen viele Organisationen die Rolle der Governance: Ohne verbindliche Richtlinien, regelmäßige Audits und klare Verantwortlichkeiten bleiben selbst technisch einwandfreie Sicherungen ein unvollständiger Schutz.

REIFEGRAD MESSEN, WIEDERHERSTELLUNG TESTEN

Deshalb brauchen Organisationen Kennzahlen, die den Reifegrad ihrer Sicherungsstrategie greifbar machen. Dazu gehören RPO und RTO, der Anteil tatsächlich unveränderlich gesicherter Workloads, die Zeit bis zum ersten sauberen Restore und der Anteil erfolgreicher Wiederherstellungen, die zuvor auf Schadsoftware geprüft wurden. Automatisierung unterstützt diesen Weg: Bei sicherheitsrelevanten Alarmen können Workflows automatisch Schutzmaßnahmen aktivieren, Aufbewahrungsfristen einfrieren und die Angriffsfläche für Löschoperationen verkleinern. Das entlastet die Teams und kann verhindern, dass in einer kritischen Lage wertvolle Wiederherstellungspunkte verloren gehen.

Tragfähig wird das Ganze erst durch eine saubere Governance: Eine Backup- und Recovery-Steuerung muss fachliche Anforderungen an Verfügbarkeit und Wiederherstellbarkeit mit Aufbewahrungspflichten und nachvollziehbaren Kontrollen verknüpfen. Wer die Sicherungsstra-

tegie sauber in die Regelwerke des Informationssicherheitsmanagements einbettet, erleichtert Audits, erhöht die Vergleichbarkeit zwischen Bereichen und schafft Klarheit über Mindeststandards. Dokumente, die Anforderungen aus etablierten Normen wie ISO 27001 abbilden, haben sich in der Praxis bewährt und helfen, den Nachweis dauerhaft zu führen.

KONKRETES VORGEHEN

Wer Immutable Backups einführen will, kann sich an sechs Schritten orientieren: Am Anfang steht ein vollständiges Inventar: Welche Systeme und Daten sind kritisch? Welche regulatorischen Aufbewahrungsfristen gelten? Welche Wiederherstellungsziele sind verbindlich? Auf dieser Grundlage definieren die Verantwortlichen eine Zielarchitektur, die mindestens eine unveränderliche Kopie und eine Isolierungsstufe vorsieht.

Im zweiten Schritt legen sie Richtlinien für Aufbewahrungsfristen und Sperren fest, die eine spätere Verkürzung ausschließen. Drittens härten sie die Steuerungsebene – mit getrennten Administrationskonten, Mehrpersonenfreigabe für kritische Eingriffe und streng geregelten Notfallzugängen. Viertens setzen sie die Isolierung technisch konsequent um: Netz und Identität trennen, Kopien in eigenständigen Konten oder Mandanten führen, Datenflüsse so gestalten, dass möglichst Pull-Mechanismen zum Einsatz kommen. Ergänzend helfen Malware-Prüfungen auf Datenpfaden und automatische Schutzlogik, die bei Bedrohungsalarmen greift.

Fünftens üben die Teams die Wiederherstellung regelmäßig. Die Ergebnisse fließen dokumentiert und geprüft in die Verbesserung der Architektur zurück. Sechstens braucht die Umgebung ein Lebenszyklusmanagement, das Änderungen an Workloads frühzeitig gegen die Unveränderlichkeitsregeln spiegelt und Speicherbedarf sowie Kosten realistisch plant.

FAZIT

Unveränderliche Backups sind kein einzelnes Produkt, sondern ein Sicherheitsprinzip. Es verbindet geschützte Speicherziele, gehärtete Steuerungsebenen, echte Isolierung und geübte Wiederherstellung. Richtig umgesetzt verkürzt es die Zeit bis zur Rückkehr in den Betrieb, reduziert den Erpressungsdruck und stärkt die Widerstandsfähigkeit der Organisation. Die Erfahrung aus Projekten zeigt: Dieser Ansatz trägt besonders dann, wenn Technik, Governance und Automatisierung gemeinsam gedacht und nachweisbar gelebt werden. ■

ZERO TRUST DATA RESILIENCE: BACKUP NACH DEM ASSUME-BREACH-PRINZIP

Das Framework Zero Trust Data Resilience (ZTDR) überträgt die Prinzipien der Zero-Trust-Sicherheit gezielt auf Datensicherung und Wiederherstellung. Entwickelt von Numberline Security in Zusammenarbeit mit Veeam, baut es auf dem Zero Trust Maturity Model (ZTMM) der US-amerikanischen Cybersecurity and Infrastructure Security Agency (CISA) auf und ergänzt drei backup-spezifische Grundsätze:

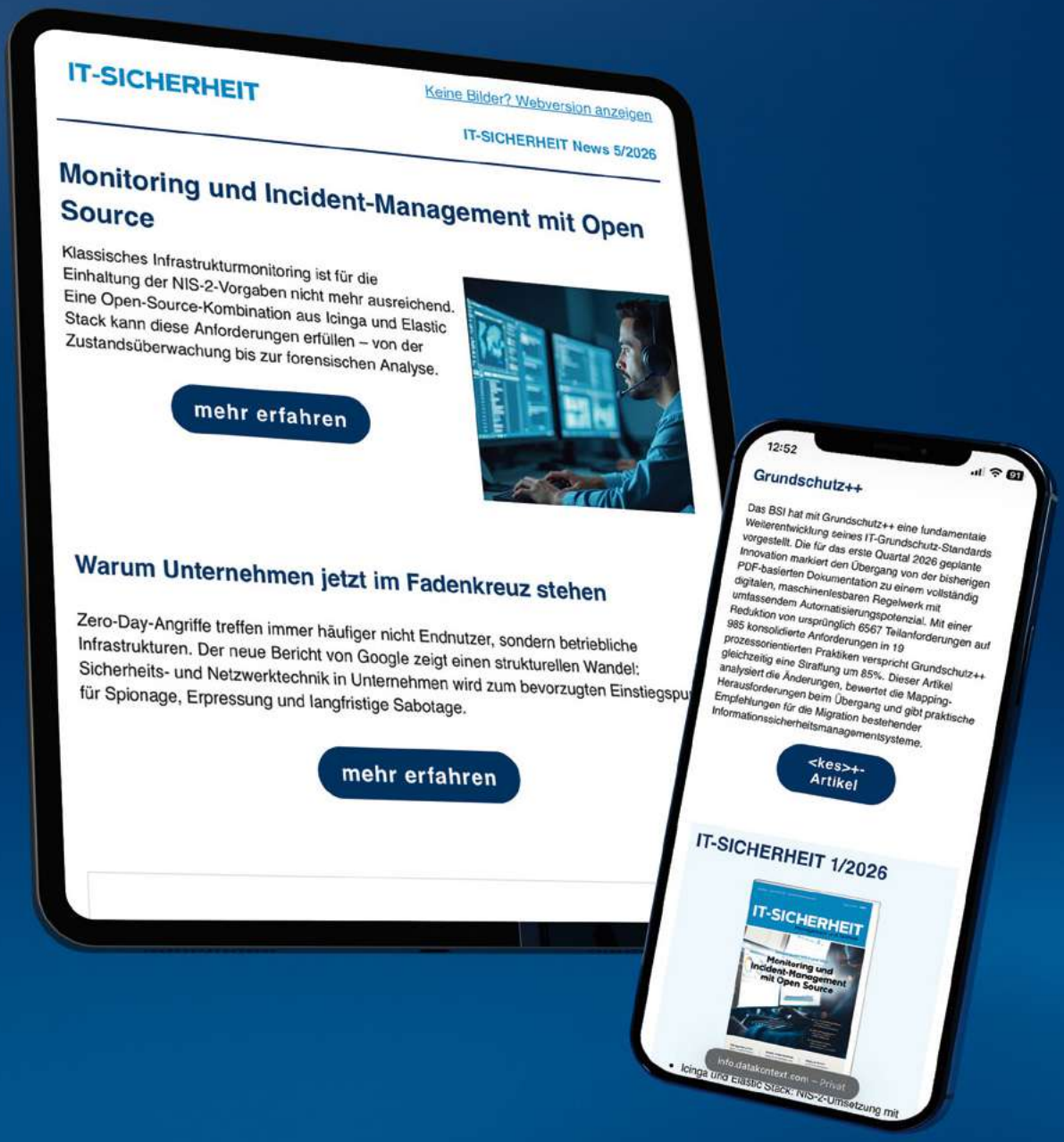
- ***Trennung von Backup-Software und Backup-Speicher:** ZTDR fordert eine konsequente Segmentierung beider Komponenten in separate Resilienz-Zonen. Selbst wenn ein Angreifer die Sicherungssoftware kompromittiert, soll eine intakte Kopie der Daten auf dem getrennten Speicherziel erhalten bleiben.*
- ***Mehrere Datenresilienz-Zonen:** Die Backup-Infrastruktur wird in mindestens drei Zonen unterteilt – Backup-Software, primärer und sekundärer Backup-Speicher. ZTDR empfiehlt dafür eine erweiterte 3-2-1-1-0-Regel: drei Datenkopien auf zwei verschiedenen Medien, davon eine extern, mindestens eine unveränderlich oder per Air-Gap isoliert – und null Fehler bei regelmäßigen Restore-Tests.*
- ***Unveränderlicher Speicher mit Zero Access:** Mindestens ein Backup-Speicher muss unveränderlich sein. ZTDR verschärft dieses Prinzip durch das Zero-Access-Konzept: Auf dem gehärteten Speicherziel wird keinerlei Root- oder Betriebssystemzugriff gewährt. So sollen auch kompromittierte Administratorkonten keine Möglichkeit haben, Unveränderlichkeitseinstellungen zu deaktivieren.*

Technisch setzt ZTDR auf S3-kompatiblen Objektspeicher mit Object Lock. Im sogenannten Compliance-Modus lassen sich Sperren weder durch Administratoren noch durch den Root-User aufheben – im Unterschied zum flexibleren Governance-Modus, der manuelle Eingriffe unter bestimmten Bedingungen erlaubt.

Quelle: Andy French, „Zero Trust fürs Backup – Besserer Schutz gegen Ransomware mit Zero-Trust-Data-Resilience", <kes> 2025#2; Jason Garbis, „Zero Trust Data Resilience", Numberline Security Whitepaper, Revision 1.1, Mai 2024

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.



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

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

Systemisches Risiko Erschöpfung

AUSGEBRANNT AN DER CYBERFRONT

Stress und Erschöpfung gehören für viele Fachleute der Cybersicherheitsbranche längst zum Alltag. Dabei handelt es sich nicht mehr um ein individuelles Problem, sondern um ein systemisches Risiko, meint unser Autor.

Die Cybersicherheitsbranche nähert sich einem Wendepunkt, und die Anzeichen lassen sich kaum noch übersehen: Stress, Erschöpfung und der ständige Druck, auf immer neue Bedrohungen reagieren zu müssen, werden für viele Fachleute zur Normalität. Burn-out ist längst nicht mehr nur ein persönliches Problem, sondern ein systemisches Risiko, und der technologische Wandel befeuert diese Entwicklung zusätzlich.

KÜNSTLICHE INTELLIGENZ VERSCHÄRFT DIE LAGE

Nirgendwo zeigt sich das deutlicher als beim Einfluss der künstlichen Intelligenz (KI) auf den Arbeitsalltag im Bereich Cybersicherheit. Automatisierung erweitert zwar die Möglichkeiten einzelner Analysten, schafft aber auch eine neue Ebene der Unsicherheit. Berufseinsteiger fürchten, dass KI genau jene Aufgaben verdrängt, die ihnen bislang dabei halfen, grundlegende Erfahrungen zu sammeln. Manche Unternehmen erproben sogar bereits, komplette Entwicklungsfunktionen durch KI zu ersetzen.

Dieser Trend trifft Studierende und Absolventen besonders hart, die ohnehin schon das Gefühl haben, sich schneller und intensiver als je zuvor beweisen zu müssen. Die traditionellen Tier-1-Positionen, die lange als Einstiegspunkt für Analysten dienten, weichen zunehmend automatisierten Workflows. Das lässt weniger Raum für Learning by Doing. Ohne sinnvolle Ausbildungswege steigen Menschen mit hohen Erwartungen in die Cybersicherheit ein, finden aber kaum Gelegenheit, sich in einem nachhaltigen Tempo weiterzuentwickeln.

BURN-OUT LAUERT ÜBERALL

Burn-out tritt auch dort auf, wo man es am wenigsten erwartet. Selbst erfüllende Arbeit bringt Fachleute irgendwann an ihre Grenzen. Viele erleben das gleiche Muster: Engagement verwandelt sich in Erschöpfung, und die Intensität, die einst zu Höchstleistungen antrieb, wird zum Problem.

Entscheidend ist das Umfeld – also die Unternehmenskultur. Negativität verbreitet sich schnell in Teams, die ohnehin überlastet sind. Sind Kollegen erschöpft, überarbeitet oder zynisch, überträgt sich diese emotionale Last auf das gesamte Team. Unternehmenskultur ist in der Cybersicherheit kein weicher Faktor, sondern ein direkter Indikator für Mitarbeiterbindung, Leistung und die Frage, ob Menschen sich eine langfristige Karriere in diesem Bereich vorstellen können.

Eine der schädlichsten Überzeugungen in der Branche ist die Vorstellung, dass echtes Engagement totale Hingabe erfordert. Die Szene belohnt oft diejenigen, die rund um die Uhr online, vernetzt und auf Abruf sind. Diese Denkweise

führt geradewegs zum Burn-out. Fachleute benötigen ein Leben und Interessen jenseits von Bedrohungsinformationen, Erkennungstechnik und Red-Team-Übungen.

PRÄVENTION BEGINNT BEI EINFACHEN GEWOHNHEITEN

Hobbys ohne Technikbezug schaffen den nötigen Abstand zum Auftanken. Ob Gartenarbeit, Sport, Kunst oder Schreiben – alles hilft, was den ständigen Kreislauf der digitalen Problemlösung unterbricht. Kurze Spaziergänge zwischendurch mildern die Intensität langer technischer Sitzungen, vor allem an der frischen Luft und bei Tageslicht. Das ist kein Luxus, sondern notwendige Hygiene für Menschen, die in einem Bereich arbeiten, der dauerhafte Aufmerksamkeit und schnelle Entscheidungen erfordert.

Burn-out vorzubeugen und sich davon zu erholen, beruht auf Routinen, die einfach klingen, aber viel bewirken: Meditation, Atemübungen und Erdungsroutinen helfen, die geistige Klarheit zurückzugewinnen. Wer Ablenkungen reduziert, beruhigt den Grundrausch, der häufig Ängste nährt. Regelmäßige Pausen im Freien fördern die Konzentration, technikferne Hobbys laden den Akku wieder auf. Vor allem aber müssen Schlaf und Ernährung Priorität haben: Wer beides vernachlässigt, kann weder klar denken noch effektiv reagieren oder gut führen.

FAZIT

Burn-out kündigt sich selten laut an. Es schleicht sich über subtile Anzeichen ein: Rückzug, liegengebliebene Aufgaben, Reizbarkeit oder das Gefühl, dass selbst Routineaufgaben plötzlich überwältigend wirken. Diese Warnsignale sind kein Anlass, noch mehr zu leisten – sondern ein Zeichen, dass sich etwas ändern muss.

Security-Verantwortliche müssen Burn-out genauso behandeln wie Schwachstellen in ihrer Infrastruktur: Man kann es identifizieren, man kann es eindämmen und es richtet erheblichen Schaden an, wenn man es ignoriert. Investieren Unternehmen in eine gesündere Kultur und nachhaltige Arbeitsbelastung, gewinnen sie mehr als bessere Moral – sie gewinnen langfristige Leistungsfähigkeit, Kreativität und stärkere Teams. Angesichts der KI-getriebenen Umbrüche müssen Führungskräfte zudem neue Karrierewege schaffen, die Fachkräften Raum zum Wachsen geben, ohne dass diese fürchten müssen, durch die Technologie ersetzt zu werden, die sie beherrschen sollen.

Eine widerstandsfähige Security-Belegschaft erfordert mehr als fortschrittliche Tools. Sie braucht Umgebungen, in denen Menschen eine sinnvolle Karriere aufbauen können, ohne sich dabei selbst zu verschleißen. Die Zukunft der Branche hängt davon ab. ■

JONATHAN REITER
ist Lead Instructor für Offensive Operations beim SANS Institute.

WENN DER ERNSTFALL KRANK MACHT – PSYCHISCHE FOLGEN VON RANSOMWARE-ANGRIFFEN

Burn-out in der Cybersicherheit entsteht nicht nur durch chronische Überlastung. Auch einzelne Sicherheitsvorfälle können massive psychische Schäden hinterlassen. Eine Studie von Northwave Cyber Security, über die die Fachzeitschrift <kes> 2023#5 berichtete, hat untersucht, was Ransomware-Angriffe mit betroffenen Mitarbeitern machen. Das Team um Eileen Walther befragte dafür CERT-Mitarbeiter, Führungskräfte und 315 Beschäftigte betroffener Unternehmen.

Drei Phasen der Belastung

*Die Ergebnisse zeigen ein Belastungsmuster in drei Phasen. In der **ersten Woche** arbeiten IT-Teams laut der Studie 12 bis 16 Stunden täglich, auch an den Wochenenden. Der Adrenalinspiegel überdecke zunächst die Erschöpfung, doch die körperlichen Folgen seien bereits messbar: 63 Prozent der direkt Beteiligten berichteten von Schlafstörungen, 44 Prozent von Kopfschmerzen. Zwei von neun befragten IT-Managern mussten Mitarbeiter wegen völliger Erschöpfung nach Hause schicken.*

*Im **ersten Monat** lässt laut Northwave das Adrenalin nach, der Druck aber bleibt. Privater Stress kommt hinzu: 48 Prozent der CERT-Mitarbeiter entwickelten Schuldgefühle gegenüber Familie und Freunden. Gleichzeitig wachse der Druck aus dem Kollegenkreis, der nicht verstehe, warum die Wiederherstellung so lange dauere. 60 bis 75 Prozent der Betroffenen berichteten von negativen Gedanken und Unsicherheiten.*

*Im **ersten Jahr** kehrt für die meisten Beschäftigten der Normalbetrieb zurück – nicht aber für das IT-Team. Das Mitgefühl der Kollegen lasse spürbar nach, so die Studie. 18 Prozent der direkt Betroffenen erwogen einen Stellenwechsel. Etwa jeder siebte Betroffene zeigte Symptome oberhalb der klinischen Schwelle, ab der professionelle Traumahilfe empfohlen wird.*

Gegenmaßnahmen nach Phasen

Northwave empfiehlt Führungskräften phasenspezifische Maßnahmen: In der akuten Krise Schichtarbeit und Pausen durchsetzen, im ersten Monat strikt zwischen störfallbezogenen und regulären Aufgaben trennen und langfristig ein offenes Umfeld schaffen, in dem Betroffene über ihre Erfahrungen sprechen können. Jeder fünfte Befragte hätte sich mehr professionelle Hilfe gewünscht. Es gab allerdings auch positive Effekte: 44 Prozent gaben an, dass sich die Zusammenarbeit im Unternehmen nach dem Angriff verbessert habe.

KI-Regulierung in Europa

MYTHOS INNOVATIONSBREMSE: EIN PLÄDOYER FÜR DEN EU AI ACT

Bremst der EU AI Act Innovation oder schafft er die Voraussetzungen für den sicheren KI-Einsatz in Unternehmen? Dem Regelwerk wird aus Wirtschaft und Politik vorgeworfen, die Entwicklung von KI-Systemen zu verlangsamen und zu verteuern, Markteintrittsbarrieren zu schaffen und Europas Wettbewerbsfähigkeit zu gefährden. Doch unsere Autoren halten in ihrem Meinungsartikel dagegen: Die Kritik beruhe auf falschen Annahmen und die tatsächlichen Innovationshemmnisse in Europa könnten woanders liegen.

Der EU AI Act trat im August 2024 in Kraft – und bereits jetzt verhandelt die EU-Kommission im Rahmen des sogenannten Digital Omnibus on AI über Änderungen, Vereinfachungen und Fristaufschübe.[1] Die Entwicklung verlief rasant: Von einem Statement für vertrauenswürdige KI und der ernsthaften Debatte über den sogenannten Brussels Effect – also die Perspektive, mit europäischen Standards einen weltweiten Maßstab zu setzen – über intensives Lobbying für Vereinfachungen und Abschwächungen, die Diskussion um „Stop the Clock" im Sommer 2025 bis hin zum Digital Omnibus on AI. Am AI Act wird weniger als zwei Jahre nach seinem Inkrafttreten gerüttelt wie bei wenigen Gesetzen sonst.

Zwei Faktoren haben diese Dynamik besonders befeuert: Zum einen die zögerliche Umsetzung in nationale Durchführungsgesetze durch die Mitgliedstaaten – Deutschland hat erst seit Februar 2026 ein nationales Durchführungsgesetz, EU-weit waren bis dahin Italien und Dänemark die einzigen Mitgliedstaaten mit tatsächlich in Kraft getretenen nationalen Gesetzen. Zum anderen hat die verzögerte Bereitstellung harmonisierter Standards, von denen sich insbesondere die Wirtschaft klarere und branchenspezifischere Richtlinien erhofft, zunehmend für Verunsicherung gesorgt.

Doch erst ein Blick über den AI Act hinaus ermöglicht eine vollständigere Einordnung: Aus den USA kommt seit Beginn der aktuellen US-Administration Gegenwind: Sie entkräftete innerhalb des ersten Amtstages eine wichtige Executive Order[2] der Biden-Administration zu KI und warnt davor, dass die europäische KI-Verordnung Innovationen ausbremse und den transatlantischen Handel gefährde.[3] Im Juli 2025 legte die Regierung unter Donald Trump zudem ihren eigenen KI-Aktionsplan vor.[4] Dieser setzt auf drei Säulen: Beschleunigung von Innovation, Ausbau technologischer Infrastruktur sowie Stärkung der globalen Führungsrolle der Vereinigten Staaten.

Auch das weltpolitische Klima hat sich gewandelt. Verschärfte geopolitische Spannungen und wirtschaftliche Unsicherheit erhöhen den Druck auf Deregulierung. Die EU steht vor der Herausforderung, ihre regulatorischen Ambitionen gegen den US-amerikanischen Deregulierungskurs zu verteidigen – und gleichzeitig, besonders präsent seit dem Weltwirtschaftsforum im Januar 2026, die oft beschworene digitale Souveränität mit konkreten Maßnahmen zu untermauern sowie europäische Werte wieder selbstbewusster in den Vordergrund zu stellen.

Das Narrativ ist auf allen drei Ebenen sehr ähnlich, ob AI-Act-bezogen, global zur KI-Regulatorik oder vor weltpolitischem Hintergrund: Regulierung gefährde die Innovationskraft und Wettbewerbsfähigkeit europäischer Unternehmen, da sie die Entwicklung von KI-Systemen verlangsame und verteure, den Wettbewerb schwäche, Markteintrittsbarrieren für kleinere Akteure schaffe und dadurch die Einführung innovativer Anwendungen behindere. Doch wie steht das im Verhältnis zu einem der Kernziele, nämlich für vertrauenswürdigen Einsatz von KI zu sorgen?

Der nachfolgende Beitrag versteht sich keineswegs als einer für den AI Act in Gänze. Mehr noch als vergleichbare Regularien ist er das Ergebnis eines demokratischen Prozesses und damit ein Kompromiss – mit allen damit einhergehenden Stärken und Schwächen, die das mit sich bringt. Wohl aber will er das beliebte Argument, wonach jede Regulierung der Innovation schade, differenziert analysieren und um Dimensionen erweitern, die in der aufgeheizten Debatte oft zu kurz kommen.

FAKT 1: NUR HOCHRISIKO-KI-SYSTEME SIND STRENG REGULIERT

Nicht alle KI-Systeme fallen automatisch unter die Vorgaben des AI Acts. Der Rechtsrahmen setzt auf einen risikobasierten Ansatz (siehe Abb. 1) und unterscheidet branchenunabhängig zwischen vier Kategorien: minimales Risiko, begrenztes Risiko, hohes Risiko und inakzeptables Risiko.

Während KI-Anwendungen mit *inakzeptablem Risiko* grundsätzlich verboten sind, konzentriert sich die Regulierung in der Praxis besonders auf Systeme der Kategorie *hohes Risiko*. Damit werden vor allem KI-Anwendungen adressiert, die ein erhebliches Gefährdungspotenzial für die Gesellschaft aufweisen.

Nach aktuellen Schätzungen betrifft dies lediglich 20 bis maximal 30 Prozent der KI-Anwendungen.[3] Demzufolge fällt die überwiegende Mehrheit der KI-Systeme nicht in diese Kategorie und somit ergeben sich für diese keine regulatorischen Anforderungen oder lediglich Transparenzpflichten *(begrenztes Risiko)*. Letztere umfassen besonders die Verpflichtung zur Kennzeichnung KI-generierter Inhalte sowie

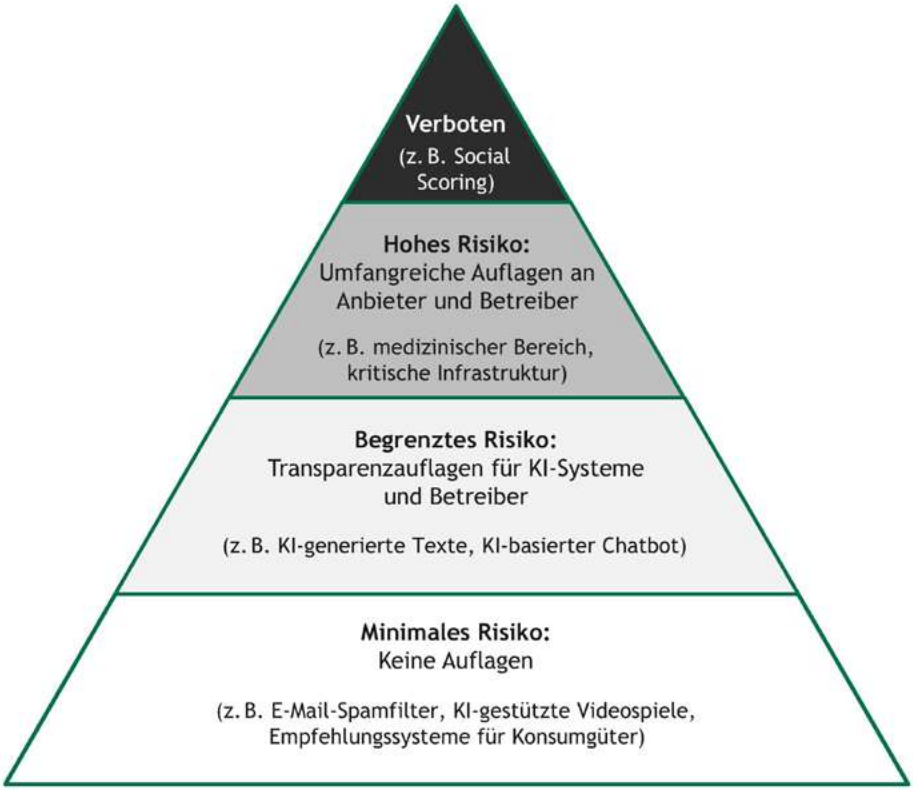


Abbildung 1: Die vier Risikostufen des AI Acts (Bild: Capgemini Invent)

den Hinweis, wenn Nutzer mit einem KI-System interagieren, beispielsweise im Rahmen von Sprachdialogsystemen (Art. 50 KI-VO).

Das bedeutet, der AI Act beschränkt Innovation lediglich in Bereichen, in denen der Einsatz von KI-Systemen mit fundamentalen Grundrechten unvereinbar ist. Zu den verbotenen Praktiken zählen unter anderem Social Scoring, die unterschwellige Beeinflussung von Personen sowie das Ausnutzen von Schwächen oder der Schutzbedürftigkeit natürlicher Personen.[1]

FAKT 2: REGULIERUNGEN KÖNNEN INNOVATIONEN FÖRDERN

In der Debatte um den AI Act wird häufig die Sorge geäußert, dass die Regulierung innovationshemmend wirken könnte. Als Gründe werden unter anderem angeführt, dass Vorschriften die Entwicklung von KI-Systemen verlangsamen und verteuern, die Qualität der Systeme beeinträchtigen, Markteintrittsbarrieren für kleinere Akteure erhöhen und die Einführung innovativer Anwendungen erschweren könnten.

Demgegenüber zeigen theoretische wie auch empirische Analysen, dass Regulierungen nicht zwangsläufig innovationshemmend wirken, sondern im Gegenteil auch als Innovationstreiber fungieren können. Tartaro et al. (2023) argumentieren, dass klare Standards und verbindliche Vorschriften Unternehmen dabei unterstützen können, Vertrauen aufzubauen und Risiken zu minimieren, wodurch Innovationsprozesse sogar begünstigt werden können.[5] Vergleichbare Effekte sind in anderen Politikfeldern nachweisbar: So haben etwa Umweltvorgaben wie die EU-Ökodesign-Richtlinie maßgeblich zur Entwicklung energieeffizienter Technologien beigetragen. Und im Bereich Datenschutz hat die Einführung der Datenschutzgrundverordnung (DSGVO) die Entwicklung sogenannter privacy-enhancing technologies (PETs) wie Differential Privacy und datensparsame Analyseverfahren deutlich vorangetrieben.

Ein regulatorisches Vakuum kann hingegen Innovationsprozesse auf mindestens drei Arten negativ beeinflussen (siehe Abb. 2): Erstens entsteht ein Mangel an Rechtssicherheit, der Investitionsentscheidungen erschwert. Ohne klare Vorgaben zu Anforderungen und Pflichten für KI-Systeme, zur Verteilung von Verantwortlichkeiten sowie zu Zertifizierungs- und Gewährleistungsmechanismen ist eine erfolgreiche und breit angelegte Einführung von KI-Technologien in Unternehmen unwahrscheinlich.

Zweitens verringert die Verbreitung unregulierter KI-Systeme auf dem Markt die Sicherheit dieser Produkte und erhöht das Risiko negativer Auswirkungen. Dies führt zu einem Vertrauensdefizit bei Verbrauchern, sowohl im privaten als auch im geschäftlichen Kontext, und erschwert dadurch die gesellschaftliche Akzeptanz von KI. Mangelndes Vertrauen stellt wiederum ein erhebliches Hindernis für Investitionen und die Einführung von KI-Lösungen in der Praxis dar.

Drittens kann das Fehlen einheitlicher europäischer Rechtsvorschriften zu einer Fragmentierung des Binnenmarktes führen. Dies wirkt sich in mehrfacher Hinsicht innovationshemmend aus: erschwerter Zugang zu nationalen Märkten – besonders für kleine und mittlere Unternehmen (KMU) und Start-ups, die über geringere Ressourcen verfügen –, Verlagerung von Investitionen in Länder mit weniger strikten Regulierungen sowie mangelnde Interoperabilität. Eine solche Fragmentierung kann nicht nur die Sicherheit von KI-Anwendungen untergraben, sondern auch das Vertrauen von Endnutzern in die Steuerungsfähigkeit von Organisationen sowie in die Qualität der eingesetzten Systeme erheblich beeinträchtigen. Schon heute zeigt sich das in der Zurückhaltung vieler Unternehmen, KI am Arbeitsplatz einzuführen. Gründe hierfür sind vor allem bestehende Unsicherheiten in Bezug auf Datenschutz, Compliance und Sicherheit von KI-Systemen.

Um Innovationen trotz dieser Herausforderungen gezielt zu fördern, verpflichtet die EU ihre Mitgliedstaaten, bis spätestens 2. August 2026 mindestens ein nationales KI-Reallabor einzurichten (Art. 57 KI-VO). Diese sogenannten „regulatory sandboxes" bieten Unternehmen, Forschungseinrichtungen und Behörden die Möglichkeit, innovative KI-Systeme unter realen Bedingungen zu testen, ohne bereits alle regulatorischen Anforderungen vollständig erfüllen zu müssen. Ziel ist es, einerseits die Entwicklung und Markteinführung innovativer KI-Anwendungen zu beschleunigen und gleichzeitig deren sichere und verantwortungsvolle Entwicklung sicherzustellen.

Wenn Regulierung und Standards mit dem technologischen Fortschritt in Einklang stehen, behindern sie Innovation nicht. Im Gegenteil: Sie können Innovation fördern. Auch wenn der

Abbildung 2: Risiken und Folgen fehlender Regulierungen (Bild: Capgemini Invent)

technologische Fortschritt innerhalb der Grenzen bestehender Regulierung erfolgt, können Standards gezielt Innovation anstoßen.

FAKT 3: REGULIERUNG KANN EIN STRATEGISCHER WETTBEWERBSFAKTOR SEIN

Regulierungen können einen Wettbewerbsvorteil darstellen, da sie institutionelle Rahmenbedingungen schaffen, die Marktakteuren klare Standards für Qualität, Sicherheit und Vertrauenswürdigkeit vorgeben. Unternehmen, die diese Anforderungen konsequent erfüllen, können sich dadurch gegenüber weniger regulierten Wettbewerbern im Markt positionieren. Im internationalen Kontext wird dies durch Herkunftsbezeichnungen wie „Made in Germany" oder „Made in Switzerland" veranschaulicht. Diese Labels sind nicht nur geografische Hinweise, sondern fungieren als anerkannte Qualitätsmarker, die auf strenge Normen, verlässliche Produktionsprozesse und technologische Kompetenz verweisen – und damit einen unmittelbaren Marktvorteil schaffen. Qualitätsstandards helfen zudem, niedrigwertige Produkte vom Markt fernzuhalten, die sonst hochwertige Angebote verdrängen könnten – ein Effekt, der als Gresham's Law bekannt ist.

Darüber hinaus bietet die Einhaltung von Standards einen zusätzlichen Vorteil: Unternehmen können sich darauf verlassen, dass auch andere Akteure innerhalb ihrer KI-Lieferkette ein definiertes Maß an Sicherheit, Qualität und Vertrauenswürdigkeit einhalten müssen.[5] Dies ist besonders relevant, da viele Verpflichtungen des EU-KI-Gesetzes nicht nur die Anbieter, sondern auch die Betreiber von KI-Systemen betreffen (Art. 3 KI-VO). Die Orientierung an Standards reduziert damit nicht nur regulatorische Risiken, sondern stärkt auch die Verlässlichkeit in komplexen Wertschöpfungsketten. Werden Standards zudem durch unabhängig geprüfte, international anerkannte Zertifizierungen oder Vertrauenssiegel ergänzt, stärkt dies zusätzlich das Vertrauen von Kunden und anderen Stakeholdern.

FAKT 4: QUALITÄTS-STANDARDS SCHAFFEN UNTERNEHMENSWERTE

Qualitätsstandards spielen eine zentrale Rolle bei der Sicherstellung von Verlässlichkeit und Transparenz in technologischen Innovationsfeldern sowie beim Schutz vor Missbrauch. Auch verbindliche regulatorische Qualitätsstandards stellen nicht nur eine Notwendigkeit dar, sondern können ein Treiber für die Wertschöpfung in Unternehmen sein.

Unternehmenswerte	EU AI Act	Unternehmen
Datenqualität	**Erwägungsgrund 67** „Qualitativ **hochwertige Daten** und der Zugang zu qualitativ hochwertigen Daten spielen eine entscheidende Rolle bei der Strukturierung und Sicherstellung der Leistung vieler KI-Systeme."	**Gartner** *„Datenqualität hat bei Datenanalyse-Initiativen höchste Priorität, da sie maßgeblich zur Steigerung des Geschäftswerts beiträgt."* [7]
Leistungsüberwachung	**Erwägungsgrund 91** „In Anbetracht der Art von KI-Systemen und der mit ihrer Verwendung möglicherweise verbundenen Risiken für die Sicherheit und die Grundrechte, auch im Hinblick auf die Notwendigkeit, eine angemessene **Überwachung der Leistung** eines KI-Systems in einer realen Umgebung zu gewährleisten, ist es angebracht, besondere Pflichten für die Einsatzkräfte festzulegen."	**Google** *„Leistung in allen Phasen des Modelllebenszyklus beobachten."* [8]
Vertrauenswürdigkeit	**Art. 1, Abs. 1** „Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern und die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen KI zu fördern [...]"	**Nvidia** *„Vertrauenswürdige KI-Prinzipien sind die Grundlage für unsere End-to-End-Entwicklung und entscheidend für die technische Exzellenz, auf die unsere Partner, Kunden und Entwickler vertrauen."* [12]
Sicherheit	**Art. 15, Abs. 1** „KI-Systeme mit hohem Risiko sind so zu konzipieren und zu entwickeln, dass sie ein angemessenes Niveau an Genauigkeit, Robustheit und Cybersicherheit erreichen [...]."	**IBM** *„Der kritische Bedarf an einem ‚Secure by Design'-Ansatz, der sicherstellt, dass Sicherheitsmaßnahmen von Anfang an integraler Bestandteil der KI-Einführung sind."* [9]

Tabelle 1: Übereinstimmung zwischen EU-AI-Act-Anforderungen und freiwilligen Qualitätsstandards von Unternehmen

Bereits vor der Einführung des AI Acts waren Standards für Qualität, Sicherheit und Transparenz in vielen Unternehmen ein zentraler Hebel für Vertrauen und nachhaltige Wettbewerbsfähigkeit. Führende Unternehmen wie Gartner, Google, IBM und Nvidia haben schon vor der KI-VO Anforderungen an Datenqualität, Leistungsüberwachung sowie Sicherheits- und Transparenzmechanismen etabliert (siehe Tabelle 1).

FAKT 5: KI BRAUCHT GLOBALE REGULIERUNG

Die Dynamik aktueller technologischer Entwicklungen im Bereich der KI und der damit einher-

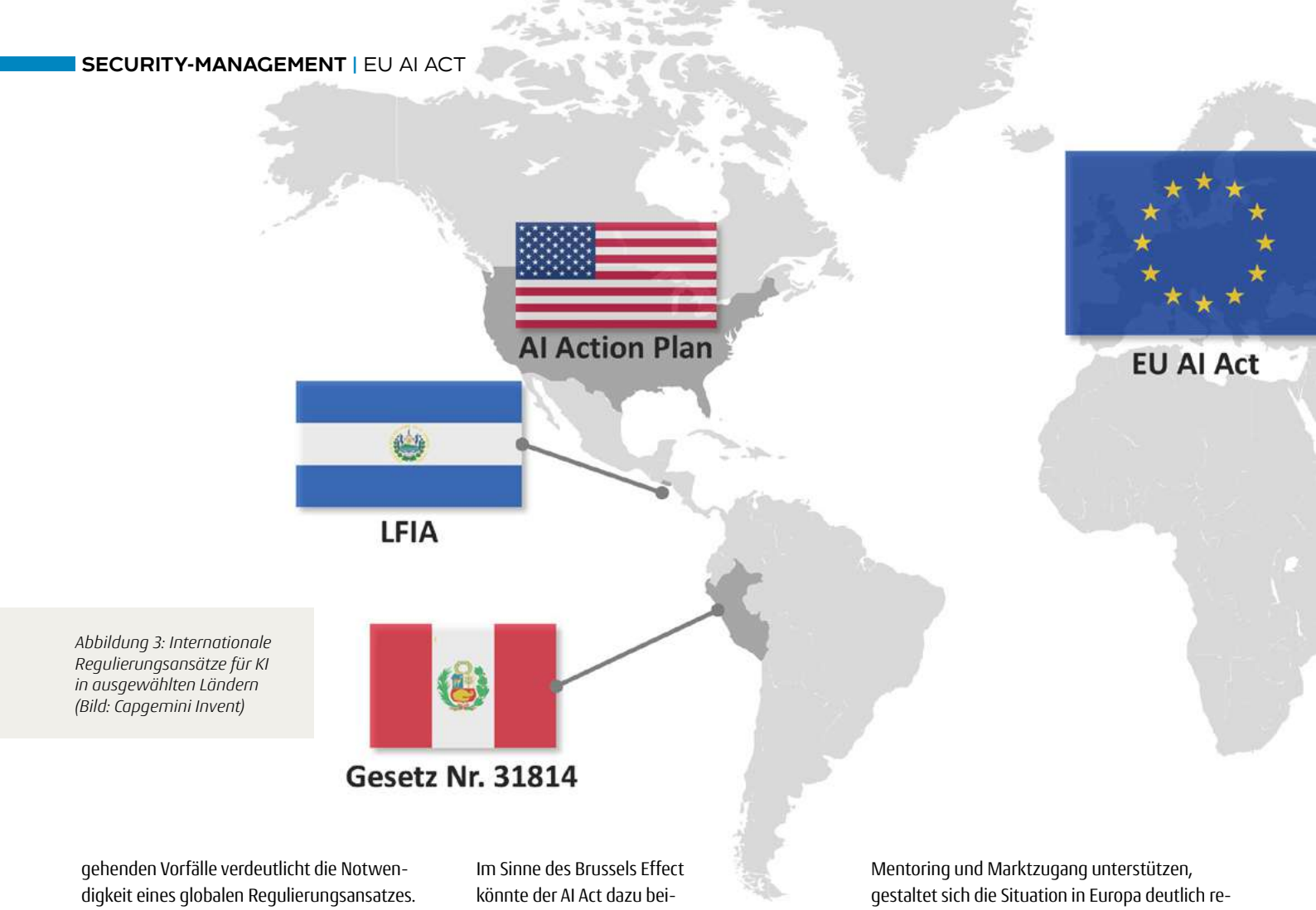


Abbildung 3: Internationale Regulierungsansätze für KI in ausgewählten Ländern (Bild: Capgemini Invent)

gehenden Vorfälle verdeutlicht die Notwendigkeit eines globalen Regulierungsansatzes. Phänomene wie Deep-Fakes, die zunehmend schwer von authentischen Inhalten zu unterscheiden sind, oder sicherheitsrelevante Vorfälle mit autonomen Robotersystemen – etwa der dokumentierte Angriff auf eine Menschenmenge in China[10] – illustrieren, dass die mit KI verbundenen Risiken transnationaler Natur sind. Angesichts der globalen Wirtschaft und der Struktur des weltweiten KI-Ökosystems besteht ein klarer Bedarf an einem systematischen Ansatz zur globalen KI-Regulierung.[5] Weltweit lassen sich bereits zahlreiche regulatorische Initiativen und Standardisierungsbestrebungen im Bereich KI beobachten (siehe Abb. 3). Allerdings fehlt es bislang an einer kohärenten internationalen Anschlussfähigkeit sowie an einer übergreifenden Harmonisierung der Regelwerke.

Die Europäische Union übernimmt mit dem AI Act eine Vorreiterrolle, indem sie einen umfassenden regulatorischen Rahmen etabliert, der im Sinne des „Brussels Effect" das Potenzial hat, weit über die europäischen Grenzen hinaus Wirkung zu entfalten. Indem die EU strenge Standards etabliert, gewährleistet sie nicht nur die Konformität innerhalb ihres Binnenmarktes, sondern übt zugleich erheblichen Einfluss auf globale Märkte aus und prägt dadurch indirekt die Entwicklung internationaler Normen und Praktiken.

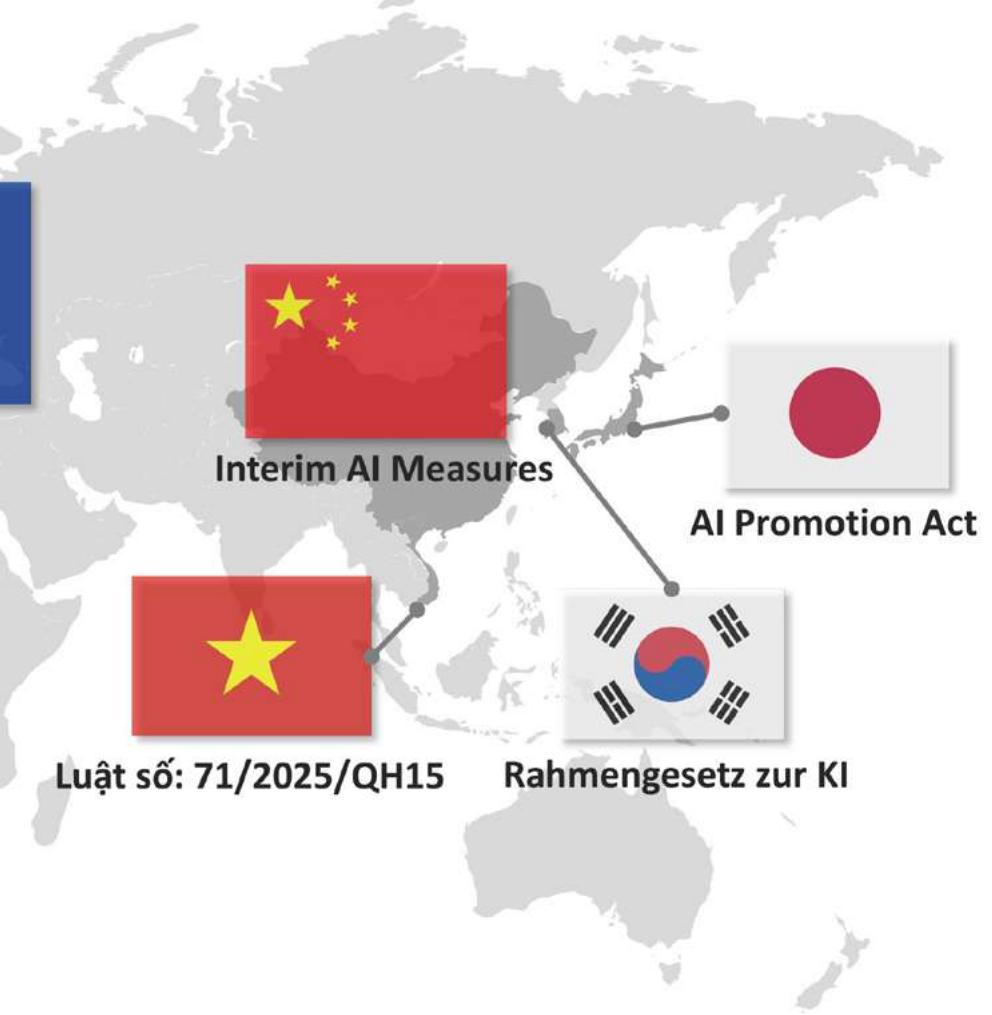
Im Sinne des Brussels Effect könnte der AI Act dazu beitragen, den internationalen Regulierungsaufwand zu verringern, rechtliche Fragmentierung zu vermeiden und die Anschlussfähigkeit nationaler Rechtsrahmen zu sichern. Eine Schlüsselrolle kommt dabei der Standardisierung zu. International anerkannte Normungsorganisationen wie ISO oder IEEE können durch die Entwicklung gemeinsamer Standards nicht nur die Senkung von Transaktionskosten, sondern auch die Sicherstellung technischer Interoperabilität sowie einheitliche Ansätze für Sicherheit und Governance von KI fördern.

FAKT 6: MANGEL AN RISIKOKAPITAL, FINANZIERUNGSMÖGLICHKEITEN UND FÖRDERPROGRAMMEN

Ein wesentlicher Hemmfaktor für die Entstehung und Skalierung innovativer Start-ups in Europa ist der vergleichsweise geringe Zugang zu Risikokapital, Finanzierungsmöglichkeiten und strukturierten Förderprogrammen. Während in den USA eine hohe Dichte an Wagniskapitalgesellschaften, Business Angels und Start-up-Hubs existiert, die Start-ups nicht nur mit finanziellen Ressourcen, sondern auch mit Netzwerken, Mentoring und Marktzugang unterstützen, gestaltet sich die Situation in Europa deutlich restriktiver. Die Verfügbarkeit von Risikokapital ist geringer, was besonders jungen Unternehmen in der Wachstumsphase den Zugang zu notwendigen Finanzmitteln erschwert und deren internationale Wettbewerbsfähigkeit limitiert.

Hinzu kommt, dass die Anzahl an Inkubatoren, Accelerator-Programmen und Innovationszentren in Europa im Vergleich zu den USA deutlich geringer ausfällt. Dies führt nicht nur zu einer Verknappung an institutionalisierter Unterstützung, sondern verlangsamt auch die Dynamik von Innovations- und Gründungsprozessen insgesamt.

Vor diesem Hintergrund lässt sich feststellen, dass nicht in erster Linie der AI Act als maßgeblicher Hemmfaktor für Innovationen im europäischen Raum zu bewerten ist. Vielmehr legen langfristige Entwicklungstendenzen nahe, dass die Innovationslandschaft im Bereich KI bereits vor der Einführung des AI Acts vergleichsweise gering ausgeprägt war. So verweist der KI-Bundesverband in seinem Statement zum „AI Continent Action Plan" darauf, dass die europäische KI-Branche keine weiteren Ankündigungen bereits bekannter Maßnahmen und kleinteiliger Einzelstrategien benötigt, sondern „... funktionierende Förder- und Vergabeverfahren, die mit der Geschwindigkeit der technologischen Entwicklung Schritt halten können."[6]



FAZIT

Mit diesem Artikel laden wir zu einer differenzierteren Analyse ein, die der Komplexität des Zusammenspiels aus Regulatorik, Technologie und wirtschaftlichen Interessen gerecht wird. Die verbreitete Annahme, Regulierung stehe Innovation grundsätzlich entgegen, ist ein Mythos.

Der risikobasierte Ansatz des AI Acts zeigt vielmehr: Nicht die Technologie, sondern deren Einsatz wird reguliert. Diese Leitplanken sind kein Selbstzweck. Sie dienen dem Schutz fundamentaler Rechte und der gesellschaftlichen Akzeptanz von KI, denn Vertrauen ist die Voraussetzung für nachhaltige Innovation. Dies ist allgemein zutreffend, noch mehr jedoch in Bezug auf eine Technologie, die sich nicht nur rasant schnell entwickelt, sondern auch nahezu unvorhersehbar vielfältig einsetzbar ist. In diesem Zusammenhang müssen die Leitplanken als Verteidigung europäischer Werte und nicht als Bedrohung interpretiert werden. Die Verordnung ist somit nicht nur ein juristisches Instrument, sondern ein Ausdruck europäischer Identität im digitalen Zeitalter. ■

Literatur

[1] *Digital-Omnibus-Verordnung zur KI, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52025PC0836*

[2] *Removing Barriers to American Leadership in Artificial Intelligence – The White House, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/*

[3] *Hauer, M. P.; Krafft, T. D.; Sesing Wagenpfeil, A.; Zweig, K. A.: Quantitative study about the estimated impact of the AI Act, CoRR abs/2304.06503, 2023, https://doi.org/10.48550/arXiv.2304.06503*

[4] *Regierung der Vereinigten Staaten: America's AI Action Plan, 2025, https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf*

[5] *Tartaro, A.; Smith, A.; Shaw, P.: Assessing the impact of regulations and standards on innovation in the field of AI, 2023, www.researchgate.net/publication/368361276_Assessing_the_impact_of_regulations_and_standards_on_innovation_in_the_field_of_AI*

[6] *KI Bundesverband: Pressestatement zum AI Continent Action Plan, 2025, https://ki-verband.de/wp-content/uploads/2025/05/20250409_Pressestatement_KI-Bundesverband_AIContinentActionPlan.pdf*

[7] *Gartner: Data Management Schwerpunktseite, www.gartner.com/en/data-analytics/topics/data-management*

[8] *Google Cloud: Performance Optimization for AI/ML, https://cloud.google.com/architecture/framework/perspectives/ai-ml/performance-optimization*

[9] *IBM: Secure by Design Ansätze für KI Einführung, https://www.ibm.com/think/topics/how-to-embrace-secure-by-design-while-adopting-ai*

[10] *NDTV: Bericht zu einem sicherheitsrelevanten Vorfall mit einem autonomen Robotersystem in China, www.ndtv.com/world-news/video-ai-robot-attacks-people-at-china-festival-internet-says-so-it-begins-7808616*

[11] *Europäische Kommission: Leitlinien zu verbotenen KI Praktiken nach AI Act, https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act*

[12] *Nvidia: Trustworthy AI Grundsätze, www.nvidia.com/de-de/trust-center/trustworthy-ai/*

[13] *t3n: Bericht zu wirtschaftlichen Forderungen bezüglich des AI Act, https://t3n.de/news/ai-act-ki-europa-eu-1699979/*

[14] *Deutsche Welle (DW): Analyse der US Kritik an europäischer KI Regulierung, www.dw.com/en/ai-policy-regulation-europe-us/a-71426911*

[15] *Tagesspiegel Background Digitalisierung & KI: Einschätzung zur geopolitischen Dimension des AI Act, https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/europa-muss-diesen-kampf-gewinnen*

[16] *Europäische Kommission: Digital Omnibus – Anpassungen für KI Regulierung, https://cdn.netzpolitik.org/wp-upload/2025/11/EU-Kommission-Digital-Omnibus-B-KI.pdf*

INNA VOGEL
ist Senior Consultant für Enterprise Data & Analytics bei Capgemini Invent. Sie berät Unternehmen in der strategischen Planung und Umsetzung von AI-Projekten und verfügt über mehrjährige Forschungserfahrung im Bereich Maschinelles Lernen an einem renommierten Institut.

ERIK LEONHARDT
ist Consultant im Bereich Enterprise Transformation - Enterprise Data & Analytics bei Capgemini Invent mit dem Fokus auf AI-Governance und AI-Strategie. Er sammelte bereits Erfahrungen in der Umsetzung von KI-Projekten, unter anderem im Bereich KI-gestütztes Controlling.

JANA SCHÖNEBORN
ist Senior Managerin im Bereich Enterprise Data & Analytics bei Capgemini Invent. Sie verfügt über jahrelange Beratungserfahrung in datengetriebenen Projekten. Ihre aktuellen Beratungsschwerpunkte sind AI-Strategie und AI-Governance Projekte.

Von der Norm zur Wirkung (5):
Wie Unternehmen Lieferanten einbinden und absichern

SICHERHEIT ENDET NICHT AM WERKSTOR

Moderne Wertschöpfung ist verteilt – über Cloud-Anbieter, IT-Dienstleister und Plattformbetreiber. Unsere Autoren zeigen im letzten Teil der Artikel-Serie, warum Unternehmen ihr Lieferantenmanagement in die zentrale Governance-Architektur integrieren müssen und wie das konkret gelingen kann.

Bild: Eigene Darstellung, generiert mit ChatGPT (SORA)

In den bisherigen Beiträgen dieser Reihe haben wir gezeigt, wie Governance von innen heraus wirksam wird: über strukturierte Prozesse, belastbares Vertrauen, systematisches Risikomanagement und ein integriertes Kontrollsystem (IKS). Ein solches System schafft Transparenz, definiert Verantwortlichkeiten und macht Risiken steuerbar.

Doch moderne Wertschöpfung endet nicht am Werkstor. Sie ist verteilt – technologisch, organisatorisch und geografisch. Cloud-Anbieter betreiben kritische Infrastruktur, IT-Dienstleister administrieren Kernsysteme, Softwarelieferanten spielen Updates mit unmittelbarem Einfluss auf Produktions- oder Klinikprozesse ein, und Plattformanbieter bündeln ganze Wertschöpfungsketten. Unternehmen agieren heute nicht mehr isoliert, sondern als Teil digitaler Ökosysteme (siehe auch Abbildung 1).

Damit verschiebt sich die zentrale Governance-Frage: Es geht nicht mehr darum, wie sicher das eigene Unternehmen ist, sondern darum, wie beherrschbar das gesamte digitale Wertschöpfungsnetzwerk ist.

Lieferantenrisiken sind keine operativen Detailfragen mehr. Sie sind strategische Risiken, Haftungsrisiken und Aufsichtsthemen. Spätestens mit der Network and Information Security Directive 2 (NIS-2) und dem Digital Operational Resilience Act (DORA) zeigt sich, was technologisch längst Realität ist: Verantwortung endet nicht an der eigenen Systemgrenze. Wer Governance nur innerhalb der eigenen Organisation definiert, schafft eine strukturelle Blindstelle – intern entsteht Ordnung, extern bleibt Unsicherheit.

„Von der Norm zur Wirkung" bedeutet deshalb im Kontext der Lieferkette, Anforderungen nicht additiv umzusetzen, sondern bestehende Steuerungsmechanismen integrativ zu erweitern. Governance wird ökosystemisch – nicht durch neue Parallelprozesse, sondern durch die systemische Einbindung externer Abhängigkeiten in bestehende Risiko-, Vertrags- und Monitoringstrukturen. Damit schließt sich der Kreis dieser Reihe und öffnet sich zugleich über die Unternehmensgrenze hinaus. Doch bevor sich die Frage nach dem Wie stellt, lohnt ein Blick auf das regulatorische Warum.

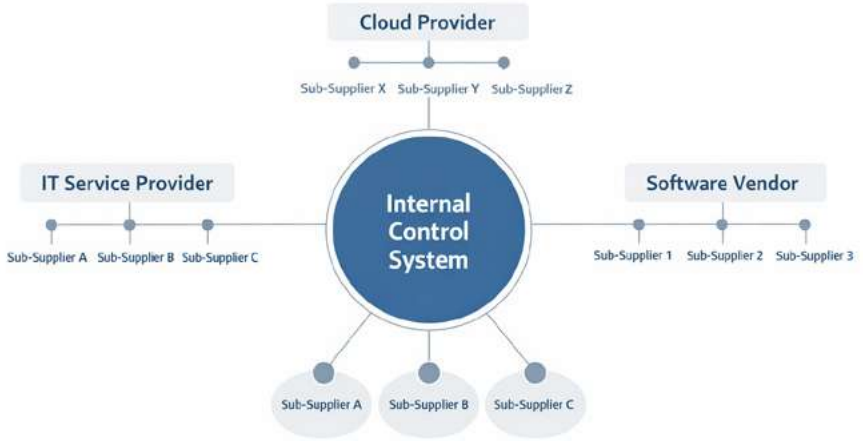


Abbildung 1: Governance im Ökosystem (Bild: SECaaS.IT)

REGULATORISCHE VERANTWORTUNG ENTLANG DER LIEFERKETTE

Die regulatorische Entwicklung der letzten Jahre ist eindeutig und folgerichtig. Was früher implizit erwartet wurde, fordert der Gesetzgeber heute explizit: Lieferkettenrisiken sind systematisch zu steuern.

Mehrere Rahmenwerke verfolgen dafür dieselbe Stoßrichtung (siehe Abbildung 2):

- NIS-2 verlangt Sicherheitsmaßnahmen einschließlich der Bewertung von Lieferkettenrisiken.
- DORA schreibt ein strukturiertes ICT Third Party Risk Management (TPRM) vor – inklusive Vertragsanforderungen, Monitoring und Exit-Strategien.
- ISO/IEC 27001:2022 A.5.19–23 adressiert die Steuerung von Lieferantenbeziehungen explizit.
- Branchen- und „Environmental, Social and Governance (ESG)"-Vorgaben erhöhen zusätzlich Transparenz- und Nachweiserwartungen.

Diese Anforderungen sind kein Nebenschauplatz mehr – sie verändern die Rolle des Lieferantenmanagements grundlegend. Lieferantenmanagement ist heute kein Einkaufsprozess, sondern Bestandteil der Governance-Architektur. Für CIOs und CISOs bedeutet das konkret: Sie klassifizieren Lieferanten risikobasiert, verankern Sicherheitsanforderungen vertraglich verbindlich, binden Drittparteien in Monitoring- und Incident-Prozesse ein und analysieren Konzentrations- sowie Abhängigkeitsrisiken transparent.

Abbildung 2: Konvergenz der Regulatorik (Bild: SECaaS.IT)

Abbildung 3: Automatisierter Governance-Regelkreis (Bild: SECaaS.IT)

Besonders relevant ist dabei das Thema systemischer Abhängigkeiten. Mehrere kritische Dienstleister nutzen häufig denselben Cloud- oder Plattformanbieter. Ein Ausfall oder regulatorischer Eingriff kann damit branchenweite Auswirkungen haben. DORA adressiert dieses Konzentrationsrisiko explizit – ein deutliches Signal an die Leitungsebene. Die regulatorische Logik ist klar: Resilienz entsteht nicht isoliert, sondern vernetzt. Organisationen tragen Verantwortung für Sicherheitsrisiken, die ihre Dienstleister verursachen – unabhängig davon, ob diese technisch oder organisatorisch außerhalb der eigenen Systemgrenzen liegen.

Damit verschiebt sich Governance strukturell: von der internen Kontrolle hin zur systemischen Steuerung eines digitalen Ökosystems. Und genau hier beginnt die eigentliche Herausforderung: Wie lassen sich externe Risiken so integrieren, dass sie steuerbar bleiben, ohne neue Parallelstrukturen zu erzeugen?

INTEGRATION IN GOVERNANCE-SYSTEME

Die eigentliche Herausforderung im Umgang mit Lieferantenrisiken ist jedoch nicht die Bewertung, sondern die Integration. Viele Organisationen reagieren auf neue regulatorische Anforderungen mit zusätzlichen Tools, Fragebögen oder separaten Prüfprozessen. Es entstehen neue Datenquellen, neue Verantwortlichkeiten, neue Berichte. Was zunächst strukturiert wirkt, entfaltet in der Praxis eine problematische Nebenwirkung: Governance wächst additiv, nicht integrativ.

Additive Governance stößt allerdings strukturell schnell an ihre Grenzen. Was fehlt, ist kein weiteres Regelwerk, sondern ein zentraler Ordnungsrahmen, der externe Risiken in die bestehende Steuerungsarchitektur einbindet. Das sogenannte Third Party Risk Management wirkt erst dann vollständig, wenn Unternehmen es systemisch einbetten. Ein isoliertes Lieferanten-Tool erzeugt Informationen – ein integriertes Governance-System erzeugt Steuerungsfähigkeit.

Für CIO und CISO bedeutet das: Lieferantenrisiken dürfen keine Parallelwelt bilden. Sie müssen Teil der bestehenden Systemlandschaft werden, nicht deren Erweiterung durch Zusatzprozesse. Drei Integrationspunkte sind dabei entscheidend.

Der erste und wichtigste Ankerpunkt ist das zentrale Risk Register. Jeder kritische Lieferant erscheint dort als eigenständiger Risikoeintrag, einer verantwortlichen Rolle zugeordnet, mit Risikobewertung, Maßnahmen und Fristen verknüpft sowie revisionssicher versioniert. Erst dadurch wird aus einer Bewertung eine steuerbare Risikoentscheidung. Ohne diese Integration bleibt das Lieferantenmanagement ein Compliance-Nebenprozess, aber mit ihr wird es Bestandteil der unternehmensweiten Risikoarchitektur.

Ebenso wichtig ist die Verbindung zu Beschaffung und Vertragsmanagement, denn Governance beginnt nicht nach Vertragsabschluss. Eine systemische Integration bindet Sicherheitsanforderungen bereits in Beschaffungs- und Vertragsprozesse ein: durch Risikoklassifizierung bei Neuanlage eines Lieferanten, Pflichtfelder zu Sicherheitsanforderungen, Verknüpfung mit Vertragsdokumenten und Eskalationsmechanismen bei fehlender Bewertung. So wird die Sicherheitsprüfung präventiv statt reaktiv. Die Beschaffung wird nicht zur Kontrollinstanz, sondern zum strukturellen Bestandteil der Governance-Kette.

Bei kritischen Dienstleistern endet Governance zudem nicht mit der Vertragsunterzeichnung. Externe Zugriffe, Application-Programming-Interface-(API)-Nutzung, Administrationsrechte oder Datenschnittstellen erzeugen operative Risiken, die sichtbar bleiben müssen. Eine sinnvolle Anbindung an Monitoring und operative Systeme umfasst daher die Integration in Security-Information-and-Event-Management-(SIEM)- oder Monitoring-Systeme, die Verknüpfung mit Incident-Management-Prozessen und die Rückkopplung von Sicherheitsereignissen in die Risikobewertung.

Ein Beispiel: Ein externer IT-Dienstleister erhält administrativen Zugriff. Das Monitoring kennzeichnet diesen Zugriff gesondert. Auffälligkeiten stufen die Risikobewertung automatisch hoch. So entsteht ein geschlossener Regelkreis – vom Ereignis über die Bewertung bis zur Managemententscheidung (siehe Abbildung 3).

Die eigentliche Wirkung entsteht allerdings erst auf der Führungsebene. Ein integriertes Governance-Dashboard kann beispielsweise die Anzahl kritischer Lieferanten, die Verteilung der Risikokategorien, offene Maßnahmen, den Zertifizierungsstatus, Konzentrationsrisiken und die historische Risikoentwicklung anzeigen. Damit wird eine zuvor diffuse Risikolandschaft visuell greifbar. Für Geschäftsführung und Aufsicht entsteht Entscheidungsfähigkeit statt bloßer Reaktion.

TPRM ALS STEUERUNGSMODELL

Nachdem die systemische Integration geklärt ist, stellt sich die operative Frage: Wie lassen sich externe Risiken strukturiert bewerten und steuern? Genau hier setzt Third Party Risk Management an. TPRM ist kein Fragebogenprozess, sondern ein Regelkreis. Ein wirksames Modell verbindet vier Elemente (siehe Abbildung 4): Erstens das Klassifizieren – wie kritisch ist der Lieferant für die eigene Wertschöpfung? Zweitens das Bewerten – wie reif ist sein Sicherheitsniveau? Drittens das vertragliche Absichern – welche Mindestanforderungen sind verbindlich? Und viertens das kontinuierliche Überwachen – wie verändert sich das Risiko über die Zeit?

Abbildung 4: TPRM-Steuerungslogik (Bild: SECaaS.IT)

TPRM wird damit zur operativen Ausprägung ökosystemischer Governance.

Nicht jeder Dienstleister ist gleich kritisch. Ein Reinigungsunternehmen unterscheidet sich zum Beispiel strukturell von einem Cloud-Provider mit administrativem Zugriff auf Kernsysteme. Entscheidend ist daher nicht die Anzahl der Lieferanten, sondern deren Einfluss auf Vertraulichkeit sensibler Daten, Verfügbarkeit kritischer Systeme, Integrität geschäftskritischer Prozesse, regulatorische Verpflichtungen und Abhängigkeiten von Subdienstleistern. Bewährt hat sich eine risikobasierte Klassifizierung in vier Stufen:

- **kritisch:** direkter Einfluss auf Kernprozesse oder regulatorisch relevante Systeme
- **hoch:** Zugriff auf sensible Daten oder produktionsnahe Systeme
- **mittel:** unterstützende Funktionen mit begrenzter Systemnähe
- **gering:** kaum sicherheitsrelevant

Diese Einstufung entscheidet über die Tiefe der Prüfung, die Intensität des Monitorings, die vertraglichen Anforderungen und das Management-Reporting. Ohne Klassifizierung entsteht Gleichbehandlung – und Gleichbehandlung erzeugt Ineffizienz.

Viele Organisationen setzen bei der Bewertung noch auf statische Excel-Fragebögen. Ein modernes TPRM-System übersetzt Bewertungen dagegen in steuerungsrelevante Kennzahlen: Fragen orientieren sich an anerkannten Standards wie ISO 27001 Annex A, die Gewichtung erfolgt abhängig von der Kritikalität, Antworten werden in Reifegrade überführt und ein aggregierter Score entsteht.

Ein vereinfachtes Bewertungsmodell könnte beispielsweise zwischen niedrigem, erhöhtem und kritischem Risiko unterscheiden. Entscheidend ist nicht die mathematische Präzision, sondern die Vergleichbarkeit und Nachvollziehbarkeit. Der Score wird damit nicht zum Selbstzweck, sondern zur Entscheidungsgrundlage.

TPRM ist dabei keine jährliche Pflichtübung. Regulatorische Anforderungen – insbesondere DORA – verlangen eine fortlaufende Bewertung von Drittparteien: Aktualisierung bei Vorfällen, Neubewertung bei Leistungsänderungen, Anpassung bei regulatorischen Entwicklungen und Eskalation bei erhöhtem Risikoscore.

Abbildung 5: Systemintegration von TPRM (Bild: SECaaS.IT)

Ein praxisnahes Beispiel verdeutlicht den Nutzen: Ein mittelständisches Unternehmen klassifiziert 120 IT- und Softwarelieferanten. Nach Einführung eines strukturierten Bewertungsmodells stuft es 14 als kritisch ein, bei fünf Lieferanten entsteht ein erhöhter Risikoscore. Maßnahmen folgen unmittelbar: vertragliche Nachschärfung, zusätzliche Nachweise und Monitoring-Anbindung. Erstmals entsteht ein konsolidiertes Bild der externen Risikolage – integriert in das zentrale Risk Register (siehe Abbildung 5).

Genau hier schließt sich der Kreis zum vorherigen Kapitel: Bewertung ohne Integration bleibt isoliert, Integration ohne Bewertungsmodell bleibt oberflächlich.

VERTRAGSARCHITEKTUR UND AUDITIERBARKEIT

Risikobewertung allein erzeugt aber noch keine Resilienz. Erst wenn Anforderungen verbindlich geregelt sind, wird Governance belastbar. Mit NIS-2 und besonders DORA wird deutlich: Drittparteirisiken müssen nicht nur erkannt, sondern steuerbar und nachweisbar abgesichert sein. Damit verschiebt sich der Fokus vom Fragebogen zur Vertragsarchitektur.

Ein identifiziertes Risiko ohne vertragliche Grundlage bleibt unverbindlich, ein Vertrag ohne Bezug zur Risikobewertung bleibt formal. Wirksame Governance verbindet beides (siehe auch Abbildung 6). Je nach Kritikalität eines Lieferanten gehören dazu etwa Mindestanforderungen an die Informationssicherheit, die Verpflichtung zur Offenlegung wesentlicher Sicherheitsvorfälle, Regelungen zu Subdienstleis-

Abbildung 6: Verbindung von Risiko und Vertrag (Bild: SECaaS.IT)

tern, Audit- und Einsichtsrechte sowie Exit- und Übergangsregelungen.

Entscheidend ist dabei nicht die Länge des Vertrags, sondern die klare Ableitung aus der Risikoklassifizierung. Vertragliche Anforderungen müssen proportional sein – aber sie müssen vorhanden sein.

Auditierbarkeit gilt häufig als Dokumentationspflicht. Tatsächlich ist sie ein Governance-Instrument. Auditfähigkeit bedeutet,

- Bewertungen sind nachvollziehbar dokumentiert,
- Vertragsanforderungen referenziert,
- Maßnahmen terminiert und überwacht sowie
- Entscheidungen begründet und freigegeben.

So entsteht ein belastbarer Nachweis gegenüber Aufsichtsbehörden, Wirtschaftsprüfern, der internen Revision und Versicherern. Auditfähigkeit ist damit kein administrativer Aufwand, sondern Ausdruck strukturierter Entscheidungsfähigkeit.

Ein besonders relevanter Aspekt ist darüber hinaus das Konzentrationsrisiko. Mehrere kritische Prozesse hängen häufig indirekt vom selben Cloud- oder Plattformanbieter ab. Ein Ausfall oder regulatorischer Eingriff kann damit zahlreiche Organisationen gleichzeitig treffen. DORA adressiert dieses Risiko explizit, auch NIS-2 impliziert eine Bewertung von Abhängigkeiten.

In der Praxis bedeutet das: Transparenz über Subdienstleister, Mapping gemeinsamer Plattformabhängigkeiten, Szenarioanalysen für Ausfall oder regulatorische Einschränkung und strategische Exit-Planung. Konzentrationsrisiken sind kein technisches Detail – sie sind Geschäftsrisiken.

KI UND AUTOMATISIERUNG

Mit steigender regulatorischer Dichte und wachsender Lieferantenlandschaft wird eine Realität deutlich: Manuelles Third Party Risk Management skaliert nicht. Große Organisationen arbeiten mit Hunderten, teilweise Tausenden Drittparteien. Re-Bewertungen, Vertragsaktualisierungen, Monitoring-Auswertungen und Auditnachweise erzeugen eine Datenmenge, die rein manuell kaum beherrschbar ist. Automatisierung wird hier nicht zur Komfortfunktion, sondern zum Stabilitätsfaktor.

Moderne Governance-Systeme ermöglichen die automatische Bewertung und Priorisierung: automatische Gewichtung von Self-Assessments, Plausibilitätsprüfung inkonsistenter Angaben, Abgleich mit bekannten Sicherheitsvorfällen und dynamische Anpassung von Risikoscores. Statt statischer Jahresbewertungen entsteht eine kontinuierliche Risikobetrachtung.

Ein Beispiel: Ein kritischer IT-Dienstleister meldet einen Sicherheitsvorfall. Das Incident-Management-System übermittelt ein Ereignis, der Risikoscore wird automatisch angepasst, Maßnahmen werden neu priorisiert. So wird aus Dokumentation operative Steuerung. Automatisierung ersetzt dabei nicht die Entscheidung – sie strukturiert die Entscheidungsgrundlage.

Eine besondere Stärke von Systemen mit künstlicher Intelligenz (KI) liegt in der Erkennung indirekter Abhängigkeiten: Mehrere Lieferanten nutzen denselben Sub-Cloud-Anbieter, identische Schwachstellen treten bei verschiedenen Drittparteien auf, wiederkehrende Kontrolllücken zeigen strukturelle Defizite. Solche Zusammenhänge bleiben in isolierten oder Excel-basierten Verfahren häufig unsichtbar. Gerade vor dem Hintergrund regulatorischer Anforderungen zu Konzentrationsrisiken gewinnt diese Fähigkeit strategische Bedeutung. KI wird hier zum Instrument, um systemische Risiken sichtbar zu machen – nicht nur einzelne Ereignisse.

Neben Bewertung und Analyse entsteht Mehrwert vor allem im Bereich der automatisierten Nachweisführung: versionierte Bewertungsstände, automatische Report-Generierung, Historienanalyse von Risikoverläufen und konsistente Management-Dashboards. Der manuelle Aufwand sinkt, die Transparenz steigt. Automatisierung erhöht nicht nur Effizienz, sondern auch Nachvollziehbarkeit – und Nachvollziehbarkeit ist die Grundlage regulatorischer Resilienz.

VERANTWORTUNG AUF LEITUNGSEBENE

Supply-Chain-Sicherheit ist kein Spezialthema der IT, sondern Ausdruck moderner Unternehmensführung. Wo Wertschöpfung vernetzt ist, muss auch Governance vernetzt sein. Resilienz entsteht nicht durch Isolation, sondern durch Transparenz, Verbindlichkeit und kontinuierliche Steuerung. Mit der Integration externer Risiken in das Risk Register, die Vertragsarchitektur, das Monitoring und die automatisierte Bewertung verschiebt sich die Perspektive endgültig: Lieferantenmanagement ist kein Nebenprozess, sondern Teil der strategischen Steuerungsarchitektur.

Damit wird auch die Verantwortung klarer – und sie verteilt sich auf mehrere Schultern:

- **Für CIO und CISO ist Third Party Risk Management Teil der Sicherheitsarchitektur:** Externe Zugriffe gehören ins Monitoring, Risikoscores müssen im zentralen Risk Register sichtbar sein, Konzentrationsrisiken sind aktiv zu analysieren, und Vertragsanforderungen müssen technisch nachvollziehbar sein. Die Aufgabe besteht nicht darin, Fragebögen zu verwalten, sondern externe Risiken steuerbar zu machen.

- **Für die Geschäftsführung sind Supply-Chain-Risiken strategische Risiken:** Abhängigkeiten beeinflussen die Geschäftskontinuität, Konzentrationsrisiken können systemische Auswirkungen haben, und fehlende Vertragsklarheit erhöht Haftungsrisiken. Transparenz reduziert die persönliche Verantwortung nicht – aber sie macht sie beherrschbar. Investitionen in strukturierte Integration und Automatisierung sind daher keine IT-Kosten, sondern Resilienz-Investitionen.

- **Für Beschaffung und Compliance gilt:** Sicherheitsanforderungen definieren sie vor Vertragsabschluss, Klassifizierung ist verpflichtend, Sicherheitsklauseln müssen risikobasiert sein und Auditfähigkeit ist ein Wettbewerbsfaktor. Beschaffung wird damit nicht nur zur wirtschaftlichen, sondern auch zur regulatorischen Schnittstelle.

VON DER NORM ZUR WIRKUNG – DER GESCHLOSSENE KREIS

Normen definieren Anforderungen, Governance strukturiert Verantwortung, Technologie ermöglicht Skalierung und Transparenz schafft Entscheidungsfähigkeit. Erst wenn diese Elemente zusammenwirken, entsteht Wirkung. Sicherheit endet nicht am Werkstor – sie beginnt dort, wo Organisationen ihre Abhängigkeiten erkennen und aktiv steuern.

Was Sie mitnehmen sollten:

- Lieferantenrisiken sind Compliance- und Haftungsrisiken.
- TPRM muss risikobasiert, vertraglich verankert und systemisch integriert sein.
- Monitoring und Dashboard-Transparenz schaffen Steuerungsfähigkeit.
- Automatisierung ermöglicht Skalierung ohne Kontrollverlust.
- Governance ist heute ökosystemisch – nicht isoliert.

Unternehmen, die Supply-Chain-Sicherheit nur als regulatorische Pflicht verstehen, verwalten Komplexität. Unternehmen, die sie als strategischen Hebel begreifen, gestalten Resilienz. Damit schließt sich die Klammer dieser Reihe: „Von der Norm zur Wirkung" bedeutet, Verantwortung dort wahrzunehmen, wo Wertschöpfung tatsächlich stattfindet – im vernetzten System. ■

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

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

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

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

Jeder Beitrag entwickelt praxisnahe Lösungsansätze und zeigt, wie diese in Rollen, Abläufen und Kennzahlen verankert werden können.

Die Serie richtet sich an Führungskräfte ebenso wie an Fachverantwortliche, die regulatorische Anforderungen nicht allein als Pflicht, sondern als Chance zur Verbesserung von Steuerung, Transparenz und Leistungsfähigkeit begreifen möchten.

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

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

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.

PrivacyAware zeigt per Ampelsystem, wie stark Websites ihre Besucher verfolgen

BROWSER-ERWEITERUNG MACHT WEBTRACKING SICHTBAR

Cookie-Banner bitten um Zustimmung zu etwas, das sie nicht verständlich erklären. Adblocker blockieren Tracker, machen aber selten transparent, was genau im Hintergrund geschieht. Mit PrivacyAware hat das Institut für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen eine kostenlose Browser-Erweiterung entwickelt, die Tracking sichtbar macht und Nutzern eine fundierte Entscheidung ermöglicht, bevor sie ihre Daten preisgeben.

Wer eine Webseite aufruft, hinterlässt Spuren. Cookies, Pixel-Tags und Fingerprinting-Verfahren erfassen Klickverhalten, Verweildauer, Suchanfragen und Geräteinformationen. Aus diesen Daten entstehen detaillierte Profile, die Rückschlüsse auf Interessen, Kaufabsichten und politische Einstellungen erlauben. Je präziser ein solches Profil, desto mehr ist es wert: Der globale digitale Werbemarkt soll 2026 rund 712 Milliarden US-Dollar erreichen.[2]

Für die meisten Betroffenen bleiben diese Vorgänge unsichtbar. Viele Onlinedienste wirken kostenfrei, finanzieren sich aber über personalisierte Werbung und datenbasierte Marktanalysen. Webtracking liefert dafür die technische Grundlage. Die eingesetzten Verfahren reichen von einfachen Cookies bis zu komplexen Fingerprinting-Techniken, die Geräte anhand ihrer Hardware- und Software-Konfiguration identifizieren. Welche Daten dabei konkret erhoben, zusammengeführt und weitergegeben werden, erfahren Nutzer in der Regel nicht.

UNTERNEHMEN WISSEN MEHR ALS NUTZER

So entsteht eine strukturelle Informationsasymmetrie: Unternehmen wissen viel über ihre Nutzer – die wissen wenig über die Unternehmen, die ihre Daten verarbeiten. Regulatorische Rahmenbedingungen wie die Datenschutz-Grundverordnung (DSGVO) und das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) setzen dem zwar Grenzen, doch zwischen Rechtsanspruch und Alltagserfahrung klafft eine Lücke. Cookie-Banner fragen nach Einwilligung, erklären aber selten, worin man tatsächlich einwilligt. Datenschutzerklärungen sind umfassend, aber kaum jemand liest sie.

Das Institut für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen hat nun die Browser-Erweiterung PrivacyAware entwickelt. Sie macht Tracking-Mechanismen sichtbar, bewertet Webseiten nach ihrer Tracking-Intensität und ermöglicht eine informierte Entscheidung, bevor Nutzer ihre Daten preisgeben.

ADBLOCKER BLOCKIEREN, ERKLÄREN ABER NICHT

Auf dem Markt existieren bereits zahlreiche Browser-Erweiterungen, die Werbung und Tracker blockieren. Doch die meisten Adblocker konzentrieren sich auf die technische Blockierung, eine verständliche, vergleichende Transparenz über Art, Umfang und Zweck der eingesetzten Tracking-Verfahren bieten sie kaum. Nutzer erhalten Schutz, jedoch keine Entscheidungsgrundlage.

Hinzu kommt, dass die technische Basis für die Erkennung selbst oft lückenhaft ist. So zeigen aktuelle Untersuchungen, dass viele regionalspezifische Filterlisten die Erwartungen an den Schutz der Nutzer nicht erfüllen. Rund 93 Prozent der darin enthaltenen Regeln erweisen sich in der Praxis als wirkungslos beim Erkennen von Tracking-Anfragen.[6] Selbst wer einen Adblocker einsetzt, kann sich also nicht sicher sein, tatsächlich umfassend geschützt zu werden.

Auch wer technisch geschützt ist, erfährt selten, welche Tracker blockiert wurden, zu welchem Zweck sie Daten erheben wollten und welche Unternehmen dahinterstehen. Dabei setzt Online-Tracking rechtlich eine informierte Einwilligung voraus. Die aus dem Tracking resultierenden Risiken bleiben ebenfalls im Dunkeln – sowohl Privacy-Risiken wie Profilbildung und Re-Identifizierbarkeit als auch Security-Risiken wie Datenlecks oder eine erhöhte Angriffsfläche durch Drittanbieter-Skripte.

COOKIE-BANNER ÜBERFORDERN

Dabei wären informierte Entscheidungen rechtlich geboten. Cookie-Banner sollen genau das ermöglichen. In der Praxis überfordern sie jedoch den Anwender. Komplexe Texte, irreführende Gestaltung und eine hohe Zahl an Auswahlmöglichkeiten führen dazu, dass Nutzer Entscheidungen eher aus Bequemlichkeit treffen als aus Überzeugung. Statt tatsächlicher Kontrolle entsteht lediglich der Eindruck von Mitbestimmung.

Die Zahlen bestätigen das: Eine Bitkom-Studie mit 1.013 Internetnutzern ab 16 Jahren zeigt, dass drei Viertel der Befragten (76 Prozent) von Cookie-Bannern genervt sind. Etwa die Hälfte (51 Prozent) verzichtet auf bestimmte Onlineangebote, weil diese zu viele Cookies verwenden.[3] Viele Menschen bemerken also die Datenerfassung – verstehen oder einordnen können sie diese aber häufig nicht.

Aus dieser Überforderung entsteht, was Forscher als „Privacy Fatigue" bezeichnen: emotionale Erschöpfung, Zynismus oder Hilflosigkeit gegenüber den ständigen Datenschutzanforderungen.[5] Wer permanent entscheiden soll, was er akzeptiert, ohne die Konsequenzen zu verstehen, hört irgendwann auf, sich zu kümmern.

Unsichtbares Tracking wirkt nicht nur technisch, sondern auch psychologisch. Nutzer fühlen sich beobachtet, selbst wenn die Daten anonymisiert erscheinen.[4] Gezielte Werbung und personalisierte Inhalte können Entscheidungen stark beeinflussen – beim Onlineshopping ebenso wie bei der politischen Meinungsbildung. Die permanente Sammlung persönlicher Daten erzeugt Stress, Misstrauen und das Gefühl von Kontrollverlust. Studien belegen, dass Tracking ohne transparente Information zu negativen Emotionen und Verhaltensänderungen führen kann.[1, 5]

Die zentrale Frage lautet daher nicht, ob Tracking stattfindet, sondern ob Nutzer verstehen, was mit ihren Daten geschieht, und auf dieser Basis selbst entscheiden können.

AMPELSYSTEM ZEIGT TRACKING-INTENSITÄT

PrivacyAware setzt an genau dieser Lücke an. Statt Tracker zu blockieren, macht die Browsererweiterung sie sichtbar: Welche Tracking-Technologien setzt eine Webseite ein? Wie intensiv verfolgt sie im Vergleich zu anderen? Und wie datenschutzfreundlich ist sie wirklich?

Das Grundprinzip: Wer eine Webseite aufruft, sieht über ein Ampelsystem auf den ersten Blick, wie stark dort getrackt wird. Grün signalisiert

geringes Tracking, Gelb eine mittlere Ausprägung, Rot warnt vor intensiver Datenerfassung. Die Entscheidung, ob man die Seite trotzdem nutzt, bleibt beim Nutzer. Das Tool trifft somit keine automatisierten Entscheidungen, sondern liefert die Grundlage für eigene.

Ein zentrales Merkmal unterscheidet PrivacyAware von anderen Tools: die präventive Transparenz. Bereits in den Trefferlisten von Suchmaschinen wie Google erscheinen Symbole neben den Links, die das Tracking-Niveau der jeweiligen Seite anzeigen. Nutzer erfahren also nicht erst nach dem Besuch einer Webseite, wie es um deren Datenschutz steht, sondern davor.

Bestehende Privacy-Tools wie Privacy Badger, Ghostery oder uBlock Origin leisten gute Arbeit beim Blockieren von Trackern und Werbung. So erkennt Privacy Badger Tracking-Domains heuristisch und blockiert sie automatisch. Es zeigt Nutzern aber nicht, welche Daten konkret erhoben werden sollten. Ghostery geht einen Schritt weiter und kategorisiert erkannte Tracker nach Unternehmen und Zweck. uBlock Origin arbeitet hocheffizient mit Filterlisten, setzt jedoch vollständig auf Blockierung ohne Transparenzebene. Keines dieser Programme bewertet Webseiten präventiv, bevor man sie aufruft, und keines ermöglicht einen systematischen Vergleich zwischen Webseiten oder Branchen.

Gedacht ist PrivacyAware auch nicht als Konkurrenz zu diesen Werkzeugen, sondern als Ergänzung. Wo Adblocker filtern, soll das Tool einordnen. Wo andere blockieren, schafft es Verständnis.

KOLLEKTIVES WISSEN DURCH GEMEINSAME DATEN

PrivacyAware baut dabei auf einem kollektiven Analyseansatz auf. Wer die Erweiterung nutzt, kann – freiwillig und mit Widerrufsrecht – anonymisierte Tracking-Daten an ein zentrales System übermitteln. Dort fließen sie mit den Ergebnissen automatisierter Scans zusammen, die das System unabhängig von einzelnen Anwendern regelmäßig durchführt. Dabei erfasst das Programm systematisch eingesetzte Tracking-Technologien – besonders Cookies, Fingerprinting-Verfahren und Pixel-Tags – und aktualisiert die Bewertungsgrundlage fortlaufend. So entsteht ein kontinuierlich wachsender Datenpool, von dem alle profitieren.

Damit dieser Pool verlässlich bleibt, gleicht PrivacyAware gespendete Daten technisch mit einer definierten „Ground Truth" ab, also einem Referenzwert aus eigenen Scans. Das reduziert Manipulationsversuche und stellt sicher, dass die Bewertungen auf einer belastbaren Grundlage basieren.

Dieser kollektive Ansatz ermöglicht etwas, das Einzellösungen nicht leisten können: eine vergleichende Betrachtung. Setzen die Webseiten bestimmter Handelsketten systematisch mehr Tracker ein als andere? Wie schneidet eine Branche im Vergleich ab? Die Ergebnisse sind über eine eigene Webseite öffentlich zugänglich. Dort entsteht ein Ranking, das aus dem aktuellen Bestand geprüfter Domains sowohl die fünf mit der geringsten als auch die fünf mit der höchsten Tracking-Intensität ausweist. So werden strukturelle Unterschiede im Umgang mit Nut-

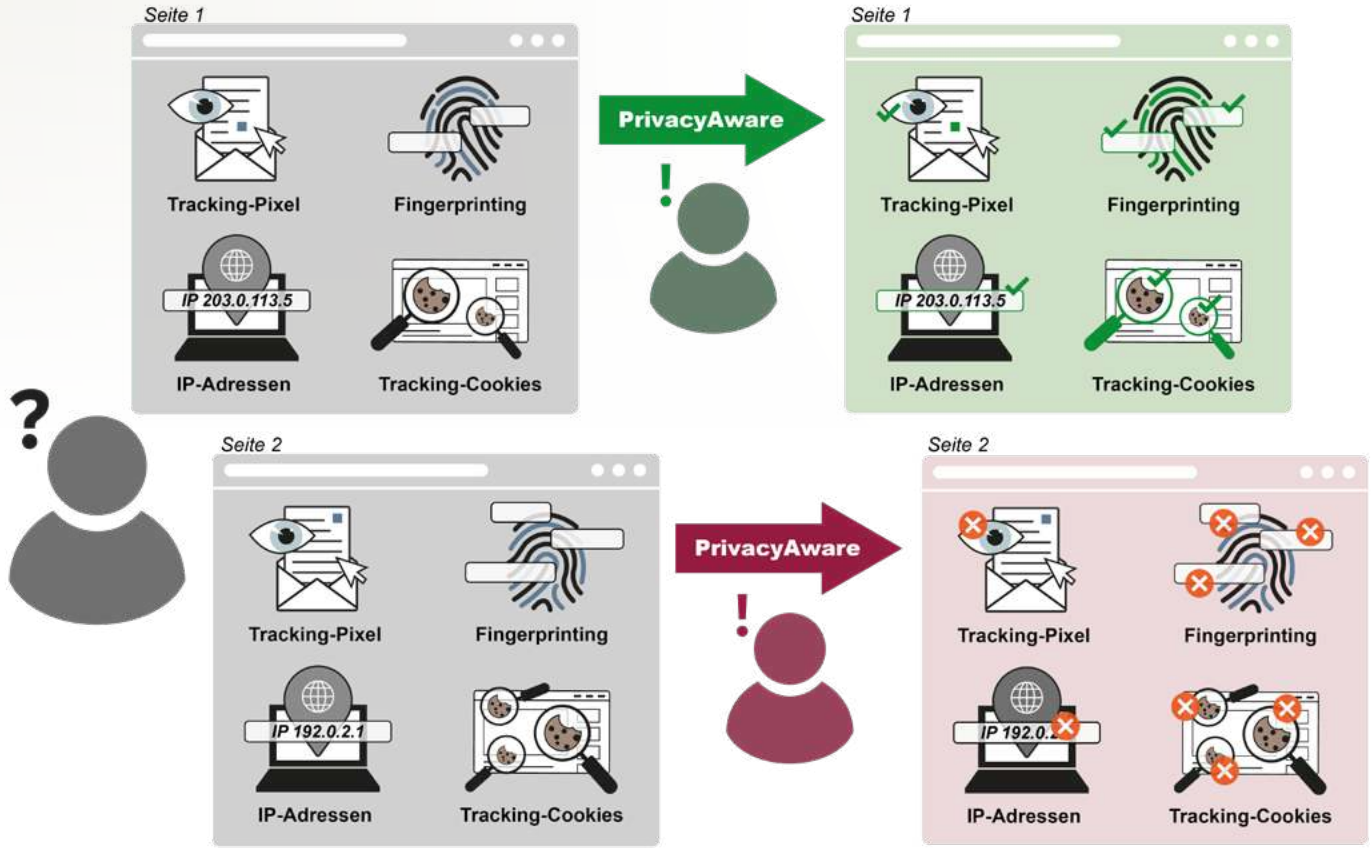


Abbildung 1: PrivacyAware (Bild: if(is))

zerdaten sichtbar – über den Einzelfall hinaus und für jeden einsehbar.

Neben der Tracking-Analyse prüft die Erweiterung auch, ob eine Domain potenziell schädliche Inhalte enthält, etwa Malware, Phishing oder betrügerische Angebote. Sie verbindet so Datenschutz-Transparenz mit grundlegender Sicherheitsinformation.

FÜR ALLE NUTZER GEDACHT

Mit PrivacyAware richten sich die Entwickler an alle, die das Internet nutzen, unabhängig vom technischen Vorwissen. Ferner kann es Aufsichtsbehörden und Datenschutzbeauftragten bei Prüfungen helfen, indem es Tracking-Technologien sichtbar macht und kritische Passagen in Datenschutzerklärungen hervorhebt. Das Browser-Add-on ist ein Angebot des Instituts für Internet-Sicherheit[7] und wird zusätzlich über den Marktplatz IT-Sicherheit[8] bereitgestellt. Das Projekt verfolgt keinen kommerziellen Zweck. Ziel ist es, möglichst vielen Menschen einen informierten Umgang mit dem Internet zu ermöglichen.

Darüber hinaus soll PrivacyAware von Behörden, Initiativen und Verbänden unterstützt und verbreitet werden. Ein sichereres Internet entsteht nicht allein durch individuelle Maßnahmen. Es braucht kollektive Ansätze, um Transparenzstandards zu stärken, Vergleichbarkeit zu ermöglichen und Anreize für eine datenschutzfreundlichere Gestaltung von Onlineangeboten zu schaffen.

FUNKTIONEN IM DETAIL

PrivacyAware untersucht jede Webseite auf drei zentrale Tracking-Technologien – Cookies, Fingerprinting und Pixel-Tags –, bewertet deren Eingriffsintensität und verdichtet die Ergebnisse zu einer Gesamteinschätzung. Ergänzend analysiert es Datenschutzerklärungen und prüft Domains auf Sicherheitsrisiken. Im Folgenden ein Blick auf die einzelnen Bausteine.

COOKIES NACH EINGRIFFSINTENSITÄT GEWICHTET

Cookie ist nicht gleich Cookie. PrivacyAware erkennt die auf einer Webseite gesetzten Cookies und ordnet sie auf Basis der Referenzdatenbank Cookiepedia automatisch Kategorien zu:

- **Strictly Necessary:** technisch erforderlich für die Grundfunktion der Webseite
- **Functionality:** Komfortfunktionen wie Spracheinstellungen oder Layout-Präferenzen
- **Performance:** Analyse und Optimierung der Webseite
- **Targeting/Advertising:** Werbung und Profilbildung
- **Unknown:** Zweck unklar
- **No Data:** keine Informationen verfügbar

Entscheidend ist dabei, dass die Browser-Erweiterung Cookies nicht einfach zählt, sondern sie nach ihrer Eingriffsintensität gewichtet. Cookies aus den Kategorien Targeting und Advertising fließen am stärksten in die Bewertung ein, weil sie der Profilbildung und verhaltensbasierten Analyse dienen. Auch manche Performance-Cookies, etwa von Google, dienen dem Tracking und erhalten eine höhere Gewichtung. Nicht klassifizierte und unbekannte Cookies stuft das Tool als potenziell risikobehaftet ein. Technisch notwendige Cookies dagegen fließen kaum in die Bewertung ein.

Damit unbekannte Cookies nicht dauerhaft als Risiko gewertet werden, kommen zwei Mechanismen zum Einsatz: Dynamische Mustererkennung (Regex) ordnet technisch bedingte, variierende Cookie-Namen korrekt zu. Zusätzlich gleicht die Erweiterung unbekannte Cookies kontinuierlich über die Cookiepedia-API ab und korrigiert die Einstufung, sobald neue Informationen vorliegen.

FINGERPRINTING ERKENNEN

Fingerprinting gehört zu den invasivsten Tracking-Methoden, und zu den unsichtbarsten. Anders als Cookies lässt es sich nicht einfach löschen, weil es keine Daten auf dem Gerät speichert. Stattdessen identifiziert es Nutzer anhand der individuellen Kombination von Hardware- und Softwaremerkmalen ihres Gerätes.

PrivacyAware analysiert den geladenen JavaScript-Stack einer Webseite heuristisch und erkennt dabei fünf Fingerprinting-Kategorien:

- **Canvas-Fingerprinting** identifiziert Geräte über unsichtbare Grafik-Renderings im Browser.
- **WebGL-Fingerprinting** wertet 3D-Grafikverarbeitung und Treiberinformationen aus.
- **Audio-Fingerprinting** erkennt Geräte anhand der Signalverarbeitung über die Web Audio API.
- **Font-Fingerprinting** analysiert installierte und darstellbare Schriftarten.
- **Media-Device-Fingerprinting** erfasst angeschlossene Geräte wie Kamera oder Mikrofon.

Die Bewertung erfolgt über ein gewichtetes Punktesystem, das die Eingriffstiefe widerspiegelt. WebGL-Fingerprinting erhält mit drei Punkten die höchste Gewichtung, weil es tiefgreifende Systeminformationen einbezieht. Canvas- und Audio-Fingerprinting liegen mit je zwei Punkten im Mittelfeld. Browsernahe Verfahren wie Font- und Media-Device-Erkennung fließen als Basis-Identifikatoren mit einem Punkt ein.

PIXEL-TAGS ZÄHLEN

Pixel-Tags – auch Zählpixel oder Tracking-Pixel genannt – sind winzige, unsichtbare Bilddateien, die beim Laden einer Webseite eine Verbindung zu einem Server aufbauen und so den Besuch registrieren. Die Erweiterung erkennt diese Pixel dynamisch: Beim Seitenaufruf erfasst sie die zunächst eingebundenen Pixel, bei Interaktionen wie Scrollen registriert sie nachladende Elemente.

Die erkannten Pixel-Tags unterscheidet das Tool nach First-Party- und Third-Party-Elementen. Eine erhöhte Anzahl gilt als Indikator für höhere Tracking-Intensität und fließt als normierter Teilscore in die Gesamtbewertung ein – allerdings mit geringerer Gewichtung als Cookies und Fingerprinting.

GRÜN, GELB ODER ROT

Alle Analyseergebnisse – Cookies, Fingerprinting, Pixel-Tags – fließen in ein Ampelsystem ein, das die Tracking-Intensität einer Webseite auf eine Farbe verdichtet: Grün bedeutet geringes Tracking – Nutzung aus Datenschutzsicht unkritisch. Gelb bedeutet mittleres Tracking – erhöhte Aufmerksamkeit empfohlen. Rot bedeutet intensives Tracking – Besuch aus Datenschutzperspektive nicht empfohlen.

Die Ampelfarben sind eine Empfehlung, keine Sperre. Wer eine rot bewertete Seite trotzdem besuchen will, kann das jederzeit tun. Das

Ampelsystem hilft, Risiken schnell zu erfassen, ohne sich durch technische Details arbeiten zu müssen.

Darüber hinaus bietet PrivacyAware drei weitere Funktionen:

- **Datenschutzerklärungen auf den Punkt bringen:** Kaum jemand liest Datenschutzerklärungen vollständig. PrivacyAware übernimmt die Vorarbeit: Die Funktion „Privacy Critics" durchsucht die Datenschutzerklärung einer Webseite nach potenziell kritischen Begriffen wie „Weitergabe", „Dritte" oder „Profiling". Die entsprechenden Sätze extrahiert die Erweiterung, hebt die Schlüsselwörter fett und rot hervor und zeigt sie übersichtlich an. Ergänzend visualisiert das Tool die kritischen Begriffe durch standardisierte Datenschutz-Icons. Diese ikonografische Darstellung reduziert komplexe Inhalte auf das Wesentliche und macht zentrale Aspekte der Datenverarbeitung schnell erfassbar – ohne dass man die vollständige Erklärung lesen muss.

- **Schutz vor schädlichen Webseiten:** Über die Schnittstelle zu Google Safe Browsing prüft PrivacyAware beim Aufruf einer Webseite, ob deren Adresse auf einer aktuellen Bedrohungsliste steht, etwa wegen Phishing, Malware oder betrügerischer Inhalte. Dabei wird lediglich ein verkürzter Hash der URL übermittelt, die Privatsphäre bleibt also gewahrt.

- **Blacklist und Whitelist:** Das Tool bietet ein integriertes Filtersystem, mit dem Nutzer problematische Domains präventiv blockieren können. Die Blacklist umfasst Kategorien wie Glücksspiel, Fake News, Adult Content, Social Media sowie bekannte Tracking- und Werbedomains. Die Whitelist ermöglicht es, zuvor blockierte Domains gezielt wieder freizugeben. Zusätzlich lassen sich eigene Domainlisten im TXT-Format hochladen – für individuelle Kontrolle über den eigenen Webzugang.

TRANSPARENZ ALS GRUNDLAGE FÜR VERTRAUEN

Webtracking ist ein struktureller Bestandteil der digitalen Ökonomie. Trotz regulatorischer Rahmenbedingungen bleibt die tatsächliche Datenverarbeitung für viele Nutzer intransparent. Die im Beitrag dargestellten Befunde und Studien zeigen: Rein formale Einwilligungsmechanismen reichen häufig nicht aus, um informierte Entscheidungen zu ermöglichen. Phänomene wie Privacy Fatigue machen deutlich, dass fehlende Verständlichkeit und kognitive Überlastung zentrale Hindernisse für die digitale Selbstbestimmung sind.

Transparenz im Umgang mit Tracking-Mechanismen und personenbezogenen Daten bleibt deshalb eine Grundvoraussetzung für die digitale Selbstbestimmung. Wer digitale Dienste langfristig akzeptieren soll, muss ihnen vertrauen können. Transparenz schafft dieses Vertrauen, weil sie informierte Entscheidungen ermöglicht und Informationsasymmetrien reduziert.

PrivacyAware verfolgt deshalb keinen primär blockierenden, sondern einen transparenzorientierten Ansatz. Die systematische Erkennung von Cookies, Fingerprinting-Techniken und Pixel-Tags, die strukturierte Kategorisierung, das Ampelsystem und der branchenbezogene Vergleich machen Tracking nicht nur technisch sichtbar, sondern auch einordbar und vergleichbar. Die visuelle Aufbereitung von Datenschutzerklärungen reduziert zusätzlich die kognitive Belastung.

Der Mehrwert für die Benutzer liegt in der Verbindung von technischer Analyse und verständlicher Darstellung. So entsteht eine belastbare Grundlage für fundierte Entscheidungen im digitalen Raum. ■

Literaturverzeichnis

[1] *Sivan-Sevilla, I., & Poudel, P. (2024). Web privacy based on contextual integrity: Measuring the collapse of online contexts. arXiv. https://arxiv.org/abs/2412.16246*

[2] *Global Market Statistics. (2026). Digital advertising market size, share, growth and industry forecast: Global digital advertising market report. https://www.globalmarketstatistics.com/de/market-reports/digital-advertising-market-12281*

[3] *Bitkom Research. (2024, 25. März). Drei Viertel sind von Cookie-Bannern genervt. Bitkom Research. https://bitkom-research.de/news/drei-viertel-sind-von-cookie-bannern-genervt*

[4] *Coopamootoo, K. P. L., Mehrnezhad, M., & Toreini, E. (2022). "I feel invaded, annoyed, anxious and I may protect myself": Individuals' feelings about online tracking and their protective behaviour across gender and country. arXiv. https://arxiv.org/abs/2202.04682*

[5] *van der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online privacy fatigue: A scoping review and research agenda. Future Internet, 15(5), Article 164. https://doi.org/10.3390/fi15050164*

[6] *Böttger, T., et al. (2025). Understanding regional filter lists: Efficacy and impact. Proceedings on Privacy Enhancing Technologies (PoPETs), 2025(2), 309–325. https://doi.org/10.56553/popets-2025-0063*

[7] *Institut für Internet-Sicherheit: https://internet-sicherheit.de/*

[8] *Marktplatz IT-Sicherheit: https://it-sicherheit.de/*

BARYALAI USMANI
studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit „Privatsphäre im Internet und Security Awareness".

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

OLIVER SCHONSCHEK
ist wissenschaftlicher Mitarbeiter mit dem Forschungsschwerpunkt „IT-Sicherheit für KMUs" im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen.

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

Awareness, die wirkt!

Wecken Sie die Superhelden in Ihrem Unternehmen

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

Inhalte

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

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

DATAKONTEXT

Cyber Resilience Act

WAS DIE EU-VERORDNUNG VON UNTERNEHMEN MIT VERNETZTEN PRODUKTEN VERLANGT

Mit dem Cyber Resilience Act (CRA) hat die Europäische Union erstmals eine unmittelbar geltende Verordnung geschaffen, die EU-weit einheitliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen festlegt. Auch wenn der CRA erst ab Dezember 2027 vollständig anwendbar ist, sollten Unternehmen die Anforderungen früh einplanen – besonders, wenn sie vernetzte Produkte entwickeln, einkaufen oder in der EU vertreiben.

Der Cyber Resilience Act (CRA) ist seit dem 10. Dezember 2024 in Kraft und gilt als EU-Verordnung unmittelbar in allen Mitgliedstaaten – ein nationales Umsetzungsgesetz ist nicht nötig. Die Pflichten greifen allerdings stufenweise, wobei für Unternehmen zwei Fristen entscheidend sind: Ab September 2026 müssen Hersteller aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle melden – Prozesse, Zuständigkeiten und Meldewege sollten bis dahin stehen. Ab Dezember 2027 gilt der CRA dann vollständig: Produkte mit digitalen Elementen dürfen nur noch in Verkehr gebracht werden, wenn sie sämtliche Anforderungen der Verordnung erfüllen. Nicht konforme Produkte dürfen dann auch nicht mehr weiterverkauft werden.

Wer Melde- und Updateprozesse frühzeitig aufsetzt und die CRA-Anforderungen in Entwicklung sowie Beschaffung verankert, spart sich später aufwendige und teure Nacharbeiten. Konkret bedeutet das: Unternehmen sollten jetzt klären, welche ihrer Produkte unter die Verordnung fallen, welche Rolle sie in der Lieferkette einnehmen und welche Nachweise sie künftig erbringen müssen.

WER UND WAS IST BETROFFEN?

Ob und wie der CRA ein Unternehmen betrifft, hängt maßgeblich von seiner Rolle in der Lieferkette ab. Die Verordnung unterscheidet dabei insbesondere:

- **Hersteller:** Person, die Produkte mit digitalen Elementen entwickelt oder herstellt, konzipiert oder entwickeln beziehungsweise herstellen lässt und sie unter eigenem Namen oder eigener Marke vermarktet.

- **Bevollmächtigter:** Person, die ein Hersteller schriftlich beauftragt und die in seinem Namen bestimmte Aufgaben übernimmt.

- **Einführer:** in der EU niedergelassene Person, die ein Produkt mit digitalen Elementen unter dem Namen beziehungsweise der Marke einer nicht in der EU niedergelassenen Person in der Union in Verkehr bringt.

- **Händler:** Person, die ein Produkt mit digitalen Elementen ohne Änderungen auf dem Unionsmarkt bereitstellt, ohne Hersteller oder Einführer zu sein.

In den Anwendungsbereich fallen grundsätzlich alle Produkte mit digitalen Elementen, die in der EU in Verkehr gebracht werden. Das betrifft Hard- und Software, einschließlich separat in Verkehr gebrachter Komponenten, sowie Lösungen zur Datenfernverarbeitung. Typische Beispiele sind vernetzte Haushaltsgeräte (Smart-Kühlschränke, Waschmaschinen, Saugroboter), Smartwatches, Smart-TVs oder Software wie Apps, aber auch Industriemaschinen, die heutzutage kaum noch ohne Softwarekomponenten auskommen.

Ausgenommen sind unter anderem Medizinprodukte und Fahrzeuge, die bereits eigenen EU-Regularien unterliegen, sowie Open-Source-Software, die ohne Gewinnerzielungsabsicht bereitgestellt wird.

WELCHE KERNANFORDERUNGEN STELLT DER CRA?

Im Kern bündelt der CRA seine Anforderungen in fünf zentralen Themenfeldern:

- **Security by Design:** Cybersicherheit muss schon in der Entwicklung mitgedacht werden. Dazu gehören zum Beispiel die Verschlüsselung gespeicherter oder übermittelter Daten und ein Design, das die Angriffsfläche möglichst klein hält.

- **Security by Default:** Produkte sollen standardmäßig mit den sichersten Einstellungen ausgeliefert werden. Nutzer sollen ein hohes Sicherheitsniveau erreichen, ohne erst Konfigurationen nachziehen zu müssen – damit Sicherheit nicht nur von „Power-Usern“ abhängt.

- **Risikobewertung:** Unternehmen müssen Sicherheitsrisiken rund um den Betrieb und die Nutzung des Produkts identifizieren, bewerten und reduzieren.

- **Schwachstellenmanagement:** Hersteller müssen Schwachstellen systematisch identifizieren, dokumentieren und zeitnah beheben. Dazu gehört auch, eine öffentlich zugängliche Übersicht bekannter Schwachstellen zu führen, einen Kommunikationskanal bereitzustellen und erforderliche Sicherheitsupdates kostenlos über sichere Kanäle auszurollen. Nutzende sind über Schwachstellen, deren Auswirkungen und verfügbare Updates zu informieren. Für die Meldung aktiv ausgenutzter Schwachstellen und schwerwiegender Sicherheitsvorfälle an Behörden gelten enge Fristen.

- **Software Bill of Materials (SBOM):** Sämtliche Softwarekomponenten müssen intern dokumentiert werden.

HERSTELLERPFLICHTEN

Viele dieser Kernanforderungen konkretisiert der CRA in den Herstellerpflichten. Da Hersteller der Produktentwicklung am nächsten stehen, treffen sie die umfangreichsten Pflichten – der CRA unterscheidet dabei zwischen Anforderungen vor und nach dem Inverkehrbringen.

Vor dem Inverkehrbringen müssen Hersteller eine Konformitätsbewertung durchführen. Der Nachweis erfolgt über die CE-Kennzeichnung. Anbringen dürfen sie das CE-Zeichen allerdings nur, wenn das Produkt sämtliche einschlägigen Cybersicherheitsanforderungen erfüllt. Die Verordnung kennt verschiedene Konformitätsbewertungsverfahren (New-Legislative-Framework-(NLF)-Module):

- **Modul A:** Selbstbewertung

- **Modul B + C: B**aumusterprüfung durch eine notifizierte Stelle

- **Modul H:** Prüfung des Qualitätsmanagementsystems durch eine notifizierte Stelle

Welches Verfahren dabei zum Einsatz kommt, richtet sich nach der Produktkategorie: Für Standardprodukte genügt in vielen Fällen eine Selbstbewertung. Bei „wichtigen“ Produkten nach Anhang III des CRA steigen die Anforderungen – je nach Produkt kann eine Prüfung

Vor dem Inverkehrbringen müssen Hersteller eine Konformitätsbewertung durchführen.

Nach dem Inverkehrbringen müssen Hersteller das Produkt über die erwartete Lebensdauer überwachen. Zudem müssen sie Schwachstellen und Sicherheitsvorfälle melden.

durch Dritte nötig sein. Für „kritische“ Produkte nach Anhang IV ist eine Zertifizierung nach dem EU-Zertifizierungsschema zwingend vorgeschrieben.

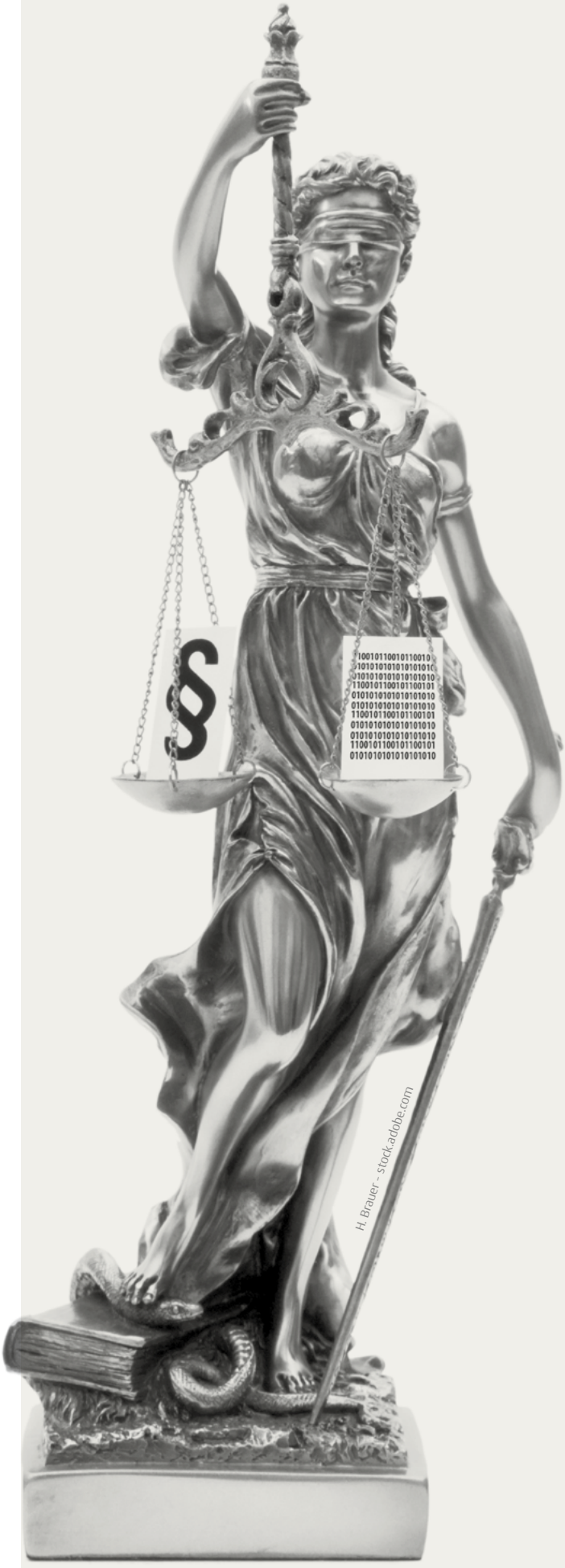
Darüber hinaus müssen Hersteller eine Risikobewertung durchführen und dokumentieren. Die Ergebnisse sind über den gesamten Produktlebenszyklus zu berücksichtigen. Außerdem sind technische Dokumentation, De-Anonymisierung und ein Identifikationskennzeichen für das Produkt erforderlich.

Nach dem Inverkehrbringen müssen Hersteller das Produkt über die erwartete Lebensdauer überwachen. Zudem müssen sie Schwachstellen und Sicherheitsvorfälle melden. Dafür sieht der CRA strenge Fristen vor: binnen 24 Stunden eine Frühwarnung und binnen 72 Stunden eine vollständige Meldung. Die Meldungen erfolgen über eine zentrale EU-Plattform.

PFLICHTEN DER ANDEREN AKTEURE

Auch die weiteren Akteure in der Lieferkette stehen in der Pflicht. So tragen Einführer eine wesentliche Kontrollfunktion: Sie müssen prüfen, ob der Hersteller das Konformitätsverfahren ordnungsgemäß durchlaufen hat und ob technische Dokumentation, CE-Kennzeichnung sowie Konformitätserklärung vorliegen. Sind Mängel erkennbar, müssen sie Korrekturmaßnahmen einleiten. Die zugehörige Dokumentation ist mindestens zehn Jahre lang aufzubewahren. Auf begründetes Verlangen müssen Einführer den Marktüberwachungsbehörden alle relevanten Informationen bereitstellen. Stellt der Hersteller seinen Betrieb ein, sind Einführer zudem verpflichtet, sowohl die Behörden als auch die Nutzenden darüber zu informieren.

Händler wiederum müssen vor dem Verkauf sicherstellen, dass das Produkt die CE-Kennzeichnung trägt und dass Hersteller sowie gegebenenfalls Einführer ihren



Pflichten nachgekommen sind und alle erforderlichen Dokumente vorliegen. Bestehen Zweifel an der Konformität, darf das Produkt erst in den Handel gelangen, wenn diese ausgeräumt sind. Stellt sich nachträglich heraus, dass ein Produkt nicht konform ist, müssen Händler Korrekturmaßnahmen ergreifen und mit den Marktüberwachungsbehörden zusammenarbeiten.

SANKTIONEN

Bei Verstößen gegen den CRA drohen empfindliche Sanktionen. Wer Informationspflichten verletzt – etwa durch falsche, unvollständige oder irreführende Angaben gegenüber Behörden oder notifizierten Stellen –, riskiert Bußgelder von bis zu 5 Millionen Euro oder 1 Prozent des weltweiten Jahresumsatzes. Deutlich teurer wird es bei Verstößen gegen die zentralen CRA-Anforderungen, etwa fehlende Sicherheitsmaßnahmen: Hier reicht der Bußgeldrahmen von 10 bis zu 15 Millionen Euro oder 2 bis 2,5 Prozent des weltweiten Jahresumsatzes. Bei der Bemessung berücksichtigen die Behörden die Umstände des Einzelfalls – insbesondere auch die Unternehmensgröße.

Neben Bußgeldern können die Behörden auch einen Produktrückruf anordnen. Betroffene Unternehmen müssen diesen koordinieren und den Kaufpreis erstatten. Zudem können Behörden öffentliche Warnungen zu bestimmten Produkten aussprechen.

FAZIT

Auch wenn bis zur vollständigen Anwendung noch Zeit bleibt: Unternehmen sollten die CRA-Pflichten nicht nach hinten schieben. Es braucht interne Programme, klare Verantwortlichkeiten und belastbare Prozesse. Meldeinfrastruktur, Security by Design und by Default, technische Dokumentation und mögliche Zertifizierungen binden erhebliche Ressourcen. Wer zu spät startet, riskiert nicht nur empfindliche Sanktionen, sondern muss unter Zeitdruck nachrüsten. Deutlich effizienter ist es, die CRA-Anforderungen von Anfang an in Entwicklung, Einkauf und Produktpflege mitzudenken. ■

DR. JAN SCHARFENBERG, LL.M. (STELLENBOSCH)
ist als Rechtsanwalt bei der Kanzlei Schürmann Rosenthal Dreyer im Bereich Datenschutz- und Informationssicherheitsrecht tätig. Zudem arbeitet er als Director für den Bereich Informationssicherheit bei der ISICO Datenschutz GmbH.

www.srd-rechtsanwaelte.de

ABGRENZUNG ZU ANDEREN EU-REGELWERKEN

Der CRA steht nicht allein, sondern reiht sich in eine wachsende Zahl europäischer Regelwerke zur Cybersicherheit und zum Verbraucherschutz ein. Die wichtigsten Abgrenzungen im Überblick:

CRA vs. NIS-2-Richtlinie

Beide Regelwerke zielen darauf ab, die Cyberresilienz in der EU zu stärken – setzen aber an unterschiedlichen Stellen an. Während der CRA konkrete Anforderungen an Produkte mit digitalen Elementen stellt und in erster Linie dem Schutz von Endverbrauchern und Unternehmen dient, richtet sich die NIS-2-Richtlinie an Unternehmen und deren organisatorische Cybersicherheit – branchenübergreifend und unabhängig von einzelnen Produkten. Anders als der CRA, der als EU-Verordnung unmittelbar gilt, erfordert die NIS-2 ein nationales Umsetzungsgesetz. In Deutschland geschieht dies über das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsCG), mit dem die europäischen Vorgaben in nationales Recht überführt werden.

CRA vs. CER-Richtlinie

Die CER-Richtlinie wurde zeitgleich mit der NIS-2-Richtlinie verabschiedet und konzentriert sich auf die physische Widerstandsfähigkeit kritischer Einrichtungen. Sie soll vor allem das Ausfallrisiko von Prozessen mindern und gibt dafür Pflichten zur Risikobewertung, Maßnahmenkataloge und Meldepflichten vor. Die betroffenen Wirtschaftszweige überschneiden sich teilweise mit denen der NIS-2-Richtlinie. Der CRA hingegen adressiert nicht die physische Infrastruktur, sondern die digitale Sicherheit von Produkten.

CRA vs. Digitale-Inhalte-Richtlinie und Warenkauf-Richtlinie

Auch diese beiden Richtlinien schützen Verbraucher – allerdings auf vertragsrechtlicher Ebene. Sie greifen nur, wenn ein Verbrauchervertrag über den entgeltlichen Erwerb digitaler Inhalte oder Dienstleistungen vorliegt. Der CRA hingegen knüpft seine Pflichten an das Inverkehrbringen eines Produkts, unabhängig davon, ob ein konkreter Verbrauchervertrag besteht. Inhaltliche Überschneidungen gibt es dennoch: Sowohl die beiden Richtlinien als auch der CRA sehen etwa eine Aktualisierungspflicht für betroffene Produkte vor.

VORSCHAU Ausgabe 3|26 JUNI/JULI

SCHWERPUNKT: Security Awareness – Der Mensch im Fokus der Cyberabwehr

Technische Schutzmaßnahmen sind unverzichtbar – doch viele erfolgreiche Angriffe beginnen nach wie vor beim Faktor Mensch. Phishing, Social Engineering und zunehmend auch KI-gestützte Deepfakes zeigen, wie gezielt Angreifer menschliche Wahrnehmung und Verhaltensmuster ausnutzen. Gleichzeitig stehen Unternehmen vor der Herausforderung, das Sicherheitsbewusstsein nachhaltig zu verankern, ohne ihre Mitarbeiter zu überfordern oder zu ermüden.

Im kommenden Heft wird beleuchtet, wie moderne Security-Awareness gestaltet sein muss, um wirksam zu sein – praxisnah, messbar und zielgruppengerecht. Im Schwerpunkt erwarten Sie unter anderem folgende Themen:

- **Aktuelle Angriffsvektoren:** Wie Phishing-Kampagnen, Social Engineering und Deepfake-Technologien immer raffinierter werden – und woran sich Angriffe erkennen lassen.
- **Zielgruppenorientierte Awareness-Programme:** Warum One-size-fits-all-Schulungen scheitern und wie sich Inhalte für unterschiedliche Rollen im Unternehmen zuschneiden lassen.
- **Gamification und interaktive Lernformate:** Wie spielerische Ansätze und Simulationen die Aufmerksamkeit erhöhen und nachhaltiges Lernen fördern.
- **Phishing-Simulationen und Tests:** Planung, Durchführung und Auswertung realistischer Angriffsszenarien – zwischen Trainingseffekt und Akzeptanz im Unternehmen.
- **KPIs und Erfolgsmessung:** Welche Kennzahlen wirklich aussagekräftig sind und wie sich der Reifegrad von Awareness-Maßnahmen objektiv bewerten lässt.

Weitere Beiträge in der Ausgabe:

- **Governance von KI-Agenten:** Kontrollmechanismen, Risiken und organisatorische Einbettung autonomer Systeme
- **LLMs in der Malware-Analyse:** Potenziale, Grenzen und neue Werkzeuge für die Sicherheitsforschung

ERSCHEINUNGSTERMIN: 16. Juni 2026

IMPRESSUM

IT-SICHERHEIT
Management und Technik

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

Chefredaktion:
Sebastian Frank (sf)
(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 € 145,– 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)

Titelbild: Chanthakan - stock.adobe.com

Fotos: Firmenbilder; ChatGPT; Deutsche Messe AG; (Carlos Montes, DLV, Gorodenkoff, H. Brauer, hodim, igor.nazlo, kaliel, komwut, Jelena, Quality Stock Arts, TensorSpark, Theyone, WrightStudio) - stock.adobe.com

32. Jahrgang 2026 · ISSN: 1868-5757

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