HZ219246 · ISSN 1868-5757 · www.itsicherheit-online.com Dezember/Januar 6/2025

IT-SICHERHEIT

Management und Technik

Schwerpunkt Identity- und Access-Management

Wege zu schlanken IAM-Strukturen

- **In sieben Schritten zur Zero-Trust-Umgebung**
  So gelingt Unternehmen der strukturierte Umstieg
- **Digitales Onboarding:**
  Warum Banken mehrere Ident-Verfahren brauchen
- **Threat-aware IAM:**
  Risikokontext statt starrer Rollen
- **Identity Governance in KRITIS**
  Berechtigungen benötigen klare Strukturen

Denken in Fallen
Kognitive Verzerrungen beeinflussen Sicherheitsentscheidungen

Cloud-Exit
Wie Unternehmen ihre digitale Souveränität zurückgewinnen

Vom Bauchgefühl zur Methode
Risikomanagement als Brücke zwischen Strategie und Umsetzung

DATAKONTEXT

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

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

Liebe Leserinnen, liebe Leser,

derzeit bewegt sich recht viel beim Thema Identity- und Access-Management (IAM) – und das hat gute Gründe. So bevölkern laut einer Studie des Unternehmens Rubrik nach Branchenberichten 82-mal mehr nicht-menschliche als menschliche Identitäten unsere Systeme, während nur noch 28 Prozent der IT-Verantwortlichen weltweit glauben, sich binnen zwölf Stunden von einem Cybervorfall erholen zu können. Ein Jahr zuvor waren es noch 43 Prozent. 15 Prozentpunkte Vertrauensverlust in nur einem Jahr.

Die Reaktion der Unternehmen zeigt zumindest, dass sie den Ernst der Lage erkannt haben. 89 Prozent weltweit beabsichtigen – laut der Studie –, innerhalb der nächsten zwölf Monate spezialisiertes Personal für Identitätsmanagement einzustellen. Noch bemerkenswerter: 87 Prozent der IT-Verantwortlichen planen einen Wechsel ihres IAM-Anbieters oder haben diesen bereits eingeleitet. Als Hauptgrund geben 58 Prozent der 1.625 weltweit befragten Entscheidungsträger Sicherheitsbedenken an. In Deutschland ist die verbesserte Integration zusätzlich ein Hauptwechselgrund. Die Flucht nach vorn hat also schon begonnen: investieren, umbauen, neu denken.

Dahinter steht die stille Invasion der KI-Agenten. 89 Prozent der Befragten haben KI-Agenten bereits in ihre Identitätsinfrastruktur integriert und beschleunigen damit das Wachstum nicht-menschlicher Identitäten. Gleichzeitig wächst die Sorge vor neuen Bedrohungen: Mehr als die Hälfte der IT-Sicherheitsverantwortlichen schätzt, dass im nächsten Jahr 50 Prozent oder mehr der Cyberangriffe von agentenbasierter KI ausgehen werden.

Vor diesem Hintergrund widmet sich diese Ausgabe der IT-SICHERHEIT dem Schwerpunkt IAM. Unsere Autoren zeigen konkrete Wege auf: Wie Threat-aware IAM aus statischen Rollen dynamische Schutzschilde macht, die Kontext und Risiko in Echtzeit bewerten (Seite 18). Wie Zero Trust in sieben strukturierten Schritten Realität wird, ohne die Produktivität zu opfern (Seite 22). Warum mittelständische Unternehmen mit No-Code-IAM-Plattformen schneller schlankere Strukturen erreichen, als viele denken. Von digitalem Banking-Onboarding (Seite 24) bis hin zur Verwaltung kritischer Infrastrukturen (Seite 26): Im Schwerpunkt dieser Ausgabe geht es um wirksame Schritte, nicht um perfekte Lösungen.

Außerdem beschäftigen wir uns in diesem Heft mit dem Denken selbst. Unser Beitrag über kognitive Verzerrungen in der Cybersicherheit zeigt, wie Bestätigungsfehler, Ankereffekte und der Status-quo-Bias systematisch unsere Sicherheitsentscheidungen sabotieren (Seite 68). Awareness-Kampagnen allein helfen nicht – wir benötigen strukturierte Gegenmaßnahmen gegen die Fallen des eigenen Verstands. Denn was nützt die beste Strategie, wenn wir die falschen Prioritäten setzen?

Das führt zu einer unbequemen Wahrheit: Manchmal ist der beste Schutz der strategische Rückzug. Unser Artikel zu souveränen Cloud-Architekturen zeigt, wie Unternehmen pragmatische Exit-Strategien entwickeln können, ohne in digitale Isolation zu verfallen (Seite 42). Das Risikomanagement nach ISO 31000 wird dabei zur Brücke zwischen strategischen Ambitionen und operativer Realität (Seite 50). Auch hier geht es nicht darum, perfekt zu sein, sondern handlungsfähig zu bleiben, wenn die nächste Welle anrollt.

Viel Freude bei der Lektüre,
Ihr Sebastian Frank

www.itsicherheit-online.com/newsletter

INHALT

14 TITELSTORY
IDENTITY GOVERNANCE IM MITTELSTAND:
WEGE ZU SCHLANKEREN IAM-STRUKTUREN

SECUNET STEIGERT UMSATZ DEUTLICH

Der Cybersecurity-Anbieter Secunet hat in den ersten neun Monaten des Jahres 2025 seinen Konzernumsatz um 11,8 Prozent auf 284,8 Millionen Euro gesteigert. Das Ergebnis vor Zinsen und Steuern (EBIT) kletterte überproportional um 41,3 Prozent auf 24,9 Millionen Euro, wie das Unternehmen mitteilte.

Besonders stark entwickelte sich das Segment Business Sector mit einem Umsatzplus von 39,9 Prozent auf 35,5 Millionen Euro. Das größere Segment Public Sector wuchs um 8,7 Prozent auf 249,3 Millionen Euro. Die länger als erwartete Diskussion über den Bundeshaushalt bremste die Umsatzentwicklung im dritten Quartal temporär aus. Der Vorstand bestätigte den Ausblick für das Gesamtjahr mit einem erwarteten Jahresumsatz von rund 425 Millionen Euro. ■

DISTRIBUTIONSPARTNERSCHAFT FÜR SASE-LÖSUNGEN

Westcon-Comstor hat eine Distributionsvereinbarung mit Cato Networks geschlossen. Die Partnerschaft erschließt Resellerpartnern in den Benelux-Staaten, der DACH-Region, Skandinavien sowie im Nahen Osten und in Afrika den Zugang zur Secure-Access-Service-Edge-(SASE)-Plattform von Cato Networks. Westcon-Comstor wird autorisierter Distributionspartner des KI-Sicherheitsanbieters.

Reseller erhalten damit Zugang zu einer SASE-Komplettlösung, die sich einfach vermarkten und schnell implementieren lässt. Dank einfacher Onboarding-Prozesse macht es die Cato SASE Cloud-Plattform dem Channel leicht, wiederkehrende Umsätze zu generieren, so der Anbieter. Das Channel First Partner-Programm von Cato Networks biete attraktive Spezialisierungspfade und verzichte vollständig auf finanzielle Vorleistungen. Der SASE-Markt soll laut Prognosen von 7 Milliarden US-Dollar (2022) auf 28,5 Milliarden US-Dollar (2028) anwachsen. ■

BEYONDTRUST GRÜNDET FORSCHUNGSLABOR

BeyondTrust hat das Forschungslabor „Phantom Labs" mit Schwerpunkt auf Identitätssicherheit gegründet. Unter der Leitung von CTO Marc Maiffret soll das Labor systematisch neue Bedrohungen aufdecken und innovative Lösungen entwickeln. Maiffret verfügt über eine einzigartige Sicht auf die Motivation und Vorgehensweise von Angreifern und hat bereits große Microsoft-Schwachstellen aufgedeckt.

Als strategische Neueinstellungen konnte BeyondTrust renommierte Experten gewinnen: Kinnaird McQuade als Chief Security Architect, dessen Open-Source-Tool Cloudsplaining mehr als 40 Millionen Mal heruntergeladen wurde, und Fletcher Davis als Leiter von Phantom Labs, einen Spezialisten für Offensive Security und Red-Team-Aktivitäten. Das Ziel der Phantom-Labs-Forscher ist es, „wie ein Hacker zu denken", um durch dauerhafte Bedrohungsanalyse unbekannte Schwachstellen offenzulegen und identitätsorientierte Sicherheitsinnovationen voranzutreiben. ■

NEUER CEO BEI **WATCHGUARD**

WatchGuard Technologies hat Joe Smolarski als neuen CEO berufen. Der ehemalige Kaseya-Manager verfügt über mehr als 25 Jahre Führungserfahrung in Technologie, Operations und Strategie. Bei Kaseya trug er dazu bei, den Umsatz zu verzehnfachen und den Unternehmenswert um mehrere Milliarden Dollar zu steigern, indem er Teams, Technologien und Partner unter einer kundenorientierten Plattformvision vereinte.

Vats Srivatsan, der seit Mai 2025 als Interims-CEO fungierte, bleibt Mitglied des Aufsichtsrats und wird WatchGuard weiterhin in strategischen und wachstumsrelevanten Fragen beratend zur Seite stehen. Smolarski soll den bisherigen Kurs des Cybersecurity-Anbieters fortsetzen und die strategischen Initiativen für operative Exzellenz und globalen Partnererfolg vorantreiben. Alex Slusky, Gründungspartner von Vector Capital und Vorstandsvorsitzender von WatchGuard, hebt Smolarskis nachgewiesene Fähigkeit hervor, Teams und Technologien in großem Maßstab zu integrieren und sich dabei auf den Erfolg der Partner zu konzentrieren. ■

ZSCALER ÜBERNIMMT KI-SICHERHEITSEXPERTEN

Der Cloud-Sicherheitsanbieter Zscaler übernimmt SPLX, einen Pionier der KI-Sicherheit. Die Zscaler Zero Trust Exchange-Plattform wird um Shift-Left KI Asset Discovery, automatisiertes Red Teaming und Governance erweitert. Unternehmen sollen ihre KI-Investitionen von der Entwicklung bis zur Bereitstellung sichern können.

Durch Rekordinvestitionen in die KI-Infrastruktur, die bis Ende 2025 voraussichtlich 250 Milliarden US-Dollar übersteigen werden, sehen sich Unternehmen mit einer wachsenden Angriffsfläche und der Zunahme von Schatten-KI konfrontiert. Sich ständig weiterentwickelnde KI-Modelle, Agenten und Large Language Models (LLM) erfordern eine kontinuierliche Erkennung, Risikobewertung und Behebung von Vorfällen. Die Technologie von SPLX erweitere das Serviceportfolio von Zscaler um eine nativ integrierte Ebene des KI-Schutzes, die über 5.000 speziell entwickelte, domänenspezifische Angriffssimulationen umfasse. ■

OPSWAT ACADEMY WIRD ISC2-PARTNER

Die OPSWAT Academy erhielt von ISC2 die Anerkennung als offizieller Ausbildungspartner. Die Zusammenarbeit ermöglicht es Schulungsteilnehmern, CPE-Punkte (Continuing Professional Education) für ISC2-Zertifizierungen wie CISSP oder CCSP zu sammeln. Je nach abgeschlossenem Kurs können bis zu 20 CPE-Punkte gesammelt werden.

Die Ernennung zum ISC2 CPE Submitter Partner ermöglicht es den Teilnehmern, ihre internationalen Sicherheitszertifikate effizient zu erweitern. Die praxisorientierten Trainings der OPSWAT Academy wie Online-Selbstlernkurse, Live-Webinare und technische Bootcamps werden direkt auf die Anforderungen der weltweit anerkannten ISC2-Security-Zertifikate angerechnet. Dies stärke gezielt die berufliche Entwicklung und fördere den Kompetenzaufbau innerhalb der europäischen Security-Community, so der Schulungsanbieter. ■

CLOUDIAN UND **CTERA** KOOPERIEREN STRATEGISCH

Die Objektspeicher-Spezialisten Cloudian und CTERA haben eine strategische globale Partnerschaft geschlossen. Nutzer profitieren von einem integrierten Ansatz zur Verwaltung ihrer Datenlandschaft vom Edge bis zur Cloud. Die Kombination vereint Cloudians skalierbaren Objektspeicher HyperStore mit CTERAs intelligenter Datenmanagementplattform.

Cloudian-Kunden erhalten Zugriff auf verteilte Unternehmensdatendienste über die CTERA Intelligent Data Platform. CTERA Edge Filer bieten intelligentes Caching mit LAN-Geschwindigkeit für den Zugriff von Edge-Standorten auf zentral gespeicherte Daten. CTERA-Kunden profitieren von Cloudians HyperStore-Plattform, die Exabyte-Skalierbarkeit, staatlich geprüfte Sicherheit und S3-API-Kompatibilität bietet. Die softwaredefinierte Architektur läuft auf Standardhardware und senkt die Gesamtspeicherkosten im Vergleich zu herkömmlichen Systemen um bis zu 70 Prozent. ■

ARCTIC WOLF ERWEITERT ENDPOINT-SCHUTZ

Arctic Wolf gibt die Übernahme von UpSight Security bekannt, um seine Aurora Endpoint Security um KI-gestützte Funktionen zur Ransomware-Prävention und Wiederherstellung zu erweitern. Nach der Integration will das Unternehmen die Technologie von UpSight nutzen, um Aurora mit prädiktiven On-Device-KI-Modellen auszustatten, die kontinuierlich Milliarden von Endpoint-Ereignissen analysieren und schadhaftes Verhalten in Echtzeit vorhersagen.

Die erweiterten Funktionen ermöglichen es Organisationen, Ransomware-Angriffe zu blockieren, bevor Daten verschlüsselt oder exfiltriert werden, kompromittierte Hosts schneller zu isolieren und betroffene Systeme durch Wiederherstellungsmechanismen umgehend zurückzusetzen. Laut dem Arctic Wolf Threat Report 2025 waren 44 Prozent aller Incident-Response-Fälle auf Ransomware oder Datenerpressung zurückzuführen. In 96 Prozent dieser Angriffe exfiltrierten die Täter zusätzlich Daten, um den Druck auf betroffene Unternehmen zu erhöhen. Die Geschwindigkeit und Raffinesse moderner Ransomware-Kampagnen habe die Bedeutung präventiver Security-Initiativen weiter erhöht. ■

ASSA ABLOY KAUFT **KENTIX**

Der schwedische Sicherheitstechnik-Konzern ASSA ABLOY hat die Kentix GmbH aus Idar-Oberstein übernommen. Das Unternehmen mit rund 50 Mitarbeitern entwickelt digitale und Internet-of-Things-(IoT)-Zugangs- sowie Überwachungslösungen für Rechenzentren. Mit der Übernahme stärkt ASSA ABLOY seine Position bei digitalen Sicherheitslösungen für Data Center-Anwendungen.

Die Geschäftsführung von Kentix sieht die Integration als positiven Schritt für nachhaltiges Wachstum. Durch die Integration eröffnen sich neue Märkte und zusätzliche Vertriebsmöglichkeiten innerhalb der globalen ASSA ABLOY Gruppe. Der Standort in Idar-Oberstein bleibt erhalten, für die Mitarbeiter ändere sich nichts. ■

MILLIARDEN-ÜBERNAHME BEI **VEEAM**

Veeam Software übernimmt Securiti AI für 1,725 Milliarden US-Dollar. Die Kombination soll Unternehmen dabei helfen, ihre gesamten Daten für KI zu verstehen, zu schützen und wiederherzustellen. Securiti AI gilt als Marktführer im Bereich Data Security Posture Management (DSPM) und deckt Datenschutz, Governance sowie AI-Trust über hybride Multi-Cloud-Plattformen ab.

Branchenstudien schätzen, dass 80 bis 90 Prozent aller KI-Projekte scheitern, vielfach aufgrund von Datenproblemen wie Genauigkeit, Herkunft und Berechtigungen. Securiti AI ist Pionier des Data Command Center, das von einem einzigartigen Knowledge Graph angetrieben wird und Datenintelligenz mit Sicherheitskontrollen vereint. Nach Abschluss der Transaktion wird Rehan Jalil, CEO von Securiti AI, als President of Security and AI zu Veeam wechseln. Jalil gründete zuvor Elastica, das mit Blue Coat für 280 Millionen US-Dollar fusionierte, bevor Symantec das gemeinsame Unternehmen für 4,7 Milliarden US-Dollar übernahm. ■

SECUREPOINT ÜBERNIMMT WHITELISTING-ANBIETER

Securepoint hat die seculution GmbH aus Werl übernommen. Der erste Zukauf stärkt das IT-Sicherheits-Portfolio im Bereich Endpoint-Security. Seculution setzt seit über 20 Jahren auf Application-Whitelisting basierend auf einem patentierten Automatisierungsverfahren. Nur ausdrücklich autorisierte Programme mit individuellem Hash dürfen auf Endgeräten ausgeführt werden.

Die Technologie gilt als besonders geeignet für Organisationen mit hohen Sicherheits- und Compliance-Anforderungen wie im Gesundheitswesen, der öffentlichen Verwaltung und in kritischen Infrastrukturen. Mit der Übernahme integriert Securepoint die Whitelisting-Technologie in sein bestehendes Portfolio aus Firewalls, VPN-Gateways, Mobile Security, Backup-Lösungen und Awareness-Schulungen. Kunden profitieren damit von einem erweiterten Sicherheitskonzept, das Netzwerke, Daten und Endgeräte in mehreren Ebenen schützt. ■

AIRLOCK WIRD PARTNER DER OPEN TELEKOM CLOUD

Der Schweizer Security-Anbieter Airlock ist neuer Circle Partner der Open Telekom Cloud. Die im November angekündigte Kooperation soll Unternehmen DSGVO-konforme Cloud-Infrastruktur mit integrierten Sicherheitslösungen bieten. Laut Ergon Informatik AG, unter deren Dach Airlock agiert, erhalten Kunden der Open Telekom Cloud künftig Zugang zur Airlock-Plattform für Application Security, API-Schutz sowie Identity- und Access-Management. Die Airlock Web Application Firewall soll Anwendungen vor Cyberangriffen schützen, während das Airlock Microgateway APIs und Microservices absichert. Die Infrastruktur wird vollständig in Europa betrieben und erfüllt Anforderungen wie DSGVO und PCI-DSS. Die native Einbindung in die Telekom-Cloud-Plattform soll laut den Unternehmen Implementierungsaufwand und Betriebskosten reduzieren. ■

DEUTSCHLAND BLEIBT CYBERSICHERHEITSTECHNISCH VERWUNDBAR

Deutschland bleibt trotz Fortschritten bei der Cybersicherheit verwundbar. Das geht aus dem aktuellen Jahresbericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) hervor. Zwischen Juli 2024 und Juni 2025 stieg die Zahl täglich neu entdeckter Schwachstellen um 24 Prozent. Viele digitale Systeme, Server und Onlinedienste sind nach Angaben des BSI weiterhin unzureichend geschützt. Webanwendungen seien besonders häufig schlecht abgesichert, Server oft falsch konfiguriert. Bekannte Sicherheitslücken würden zu spät oder gar nicht behoben.

Bundesinnenminister Alexander Dobrindt kündigte zudem den Aufbau des „Cyberdome" an – ein teilautomatisiertes System zur Detektion und Analyse von Angriffen sowie zur Reaktion darauf. Finanziell motivierte Cyberangriffe gingen im Vergleich zum Vorjahr um neun Prozent zurück, unter anderem aufgrund erfolgreicher internationaler Ermittlungen unter Beteiligung des Bundeskriminalamts (BKA) und des BSI. Ransomware-Gruppen bleiben jedoch die größte Bedrohung. Kleineren Unternehmen und Kommunen fehlen oft Ressourcen und das Bewusstsein für ihre Verwundbarkeit. ■

DEMONSTRATOR FÜR QUANTENSICHERE PERSONALAUSWEISE ENTWICKELT

Die Bundesdruckerei und Giesecke+Devrient haben gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und Infineon einen Demonstrator für quantensichere Personalausweise entwickelt. Die Machbarkeitsstudie ist eine der weltweit ersten funktionalen Umsetzungen eines Personalausweises mit klassischer Kryptografie sowie Post-Quantum-Kryptografie (PQC) und zeigt, wie sich hoheitliche Dokumente mit Post-Quantum-Kryptografie gegen Angriffe von Quantencomputern schützen lassen.

Die Migration erfolgt in zwei Phasen: Zunächst werden Ausweisdaten mit einem quantenresistenten Signaturverfahren gegen Fälschungen geschützt. Anschließend folgt die vollständige Umstellung auf quantensichere Technologie. „Wir müssen jetzt handeln, um unsere digitale Infrastruktur zu schützen", sagt Gabriel von Mitschke-Collande von Giesecke+Devrient. BSI-Präsidentin Claudia Plattner betont die Relevanz: „Wir müssen ab 2030 mit leistungsfähigen Quantencomputern rechnen, die aktuelle kryptografische Verfahren brechen können." Eine EU-Roadmap sieht die Umsetzung für kritische Anwendungsfälle mit hohem Risiko bis 2030 vor. Da Personalausweise zehn Jahre gültig sind, ist die frühe Umsetzung von hybridem PQC wichtig. ■

BACKUP OHNE CLOUD-ANBINDUNG

Acronis hat eine neue Version seiner Cyber-Protection-Plattform vorgestellt, die speziell für lokale und souveräne IT-Umgebungen entwickelt wurde. Acronis Cyber Protect Local kombiniert nach Unternehmensangaben Backup, Datenwiederherstellung, Cybersicherheit und Endpunktverwaltung in einer einzigen Plattform. Die Lösung richtet sich an Unternehmen, für die eine Cloud-Bereitstellung keine Option darstellt. Alle Daten verbleiben dabei innerhalb des Kundennetzwerks, um die Einhaltung gesetzlicher Vorgaben sicherzustellen, so Acronis. Die Software unterstützt sowohl ältere Systeme wie Windows XP als auch moderne Hypervisoren wie VMware, Hyper-V, Nutanix und Proxmox.

Zu den Kernfunktionen gehören eine automatische Erkennung ungeschützter Geräte über Device Sense sowie eine Self-Service-Wiederherstellung. Durch künstliche Intelligenz (KI) gestützte Automatisierung soll zudem die Anomalieerkennung und die Behebung von Vorfällen verbessert werden. Die Lösung ermöglicht ferner plattformübergreifende Wiederherstellungen ohne zusätzliche Agenteninstallationen und erleichtert die reibungslose Migration von Workloads. ■

DATA LAKE REDUZIERT SIEM-KOSTEN

Der Sicherheitsanbieter Bitdefender zeigt mit GravityZone Security Data Lake und Data Lake for Managed Detection and Response (MDR) zwei neue Lösungen, die Sicherheitstelemetriedaten aus verschiedenen Tools auf einer einzigen Plattform zusammenführen. Die Lösungen wandeln in Echtzeit Daten in nutzbare Erkenntnisse um und bieten nach eigenen Angaben die Transparenz und Effizienz eines modernen Security-Information-and-Event-Management-(SIEM)-Systems bei reduzierten Betriebskosten.

Laut der International Data Corporation (IDC) steigen die Kosten für SIEM-Lösungen mit der Menge der erfassten Daten. Der Security Data Lake soll diese Herausforderung durch intelligentes Tiering der Speicherung adressieren. Zu den Hauptvorteilen zählen verbesserte Bedrohungserkennung, zentrale Datenerfassung aus verschiedenen Quellen, vereinfachte Compliance-Funktionen und geringere Speicherkosten. Die Lösungen sind ab sofort als Add-on für zahlreiche GravityZone-Angebote und MDR-Servicestufen erhältlich und integrieren sich nahtlos in die Bitdefender-MDR-Dienste. ■

BACKUP-DATEN IN SICHERHEITS-OPERATIONEN INTEGRIERT

Veeam Software hat die Einführung einer neuen App für Microsoft Sentinel bekannt gegeben. Sie integriert die Veeam Data Platform mit Microsoft Sentinel und ermöglicht Unternehmen, Cyberbedrohungen und Backup-Anomalien zu erkennen, zu untersuchen und darauf zu reagieren.

Da Cyberangriffe zunehmend auf Backup-Umgebungen abzielen, sehen sich Security Operations Center (SOC) mit Transparenzlücken in ihren Sicherheits-Ökosystemen konfrontiert, so der Anbieter. Die Veeam-App schließe diese Lücke durch die Integration von Backup-Informationen direkt in das SOC. Die Lösung nimmt mehr als 300 Veeam-Backup- und Sicherheitsereignisse auf, darunter Job-Ausfälle, verdächtige Aktivitäten und Ransomware-Erkennungen. Diese werden MITRE ATT&CK für eine schnelle Bedrohungserkennung zugeordnet. Integrierte Playbooks und bidirektionale Application-Programming-Interface-(API)-Konnektivität ermöglichen es SOC-Teams, Wiederherstellungen auszulösen und Malware-Scans durchzuführen. Die App ist ohne zusätzliche Kosten für Veeam Data Platform Advanced- und Premium-Kunden über den Microsoft Marketplace erhältlich. ■

IOS- UND ANDROID-VERWALTUNG PER REMOTE-ZUGRIFF

Die Baramundi Management Suite erhält in der Version 2025 R2 umfassende Erweiterungen für das Management mobiler Endgeräte. Das Unified-Endpoint-Management-System kann nun auch iOS- und Android-Geräte per Fernzugriff verwalten. Mit dem neuen Feature Baramundi Remote Desk können IT-Administratoren direkt auf iPhones, iPads und Android-Smartphones zugreifen. Bei iOS-Geräten ist eine Bildschirmfreigabe zur visuellen Unterstützung möglich, Android-Geräte lassen sich vollständig steuern. Die Lösung basiert auf der Technologie von AnyDesk und erfordert die Zustimmung des Nutzers.

Das Linux-Management wurde erweitert. Die neue Version unterstützt zusätzliche Distributionen wie Rocky Linux, Red Hat Enterprise Linux und OpenSuse. Der SSH-Enrollment-Prozess wurde vereinfacht – Sudo-Credentials können nun global hinterlegt werden. Neben der bisherigen Push-Kommunikation ist jetzt auch die Pull-Kommunikation über einen Baramundi-Agenten möglich. Der Vulnerability Scanner erhielt einen neuen Algorithmus, der etwa dreimal schneller arbeitet als die Vorgängerversion. Der Scanprozess läuft mit niedrigerer CPU-Priorität, um andere Anwendungen nicht zu beeinträchtigen. Zusätzlich unterstützt die Software das neuere Open-Vulnerability-and-Assessment-Language (OVAL)-Schema 5.11.2. Weitere Neuerungen umfassen Multi-Tenant-Support für Microsoft Intune, zentrales Job-Management mit Wartungsfenstern und erweiterte PowerShell-Integration. ■

PROMPT SECURITY FÜR VERSCHIEDENE KI-ANWENDUNGEN

SentinelOne hat auf der OneCon 2025 neue Funktionen seiner KI-Plattform präsentiert. Das Portfolio umfasst Lösungen für sichere KI, eine KI-fähige Datenpipeline und Erweiterungen für Purple AI. Das Unternehmen will nach eigenen Angaben Organisationen dabei helfen, KI-Chancen zu nutzen, ohne Sicherheitsrisiken einzugehen.

Das neue KI-Sicherheitsportfolio umfasst drei verfügbare Produkte und eine Beta-Version: Prompt Security für Mitarbeiter überwacht die Generative-Artificial-Intelligence-(GenAI)-Nutzung in Echtzeit und unterstützt über 15.000 KI-Plattformen. Prompt Security für KI-Code-Assistants entfernt automatisch sensible Informationen und personenbezogene Daten aus Code. Eine weitere Variante schützt selbstentwickelte KI-Lösungen vor Angriffen. Noch in der Beta-Phase befindet sich das Produkt Prompt Security für Agentic AI, das autonome KI-Agenten überwacht. ■

PKI-LÖSUNG FÜR AUTONOME KI-SYSTEME

Keyfactor stellt eine neue Funktion vor, die autonome KI-Agenten in Unternehmensumgebungen mit Public-Key-Infrastructure (PKI) absichert. Das Unternehmen nutzt seine Certificate-Lifecycle-Management-(CLM)-Lösungen, um KI-Systemen kryptografische Identitäten zu verleihen. Jeder KI-Agent erhält ein einzigartiges X.509-Zertifikat, wodurch eine überprüfbare, nicht abstreitbare Identität entsteht. OAuth-Token werden an Client-Zertifikate gebunden, die Kommunikation wird durch mutual TLS geschützt. Für containerisierte oder kurzlebige Agenten lässt sich Keyfactor in SPIFFE integrieren, um Zertifikate automatisch zuzuweisen, zu rotieren und zu widerrufen.

„Unternehmen sind bestrebt, KI-Agenten zu skalieren, stehen jedoch vor einer neuen Identitätskrise – einer Krise, in der statische Anmeldedaten wie API-Schlüssel und Client-Geheimnisse einfach keine Verantwortlichkeit oder Sicherheit bieten", erklärt Ellen Boehm, Senior Vice President of IoT and AI Identity Innovation bei Keyfactor. Zertifikatserweiterungen legen fest, auf welche Systeme ein Agent zugreifen kann und welche Operationen erlaubt sind und wann. Der Ansatz erweitert Zero-Trust-Prinzipien auf KI-Umgebungen und ermöglicht nach Angaben des Unternehmens die sichere Skalierung autonomer Agenten ohne Abstriche bei Sicherheit, Compliance oder Aufsicht. ■

OPEN-SOURCE-TOOL FÜR CLOUD-BEDROHUNGSANALYSE ERWEITERT

Auf der KubeCon hat Sysdig neue Open-Source-Funktionen für Falco zur Untersuchung und Analyse von Bedrohungen vorgestellt. Die Updates vertiefen die Integration mit Stratoshark und schaffen einen einheitlichen, durchgängigen Cloud-Security-Workload auf Open-Source-Basis.

Falco, ein Cloud-Native-Computing-Foundation-(CNCF)-Projekt mit über 175 Millionen Downloads, kann nun Security-Content-Automation-Protocol-(SCAP)-Dateien (System Capture) aufzeichnen, wenn bestimmte Regeln ausgelöst werden. Diese Dateien lassen sich nahtlos mit Stratoshark, dem „Wireshark für die Cloud", analysieren. Zudem wurden Verbesserungen an Falco-Plug-ins wie k8saudit und gcpaudit vorgenommen, die Stratoshark helfen, Zusammenhänge in Ereignissen aufzudecken. Die neuen Funktionen ermöglichen einheitliche Workflows, fördern Community-getriebene Innovation und demokratisieren Cloud-Sicherheit durch frei verfügbare Open-Source-Technologien. ■

AUTOMATISIERTE BEDROHUNGS-UNTERSUCHUNG MIT KI

Das Unternehmen Barracuda Networks hat einen KI-basierten Assistenten für seine Cybersicherheitsplattform BarracudaONE vorgestellt. Der Barracuda Assistant soll Sicherheitsprozesse beschleunigen und die Reaktionszeiten auf Cyberbedrohungen verkürzen. Er nutzt nach Herstellerangaben aktuelle Bedrohungsdaten aus Barracudas globalem Informationsnetzwerk. Der Assistent bietet konkrete Handlungsempfehlungen und ermöglicht es Nutzern aller Erfahrungslevel, Cyberbedrohungen schnell zu untersuchen. Dabei sollen zeitaufwendige Kontextwechsel zwischen verschiedenen Sicherheitstools entfallen.

Zudem reduziert er laut Anbieter die für Bedrohungsuntersuchungen notwendige Zeit und minimiert kostspielige Fehler. Er optimiert Arbeitsabläufe und ermöglicht nahtlose Wechsel zwischen Schwachstellenbewertung, Vorfallüberprüfung und anderen Aufgaben. Dadurch können sich Sicherheitsteams wieder auf strategische Prioritäten konzentrieren. Das Tool ist ab sofort über BarracudaONE verfügbar. Künftig soll es auch über Barracuda XDR, Barracuda SecureEdge und das Support-Portal zugänglich sein. ■

Nachbericht

IT-SA 2025 MIT REKORDZAHLEN UND STÄRKERER INTERNATIONALER BETEILIGUNG

Die größte europäische IT-Sicherheitsmesse wächst um über neun Prozent bei Besuchern und über 22 Prozent bei internationaler Beteiligung. Erstmals wurden für die Veranstaltung fünf Messehallen genutzt.

Die it-sa Expo&Congress erreichte mit neuen Bestmarken erneut hohe Resonanz in der Fachwelt. Laut NürnbergMesse besuchten 28.267 Besucher aus 64 Ländern die vom 7. bis 9. Oktober 2025 in Nürnberg abgehaltene Messe – ein Zuwachs gegenüber den 25.830 Teilnehmern aus 65 Ländern im Vorjahr. Die Zahl der ausstellenden Unternehmen stieg von 897 auf 993. „Das Besucherplus und die wachsende internationale Beteiligung zeigen, wie stark der europäische Austausch zur Cybersicherheit geworden ist", so Thimo Holst, Veranstaltungsleiter der it-sa.

EUROPA ZEIGT FLAGGE

Die internationale Bedeutung der Messe zeigte sich an der Beteiligung zentraler Akteure der europäischen Cybersicherheitslandschaft. Neben den etablierten ideellen Trägern – dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bitkom sowie dem Premium-Partner TeleTrusT – war erstmals auch die European Union Agency for Cybersecurity (ENISA) mit einem gemeinsamen Arbeitstreffen in Kooperation mit dem BSI vertreten. Zusätzlich unterstützte die European Cyber Security Organisation (ECSO) die Veranstaltung.

Auch die globale Ausrichtung der it-sa wurde deutlich: Gemeinschaftsstände aus Israel, den Niederlanden, Österreich, Tschechien und dem US-Bundesstaat Virginia bekräftigten den internationalen Charakter der Fachmesse. Wie die NürnbergMesse mitteilte, unterzeichneten die Messegesellschaft und die ECSO während der Veranstaltung eine Absichtserklärung, um ihre Zusammenarbeit zu vertiefen. Eine neue Eventpartnerschaft mit den Swiss Cyber Security Days soll zudem den Austausch zwischen Deutschland und der Schweiz fördern.

Darüber hinaus kündigte BSI-Präsidentin Claudia Plattner am ersten Messetag eine politische Entscheidung von europäischer Tragweite an: Die Bundesregierung hat das BSI gegenüber der Europäischen Kommission als notifizierende und marktüberwachende Behörde zur Umsetzung des Cyber Resilience Act (CRA) benannt.

FREIBURGER START-UP INFRAFON GEWINNT GRÜNDERWETTBEWERB

Neben Politik und Regulierung stand auch die Förderung junger Unternehmen im Mittelpunkt. Beim *ATHENE Startup Award UP25@it-sa* setzte sich Infrafon aus Freiburg durch und erhielt den ersten Preis mit 7.500 Euro. Das Unternehmen überzeugte mit kreditkartengroßen Smart-Badges für Krankenhäuser und andere regulierte Umgebungen. Die Geräte kombinieren Ausweisfunktionen mit Zugangs- und Zugriffskontrolle, verfügen über E-Paper-Touchscreens und unterstützen Messaging sowie Ortung via WLAN, BLE oder LoRa.

Den zweiten Platz belegte Onekey aus Düsseldorf (5.000 Euro). Die Plattform des Unternehmens automatisiert Sicherheitsanalysen von Firmware und prüft vernetzte Geräte auf Schwachstellen und Compliance-Probleme – von der Produktion bis zum laufenden Betrieb. Nenna.ai aus Berlin erreichte den dritten Platz (2.500 Euro) mit einer Privacy-Infrastruktur, die beim Einsatz generativer KI personenbezogene und vertrauliche Daten erkennt, anonymisiert und so die Rechtskonformität wahrt.

Weitere Finalisten waren Devity aus Paderborn mit einer Lösung zur automatisierten Identitätsverwaltung für IoT-Geräte sowie AlpenShield aus Wien, das Unternehmen den Aufbau eigener Security Operation Center auf Basis von Microsoft Sentinel erleichtert.

◀ *Die Messehallen waren gut besucht und zeigten das große Interesse an IT-Sicherheitslösungen. (Bild: NürnbergMesse/Thomas Geiger)*

Auch auf der it-sa sind scharfe Augen gefragt, um Sicherheitslücken zu entdecken. (Bild: NürnbergMesse/Frank Boxler) ▶

Dr. Jean-Marc Rickli sprach als Keynote-Speaker auf der it-sa über die Herausforderungen globaler und aufkommender Sicherheitsrisiken. (Bild: NürnbergMesse/Frank Boxler) ▼

Ausstellungsstück Kill Switch: Ein Knopfdruck und die Welt pausiert. (Bild: NürnbergMesse/Frank Boxler)

Der Live-Pitch fand am 8. Oktober auf der Messebühne der *it-sa Expo & Congress* statt. Eine unabhängige Fachjury bewertete die Präsentationen der fünf Finalisten. Laut Veranstalter zeigt der Wettbewerb, wie vielfältig die Ansätze junger Unternehmen zur Stärkung der Cybersicherheit sind – von Hard- und Software-Schutz über Cloud- und IoT-Security bis hin zu KI-gestützten Datenschutzlösungen.

CONGRESS@IT-SA MIT ÜBER 70 FACHSESSIONS

Das begleitende Kongressprogramm *Congress @it-sa* umfasste mehr als 70 Sessions und Workshops zu aktuellen Herausforderungen der Informationssicherheit. Schwerpunkte bildeten die Jahrestagung der IT-Sicherheitsbeauftragten in Ländern und Kommunen sowie Beiträge zu Governance, Risikomanagement und Compliance.

Das Rahmenprogramm umfasste über 400 Forenbeiträge auf sechs offenen Bühnen. Laut NürnbergMesse wurden unter anderem die *it-sa insights* mit Panels zu Karrierechancen für Frauen in der IT-Sicherheit und das neue Format CIO Match hervorgehoben, das Führungskräfte mit Anbietern zusammenbrachte. Besonders gefragt waren Sessions zu KI-Sicherheit, Cloud-Security und zur praktischen Umsetzung von Zero-Trust-Konzepten. Auch Themen wie NIS-2, DORA und der CRA prägten viele Diskussionen.

Die Finalisten des ATHENE Startup Award UP25@it-sa präsentierten ihre Sicherheitslösungen auf dem Forum. (Bild: NürnbergMesse/Frank Boxler)

DIGITALE PLATTFORM ERREICHT ÜBER 16.000 NUTZER

Die ganzjährige Digitalplattform *it-sa 365* verzeichnete laut Veranstalter über 16.350 registrierte Nutzer – ein Hinweis auf das wachsende Interesse an hybriden Messeformaten, so der Veranstalter. Sie unterstützte Besucher vor Ort mit einem Digital Guide, der Hallenplan-, Aussteller- und Produktsuche sowie Matchmaking-Funktionen kombinierte, und stellt zentrale Inhalte auch online bereit.

Zahlreiche Forenbeiträge wurden live übertragen; aus dem *it-sa@home-Studio* in Messehalle 7 gingen Experteninterviews direkt online. Das hybride Format ermöglichte es Interessierten, auch ohne persönliche Teilnahme in Nürnberg zentrale Inhalte zu verfolgen. Nach der Messe bleiben die Beiträge auf der Digitalplattform kostenfrei abrufbar (www.itsa365.de/de-de).

BRANCHENTRENDS UND TECHNOLOGIESCHWERPUNKTE

Die Ausstellerstruktur der it-sa 2025 spiegelte zentrale Entwicklungen der Cybersecurity-Branche wider. Besonders stark vertreten waren Lösungen für Cloud-Security, Identity- und Access-Management (IAM) sowie KI-gestützte Sicherheitstools. Auch das Thema OT-Security gewann angesichts zunehmender Angriffe auf industrielle Infrastrukturen an Bedeutung.

Zahlreiche Anbieter präsentierten Lösungen zur Umsetzung neuer EU-Regularien wie NIS-2 und DORA. Deren praktische Implementierung beschäftigt Unternehmen verschiedenster Branchen und erhöht die Nachfrage nach spezialisierten Compliance-Tools. Parallel gewinnen Zero-Trust-Architekturen als Antwort auf hybride Arbeitsmodelle und komplexe IT-Landschaften an Relevanz.

Die nächste *it-sa Expo&Congress* findet vom 27. bis zum 29. Oktober 2026 im Messezentrum Nürnberg statt. ■ ***(SF)***

ENISA THREAT LANDSCAPE 2025

DAS ENDE KLARER FRONTEN

Die Grenzen verschwimmen: Cyberkriminelle nutzen Spionage-Taktiken, Staatshacker setzen Ransomware ein und Hacktivisten monetarisieren ihre Angriffe. Die europäische Bedrohungslandschaft 2025 ist von einer Konvergenz der Akteure geprägt, die traditionelle Verteidigungsstrategien stark herausfordern.

Der aktuelle ENISA Threat Landscape Report 2025 dokumentiert einen fundamentalen Wandel. Zwischen Juli 2024 und Juni 2025 analysierte die EU-Agentur für Cybersicherheit knapp 4.900 Vorfälle. Die zentrale Erkenntnis: Die Ära einzelner, hochimpaktiger Angriffe ist vorbei. An ihre Stelle treten kontinuierliche, diversifizierte Kampagnen, die systematisch an der Resilienz von Organisationen zehren. Für Unternehmen bedeute dies eine grundlegende Neuausrichtung der Verteidigung.

PHISHING WIRD ZUR INDUSTRIE

Der Einstieg gelingt Angreifern am häufigsten über Social Engineering. Phishing war mit etwa 60 Prozent der häufigste initiale Angriffsvektor – doch die Methoden haben sich radikal professionalisiert. Phishing-as-a-Service-Plattformen industrialisieren den Prozess und senken die Einstiegshürden erheblich. Die Plattform Darcula imitierte zum Beispiel mehr als 200 Organisationen und erreichte Opfer in über hundert Ländern. Lucid erweiterte das Portfolio um mobile Messaging-Dienste wie iMessage und RCS und traf 169 Ziele in 88 Ländern.

Besonders perfide ist die ClickFix-Technik: Gefälschte CAPTCHA-Prompts auf kompromittierten Websites verleiten Nutzer dazu, PowerShell-Befehle auszuführen – getarnt als Sicherheitsüberprüfung. Über diese Methode verbreitete die ClearFake-Kampagne Infostealer wie Lumma und Vidar und verursachte rund 9.300 bestätigte Infektionen.

Parallel dazu nutzen Angreifer vermehrt künstliche Intelligenz (KI). Zwischen September 2024 und Februar 2025 verwendeten über 80 Prozent aller identifizierten Phishing-E-Mails KI-Unterstützung. Large Language Models erstellen überzeugendere Texte, während Deepfake-Videos und KI-gestütztes Voice-Cloning bei Vishing-Angriffen zum Einsatz kommen. Im Februar 2024 führte beispielsweise ein Deepfake-Video-Call zur Überweisung von mehreren Millionen Dollar in Hongkong.

DIE LIEFERKETTE ALS STRATEGISCHES ZIEL

Wo direkter Zugriff schwierig wird, wählen Angreifer zunehmend den Umweg über die Lieferkette. Die Kompromittierung von Drittanbietern entwickelte sich 2024/25 zu einer bevorzugten Strategie, so der ENISA-Report: Einen IT-Dienstleister zu kompromittieren, ist oft effizienter als hunderte Einzelziele anzugreifen.

Auch Entwicklungsumgebungen und Open-Source-Ökosysteme geraten verstärkt in den Fokus. Nordkorea-nahe Lazarus-Gruppen platzierten manipulierte Node Package Manager-Pakete in GitHub-Repositories, die legitime Bibliotheken imitierten. Ende 2024 kam es zu einer Welle von Angriffen auf Browser-Erweiterungen. Mehrere Chrome-Extensions für KI-Anwendungen und VPN-Dienste wurden kompromittiert.

Zudem entstehen jenseits kommerzieller Tools spezialisierte bösartige KI-Systeme: Nach WormGPT, EscapeGPT und FraudGPT tauchte Anfang 2025 Xanthorox AI auf – mutmaßlich ein lokal betriebenes System, das Erkennung umgeht. Die KI-Lieferkette selbst wird zum Angriffsvektor: Vergiftete Machine-Learning-Modelle und trojanisierte Python-Pakete dienen der Malware-Verbreitung. Ein neuer Vektor, die „Rules-File-Backdoor", ermöglicht die Injektion bösartiger Instruktionen in Konfigurationsdateien von KI-Coding-Assistenten wie Cursor und GitHub Copilot.

MOBILE GERÄTE UNTER DAUERBESCHUSS

2024/25 standen auch Android-Geräte massiv unter Beschuss. So zielte die Rafel-RAT-Kampagne vor allem auf veraltete Geräte in mehreren EU-Ländern. Varianten des Medusa-Banking-Trojans weiteten ihre Aktivitäten nach Frankreich und Italien aus und konzentrierten sich immer mehr auf On-Device-Fraud durch Account-Takeover. Die BingoMod-RAT ging noch einen Schritt weiter: Berichten zufolge räumte die Malware Bankkonten aus und löschte anschließend die kompromittierten Geräte.

Ebenso brisant ist die staatliche Nutzung mobiler Überwachung. Das legale Überwachungsprogramm EagleMsgSpy wird nachweislich von chinesischen Stellen seit mindestens 2017 eingesetzt. Im Februar 2025 meldeten Sicherheitsanbieter gezielte Angriffe russischer Gruppen auf WhatsApp-, Signal- und Telegram-Accounts in der Ukraine; Sandworm soll dabei Signal-Accounts von auf dem Schlachtfeld geborgenen Geräten mit eigener Infrastruktur verknüpft haben. Ein Bericht von iVerify legt nahe, dass staatlich verbundene Telekom-Anbieter veraltete Signalisierungsprotokolle ausnutzen, um mobile Kommunikation grenzüberschreitend zu überwachen — und das ohne direkten Zugriff auf das Zielgerät.

WENN GRENZEN VERSCHWIMMEN: DIE KONVERGENZ DER AKTEURE

Die klassischen Trennlinien zwischen Cybercrime, staatlich unterstützten Operationen und Hacktivismus verschwimmen zunehmend, wie der aktuelle ENISA-Report festhält. Diese Konvergenz gilt als prägendes Merkmal der heutigen Bedrohungslandschaft. Staatliche Akteure greifen dabei auf kriminelle Infrastruktur zurück: APT29 und Sandworm wurden etwa beim Einsatz kommerzieller Residential-Proxy-Netzwerke beobachtet. Die nordkoreanische Gruppe Andariel agierte zeitweise als Affiliate der Play-Ransomware, während Moonstone Sleet auf die Qilin-Ransomware zurückgriff.

Umgekehrt adaptieren Cyberkriminelle staatliche Methoden. FIN6 setzte etwa auf gefälschte Stellenanzeigen und fingierte LinkedIn-Profile – eine Taktik, die auch nordkoreanische Gruppen nutzen. Zugleich monetarisieren vormals ideologisch motivierte Akteure ihre Angriffe: Gruppen wie FunkSec, CyberVolk und KillSec bieten inzwischen eigene Ransomware-as-a-Service-Plattformen an. Diese Verschmelzung staatlicher, krimineller und hacktivistischer Methoden macht Attribution und Abwehr deutlich schwieriger.

Ransomware bleibt eine der dominierenden Angriffsformen gegen EU-Organisationen – auch wenn hacktivistische Kampagnen im Berichtszeitraum rund 80 Prozent der gemeldeten Vorfälle ausmachten. Das Ökosystem ist jedoch zunehmend fragmentiert. Während LockBit im Vorjahr noch ein Viertel aller Angriffe verantwortete, brach die Dominanz der Gruppe nach der Strafverfolgungsoperation Cronos im Februar 2024 ein. An ihre Stelle traten über 80 verschiedene Varianten. Angeführt wurde das Feld von Akira (11,6 %), SafePay (10,1 %) und Qilin (7,5 %).

Die Professionalisierung zeigt sich auch in neuen Erpressungstaktiken. Fog und Qilin nutzen Countdown-Timer und „Call-Lawyer"-Funktionen, die rechtliche Schritte simulieren und zusätzlichen Druck erzeugen – besonders in der EU, wo Meldepflichten und Datenschutzvorgaben die Lage der Betroffenen verschärfen. Technisch rüsten die Gruppen mit EDR-Kill-Tools auf: FIN7 bewarb AvNeutralizer an mehrere Ransomware-Akteure, während RansomHub mit EDRKillShifter und TDSSKiller gezielt Endpoint-Schutzmechanismen ausschaltete.

Infostealer bilden weiterhin ein zentrales Glied der kriminellen Lieferkette. Nach der Zerschlagung von RedLine und META im Oktober 2024 stieg der Einsatz von Lumma Stealer um mehr als 350 Prozent. Zwischen März und Mai 2025 wurden weltweit rund 394.000 Windows-Systeme infiziert – mit auffällig hoher Aktivität in der EU.

STAATLICHE SPIONAGE UND IDEOLOGISCHE STÖRUNGEN

Staatlich gestützte Operationen machten zwar nur 7,2 Prozent aller dokumentierten Vorfälle aus, ihr strategischer Impact war jedoch erheblich. Insgesamt waren 46 Intrusion Sets in der EU aktiv. Russische Gruppen wie APT29, APT28 und Sandworm konzentrierten sich auf öffentliche Verwaltung, Verteidigung und digitale Infrastruktur in Polen, Frankreich, Deutschland, Belgien und Griechenland.

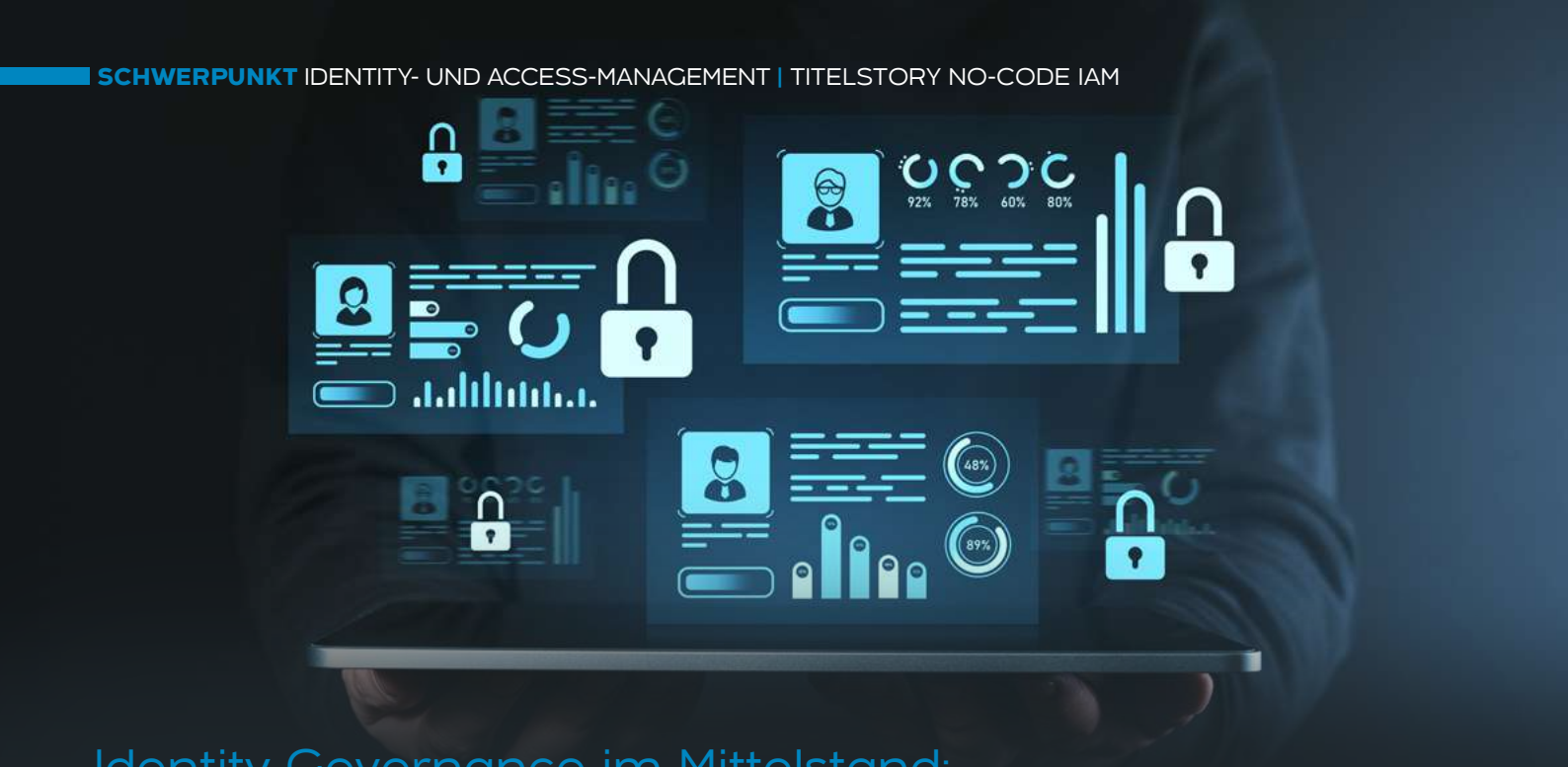
Auch chinesische Gruppen – darunter UNC5221, Mustang Panda, APT41 und Salt Typhoon – waren aktiv und richteten ihre Angriffe auf Transportsektor, Zivilgesellschaft und digitale Infrastruktur in Italien, Deutschland, Frankreich und Belgien. UNC5221 kompromittierte Edge-Geräte, um sogenannte Operational Relay Boxes zu betreiben. Salt Typhoon nahm gezielt Telekommunikationsinfrastrukturen ins Visier und war seit Dezember 2024 in mindestens drei EU-Mitgliedstaaten aktiv. Nordkoreanische Gruppen wie Famous Chollima und Lazarus fielen besonders durch IT-Worker-Kampagnen auf, bei denen sich Agenten als Freelancer in EU-Unternehmen einschleusten.

Auch Foreign Information Manipulation and Interference (FIMI) blieb eine kontinuierliche Bedrohung – besonders im Umfeld von Wahlen. Der Europäische Auswärtige Dienst (EEAS) dokumentierte 86 FIMI-Operationen. Russlandnahe Akteure wie Doppelgänger, Matryoshka und Storm-1516 zielten vor allem auf Frankreich, Deutschland und Polen. Matryoshka nutzte KI-gestütztes Voice Cloning, um Videos zu erzeugen, die EU-Institutionen imitierten und gezielt Desinformationen verbreiteten.

AUSBLICK: DIE NEUE NORMALITÄT

Die Bedrohungslandschaft 2025 war laut ENISA geprägt von Konvergenz, Automatisierung und Industrialisierung. Künstliche Intelligenz beschleunigt die Angriffsinnovation, während digitale Abhängigkeiten vermehrt als strategisches Ziel missbraucht werden. Mit dem Cyber Resilience Act schafft die EU verbindliche Sicherheitsanforderungen, der Cyber Solidarity Act stärkt die grenzüberschreitende Incident Response. Einzeln gesetzte Maßnahmen greifen jedoch zu kurz. Wirksamer Schutz erfordere einen ganzheitlichen, nachrichtendienstlich gestützten Ansatz. Verteidigung müsse proaktiv, adaptiv und kollaborativ erfolgen – über Organisations- und Ländergrenzen hinweg. ■ ***(SF)***

Der „ENISA THREAT LANDSCAPE 2025"-Report ist kostenlos als PDF verfügbar.



Identity Governance im Mittelstand:

WEGE ZU SCHLANKEREN IAM-STRUKTUREN

Während Unternehmen Millionen in Firewalls und Verschlüsselung investieren, entstehen die größten Sicherheitsrisiken dort, wo digitale Identitäten unkontrolliert wachsen. No-Code-Ansätze bieten einen pragmatischen Weg, die Verwaltung digitaler Identitäten zu vereinfachen.

Teure Firewalls, ausgefeilte Verschlüsselung, moderne Endpoint-Security – all diese Investitionen haben eine gemeinsame Schwachstelle: den Menschen und seine digitalen Identitäten. In vielen Organisationen liegt das Problem nicht beim Log-in-Prozess, sondern bei dem, was danach kommt: unklare Verantwortlichkeiten, zu weitreichende Zugriffsrechte und veraltete Accounts, die niemand deaktiviert.

Der *„Identity Theft Resource Center (ITRC) Data Breach Report 2024"* zeigt die Dimension des Problems: Fünf sogenannte Mega-Breaches waren laut ITRC für über 83 Prozent aller Opfermeldungen weltweit verantwortlich.[1,2] Vier davon hätten sich mit grundlegenden Maßnahmen im Identitäts- und Berechtigungsmanagement verhindern lassen. Insgesamt meldeten die USA im Jahr 2024 über 3.158 Datenschutzverletzungen mit rund 1,35 Milliarden Betroffenen. Als Mega-Breaches gelten laut ITRC Vorfälle, bei denen mindestens 100 Millionen Personen betroffen sind. Gestohlene Zugangsdaten werden auf kriminellen Marktplätzen im Durchschnitt für etwa zehn US-Dollar angeboten, wie Spacelift Password Statistics 2025 dokumentiert.[3]

REGULATORISCHER DRUCK STEIGT MASSIV

Für europäische Unternehmen verschärft sich die Lage zudem durch regulatorische Anforderungen. Die „DLA Piper GDPR Fines and Data Breach Survey 2024" dokumentiert Bußgelder in Höhe von 1,2 Milliarden Euro europaweit im Jahr 2024.[4] Seit Einführung der Datenschutz-Grundverordnung (DSGVO) summieren sich die Strafen laut der Erhebung auf insgesamt 5,88 Milliarden Euro. In Deutschland beliefen sich die kumulierten Strafzahlungen auf 89,1 Millionen Euro. Die Zahlen zeigen, dass grundlegende Schutzmaßnahmen wie Multi-Faktor-Authentifizierung in vielen Fällen fehlen und ein effektives Identitätsmanagement ein zentraler Präventionsfaktor ist.

Mit der NIS-2-Richtlinie, die nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Fraunhofer IESE etwa 29.000 bis 29.500 deutsche Unternehmen betrifft, stehen mittelständische Firmen vor neuen Anforderungen an das Identity- und Access-Management (IAM).[5] Für viele Unternehmen bedeutet dies, dass sie erstmals verbindliche IAM- und

IGA-Prozesse einführen müssen, um Bußgelder und Haftungsrisiken zu vermeiden.

18 MONATE BIS ZUM GO-LIVE

Diese verschärften Vorgaben treffen auf eine IAM-Praxis, die in vielen Unternehmen noch von aufwendigen, klassischen Projekten geprägt ist. Die meisten IAM-Systeme wurden für eine andere IT-Welt konzipiert: zentralisierte Rechenzentren, klar definierte Netzwerkgrenzen, überschaubare Anwendungslandschaften. Doch die heutige Realität sieht anders aus: Hybride Cloud-Infrastrukturen, Software-as-a-Service-Anwendungen, mobile Endgeräte und externe Dienstleister haben die IT-Landschaft grundlegend verändert.

Die Folge: Jede Systemintegration wird zum eigenständigen Projekt mit individueller Entwicklungsarbeit. SAP-Anbindungen, Active-Directory-Integrationen, HR-Systeme oder Cloud-Services – alles erfordert maßgeschneiderte Schnittstellen. Branchenanalysen zeigen, dass IAM-Einführungen im Mittelstand oft zwischen 12 und 18 Monaten dauern.[7]

VON ACCESS-MANAGEMENT ZU IDENTITY-GOVERNANCE

Diese Situation macht deutlich, dass klassische Implementierungsansätze an ihre Grenzen stoßen. Hier setzt Identity Governance and Administration (IGA) an – als konzeptioneller Rahmen für eine nachvollziehbare und regelbasierte Zugriffsverwaltung. Während das traditionelle Identity- und Access-Management vor allem die Bereitstellung und Kontrolle von Zugriffsrechten abbildet, rückt IGA den gesamten Lebenszyklus dieser Rechte in den Fokus – von der Vergabe über die Überprüfung bis zur Entziehung. Ziel ist eine nachvollziehbare, regelbasierte und revisionssichere Steuerung sämtlicher Identitäten und Berechtigungen im Unternehmen.

Kern einer effektiven Identity Governance ist die rollenbasierte Zugriffskontrolle. Sie ersetzt manuelle Rechtevergaben durch standardisierte Rollenmodelle, wodurch sich Berechtigungen konsistent und fehlerarm verwalten lassen. Ergänzend sorgt das Prinzip der Funktionstrennung (Separation of Duties) dafür, dass kritische Berechtigungskombinationen ausgeschlossen bleiben – etwa wenn ein Mitarbeiter gleichzeitig Bestellungen freigeben und Wareneingänge prüfen könnte.

Ebenso zentral ist die kontinuierliche Überprüfung und Rezertifizierung von Zugriffsrechten. Automatisierte Prozesse prüfen in regelmäßigen Intervallen, ob Berechtigungen noch erforderlich und angemessen sind. Änderungen im Beschäftigungsstatus – Onboarding, Rollenwechsel oder Offboarding – werden damit automatisch in der Rechteverwaltung nachvollzogen. Die lückenlose Protokollierung aller identitätsbezogenen Aktivitäten schafft zudem Transparenz und Nachweisfähigkeit gegenüber Aufsichtsbehörden und interner Revision.

Diese Governance-Funktionen sind längst kein „Nice-to-have" mehr, sondern regulatorische Notwendigkeit. Artikel 32 der Datenschutz-Grundverordnung (DSGVO) fordert „angemessene technische und organisatorische Maßnahmen", um ein dem Risiko entsprechendes Schutzniveau sicherzustellen. Die NIS-2-Richtlinie geht noch weiter: Sie verlangt explizit Verfahren zur Zugriffskontrolle, Multi-Faktor-Authentifizierung sowie zur kontinuierlichen Überwachung und Protokollierung.[6]

KLICKEN STATT CODEN

Damit steigt der Druck, Identity-Management-Prozesse effizienter und zugleich revisionssicher umzusetzen. No-Code-Plattformen bieten dafür einen pragmatischen Ansatz.

Sie setzen auf vorgefertigte Workflows und intelligente Automatisierung. Anstatt für jede Systemanbindung individuellen Code zu entwickeln, nutzen Unternehmen standardisierte Konnektoren und Templates. IT-Administratoren können so Geschäftsprozesse definieren und anpassen, ohne selbst programmieren zu müssen.

Der Unterschied zeigt sich in der Praxis: Während klassische IAM-Projekte oft monatelange Entwicklungszyklen für die Integration von Unternehmensanwendungen einplanen müssen, verkürzen No-Code-Plattformen diese Phase erheblich. Statt spezialisierter Entwicklungsteams können IT-Administratoren die Systeme eigenständig einrichten und konfigurieren. Der Vorteil liegt nicht nur in der beschleunigten Erstimplementierung, auch spätere Anpassungen – etwa bei Organisationsänderungen oder neuen Geschäftsprozessen – lassen sich durch Konfiguration statt durch Entwicklung umsetzen.

Moderne No-Code-IAM-Plattformen basieren auf ereignisgesteuerten Architekturen, die automatisch auf Änderungen in verbundenen Quellsystemen reagieren. Wird ein neuer Mitarbeiter im HR-System angelegt, triggert dies automatisch den Onboarding-Workflow. Austrittsdaten aktivieren systematische Deprovisioning-Prozesse über alle Systeme hinweg. Vorkonfigurierte Konnektoren für gängige Anwendungen – etwa Active Directory, Microsoft Entra ID, SAP oder Salesforce – funktionieren „out of the box" und werden vom Hersteller bei Systemupdates aktualisiert.

Self-Service-Portale ermöglichen es Mitarbeitern, benötigte Zugriffsrechte selbst zu beantragen. Das System prüft automatisch gegen Rollenmodelle und Funktionstrennung, leitet an die richtigen Genehmiger weiter und dokumentiert alle Schritte lückenlos. Automatisierte Compliance-Funktionen führen kontinuierlich Überprüfungen durch und melden oder korrigieren proaktiv verwaiste Accounts, Berechtigungsanhäufungen oder Policy-Verstöße.

WAS EINE DATENPANNE WIRKLICH KOSTET

Die wirtschaftlichen Auswirkungen von No-Code-IAM-Systemen zeigen sich in mehreren Dimensionen. Bei den Projektkosten und der Implementierungsdauer ergibt sich eine deutliche Reduktion gegenüber klassischen Ansätzen. Was bei traditionellen IAM-Projekten erhebliche Budgets über mehrere Jahre bindet, lässt sich mit No-Code-Lösungen deutlich ressourcenschonender umsetzen. Auch die laufenden Betriebskosten sind niedriger, da sich Updates standardisiert einspielen lassen und die Abhängigkeit von Wartungsverträgen sinkt.

Neben der Kosteneffizienz wirkt sich auch der Automatisierungsgrad unmittelbar auf das Sicherheitsniveau aus. Laut dem IBM Cost of a Data Breach Report 2024 lagen die durchschnittlichen Kosten einer Datenpanne zuletzt bei 4,88 Millionen US-Dollar – ein Anstieg um zehn Prozent gegenüber dem Vorjahr.[1] Unternehmen, die Prozesse im Identity- und Access-Management automatisiert haben, verzeichneten dabei signifikant geringere Schadenssummen.

Zudem sanktionieren Datenschutzbehörden technische und organisatorische Defizite zunehmend konsequent – besonders mangelhafte Zugriffskontrollen und fehlende Löschkon-

zepte zählen zu den häufigsten Verstößen.[4] Mit der NIS-2-Richtlinie werden ab 2025 rund 29.500 Unternehmen in Deutschland verpflichtet, verbindliche Vorgaben für Zugriffskontrollrichtlinien, Multi-Faktor-Authentifizierung und kontinuierliche Überwachung umzusetzen. Für mittelständische Organisationen ohne etabliertes IAM sind diese Anforderungen kaum zu erfüllen – umso wichtiger wird der Einsatz skalierbarer, automatisierter Lösungen.[6]

WO NO-CODE AN SEINE GRENZEN STÖßT

Ein No-Code-IAM eignet sich besonders für standardisierbare Prozesse und typische IAM-Anforderungen. Schätzungen gehen davon aus, dass 90 bis 95 Prozent der üblichen IAM-Anforderungen mittelständischer Unternehmen ohne Programmierung umsetzbar sind.

Komplexe, stark verästelte Berechtigungsmodelle oder proprietäre Systeme mit fehlenden Schnittstellen bleiben jedoch eine Herausforderung. In solchen Fällen kommen hybride Ansätze zum Einsatz: Standardfunktionen werden über No-Code realisiert, Spezialfälle gezielt durch Entwicklung ergänzt. Viele Plattformen bieten hierfür modulare Erweiterungen oder API-basierte Konnektoren, um auch ältere Systeme einzubinden.

No-Code reduziert den technischen Aufwand, ersetzt aber keine konzeptionelle Vorarbeit. Die Definition von Rollenmodellen, die Analyse von Geschäftsprozessen und die Festlegung von Verantwortlichkeiten bleiben jedoch erforderlich. Das größte Risiko liegt daher weniger in der Technologie selbst, sondern in unklaren Zuständigkeiten und unzureichend dokumentierten Prozessen.

In der Praxis folgen Implementierungen häufig einem phasenweisen Vorgehen. Sie beginnen mit der Identifikation von Prozessen mit hohem manuellen Aufwand, gehen über die Pilotierung mit definierten Benutzerkreisen und die sukzessive Erweiterung auf weitere Systeme bis hin zur Aktivierung von Governance-Funktionen wie Access-Reviews und Funktionstrennung.

KI UND ZERO TRUST ALS ZUKUNFTSTRENDS

Mehrere Entwicklungen werden die Identity Governance in den kommenden Jahren prägen. Künstliche Intelligenz hält zunehmend Einzug in das Berechtigungsmanagement: KI-gestützte Systeme analysieren Zugriffsverhalten, erkennen Anomalien und liefern Hinweise auf kompromittierte Accounts. Sie schlagen automatisch optimierte Rollenmodelle vor oder identifizieren überflüssige Berechtigungen – ein wichtiger Schritt hin zu adaptiven, risikobasierten Zugriffsentscheidungen.

Gleichzeitig etabliert sich die Zero-Trust-Architektur als Leitprinzip moderner Sicherheitsstrategien. Ihr Grundsatz „Never trust, always verify" verschiebt den Fokus weg von Netzwerkgrenzen hin zu Identitäten und Kontexten. Zugriffe werden kontinuierlich überprüft, authentifiziert und anhand von Faktoren wie Standort, Gerätetyp oder Nutzerverhalten bewertet.[8] Damit wird die digitale Identität zum zentralen Kontrollpunkt der Sicherheitsarchitektur.

Ein weiteres Handlungsfeld betrifft nichtmenschliche Identitäten. Service-Accounts, API-Keys und Machine Identities gewinnen in automatisierten IT-Umgebungen rasant an Bedeutung – und müssen denselben Governance-Regeln unterliegen wie Benutzerkonten.

Parallel schreitet der Übergang zu passwortlosen Verfahren voran. Passkeys, biometrische Authentifizierung und FIDO2-Standards entwickeln sich zum neuen Standard und markieren den Abschied vom klassischen Passwort – hin zu einer sichereren und zugleich nutzerfreundlicheren Authentifizierungskultur.

FAZIT

Die Bedrohungslage hat sich verschoben, denn digitale Identitäten sind heute das bevorzugte Angriffsziel – und zugleich der zentrale Hebel für Resilienz und Compliance. Mit der Verschärfung regulatorischer Anforderungen durch die DSGVO und NIS-2 ist nicht mehr die Frage, ob, sondern wie Unternehmen Identity Governance umsetzen.

No-Code-Ansätze bieten dafür einen pragmatischen und wirtschaftlich tragfähigen Weg. Sie verkürzen Implementierungszeiten, senken Kosten und erleichtern die Einhaltung regulatorischer Vorgaben. Zugleich schaffen sie die Grundlage für ein automatisiertes, transparentes Berechtigungsmanagement.

Die Technologie ist längst verfügbar und in der Praxis erprobt. Was vielerorts noch fehlt, ist die Entscheidung, den ersten Schritt zu tun. No-Code IAM ermöglicht einen risikoarmen Einstieg in moderne Identity Governance – mit überschaubarem Aufwand und spürbarem Sicherheitsgewinn. ■

Literatur

[1] *IBM Security, Cost of a Data Breach Report 2024, August 2024, www.northdoor.co.uk/about-us/resources/ibm-cost-of-a-data-breach-report-2024/*

[2] *Identity Theft Resource Center (ITRC), 2024 Data Breach Report, Februar 2025, https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport_Final_020325.pdf*

[3] *Spacelift, Password Statistics: How Users and Companies Manage Credentials, Januar 2025, https://spacelift.io/blog/password-statistics*

[4] *DLA Piper, GDPR Fines across Europe Total €1.2 Billion in 2024, Januar 2025, https://legalcommunitygermany.com/gdpr-fines-across-europe-total-e1-2-billion-in-2024-according-to-dla-piper/*

[5] *Fraunhofer IESE, NIS-2-Richtlinie – Zusammenfassung und Umsetzung in Deutschland, Blogbeitrag, Juli 2024, https://www.iese.fraunhofer.de/blog/nis-2-richtlinie-zusammenfassung-umsetzung-deutschland/*

[6] *Industrie- und Handelskammer zu Leipzig (IHK Leipzig), NIS-2-Richtlinie: Neue gesetzliche Anforderungen für Unternehmen zur IT-Sicherheit, undatiert, https://www.leipzig.ihk.de/infos-fuer-unternehmen/themen/business-digital/it-sicherheit/nis2-richtlinie-neue-gesetzliche-anforderungen-fuer-unternehmen-zur-it-sicherheit/*

[7] *Anakage Inc., Guide to Active Directory and Identity & Access Management, Blogbeitrag, 2025, https://anakage.com/blog/guide-to-ad-iam/*

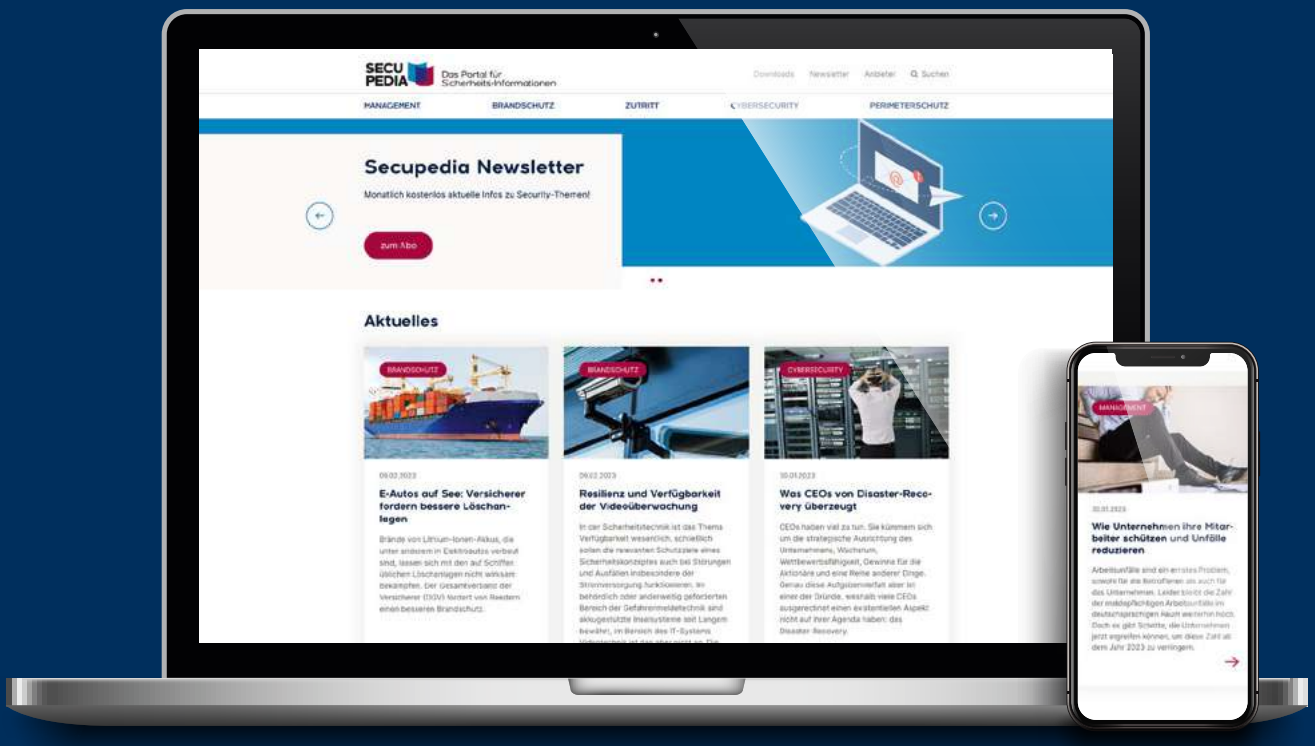
[8] *Microsoft Corporation, Deploy Identity for Zero Trust, Dokumentation, undatiert, https://learn.microsoft.com/en-us/security/zero-trust/deploy/identity*

SVENJA WINKLER
ist CEO & Head of Products bei der BAYOOSOFT GmbH.

Leitfaden UAM in der Praxis: So realisieren Sie mit No-Code IAM Onboarding-Automation

SECU PEDIA

Die Plattform für Sicherheitsinformationen



✓ Aktuelle News
✓ Webinare & Webkonferenzen
✓ Whitepaper
✓ Fachbeiträge

www.secupedia.de

Risikokontext statt starre Rollen

THREAT-AWARE IAM: WENN ZUGRIFFSRECHTE ZUR VERTEIDIGUNGSLINIE WERDEN

Identitäten sind mittlerweile zur dominanten Angriffsfläche digitaler Infrastrukturen geworden. Wer Zugriff auf Systeme, Anwendungen und Daten erhält, kontrolliert nicht nur Informationen, sondern beeinflusst Betriebsfähigkeit, Entscheidungsautonomie und regulatorische Haftung. Das klassische Identity- und Access-Management (IAM) verwaltet diese Zugriffsrechte entlang statischer Rollen, verteilter Verzeichnisse und periodischer Prüfzyklen. Doch angesichts dynamischer Bedrohungen, hybrider Cloud-Architekturen und automatisierter Zugriffspfade verliert dieses Modell an Wirksamkeit. Threat-aware IAM ersetzt die statische Logik durch kontinuierliche Risikoanalyse, adaptive Kontrolle und operative Verteidigungsfähigkeit.

Angriffe zielen längst nicht mehr auf Systeme, sondern stark auf Identitäten. Malware, Phishing, gestohlene Token oder kompromittierte Servicekonten dienen als Einfallstor, Eskalationsvektor und Persistenzanker. Angreifer bewegen sich entlang legitimer Pfade durch verteilte Infrastrukturen, getarnt durch formale Berechtigungen. Wer sich auf Rollenmodelle und Passwortwechsel verlässt, erkennt diese Bewegungen zu spät.

KONTEXTBEZOGENE BEWERTUNGEN STATT STARRER REGELN

Ein Threat-aware IAM ersetzt statische Zugriffsentscheidungen durch kontextbezogene Bewertungen in Echtzeit. Standort, Geräteintegrität, Uhrzeit, Sitzungsdynamik, Datenmuster und Authentifizierungsverhalten fließen in eine kontinuierliche Risikoanalyse ein. Zugriffe werden freigegeben, begrenzt oder verweigert, je nachdem, ob sie dem erwartbaren Handlungskontext entsprechen oder nicht.

Das klassische IAM erkennt keine Zusammenhänge. Es prüft lediglich, ob jemand eine Rolle besitzt, nicht jedoch, ob diese Rolle gerade zum Verhalten passt. Threat-aware IAM analysiert dagegen die Wechselwirkungen. Es erkennt, wenn ein Konto kurz nach der Privilegienausweitung aus ungewohnten Regionen auf sensible Systeme zugreift. Es eskaliert, wenn Servicekonten plötzlich interaktive Sessions starten. Es greift ein, wenn Authentifizierungsversuche scheitern, aber anschließend durch Multi-Faktor-Authentifizierungs-(MFA)-Fatigue erfolgreich umgangen werden. Diese Reaktionsfähigkeit macht Identitätskontrolle zur Sicherheitsdisziplin.

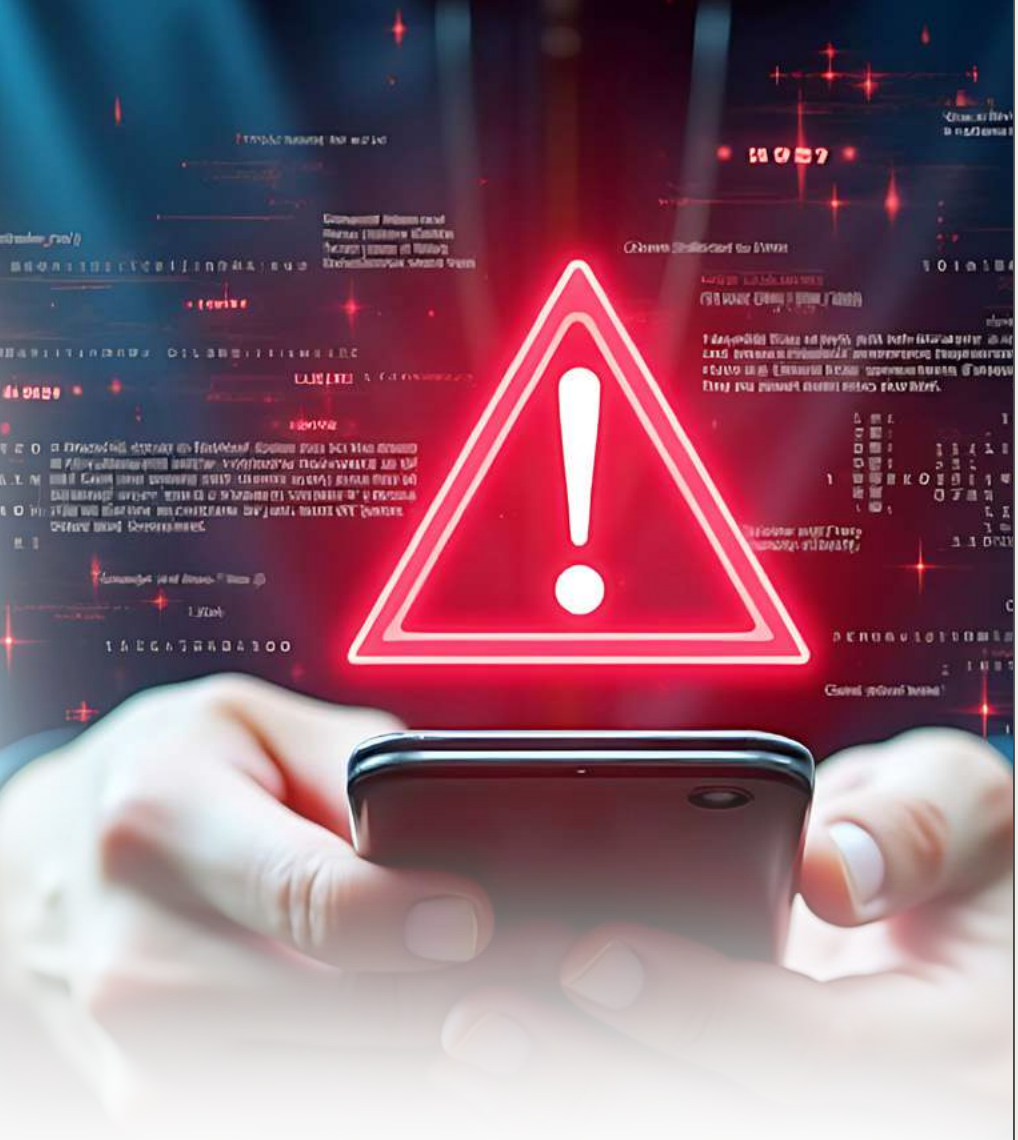
IDENTITÄTEN ALS DYNAMISCHE RISIKOQUELLE

Die Herausforderung liegt nicht allein in der Detektion, sondern in der Struktur. Unternehmen in Deutschland und Europa betreiben verteilte Identitätslandschaften: Active Directory, Entra ID, lokale Verzeichnisse, Cloud-Konnektoren, Application Programming Interfaces (APIs), Software-as-a-Service-(SaaS)-Anwendungen. Daraus entstehen Inkonsistenzen, Dubletten, Schattenidentitäten. Jeder neue Service erzeugt neue technische Konten, jedes neue Projekt zusätzliche Rechtekombinationen. Die Folge ist Identitätsschattenwuchs: verwaiste Konten, vergessene Keys, historische Berechtigungen, die nie reduziert wurden.

Ein Threat-aware IAM beginnt mit der Konsolidierung. Es schafft einen zentralen Identitätsbestand, in dem jede Person, jede Maschine, jeder Dienst eindeutig referenzierbar ist. Rollen, Gruppen, Rechte und Zugriffspfade werden vereinheitlicht, normalisiert und über alle Plattformen hinweg korreliert.

Dieser Bestand bildet die Grundlage für Angriffspfadanalysen. Nicht jede Berechtigung ist für

Bild: Mobasser - stock.adobe.com



sich kritisch, aber in Kombination mit anderen entsteht eine Eskalationskette. Threat-aware IAM identifiziert diese Pfade. Welche Konstellation führt vom einfachen SaaS-Nutzer zum Cloud-Admin? Welche Gruppenmitgliedschaft öffnet indirekten Zugriff auf operative Systeme? Welche Verbindung zwischen Testumgebung und Produktivsystem existiert nur auf Rechteebene? Die Analyse dieser Ketten macht aus einem statischen Rollenmodell eine dynamische Bedrohungslandschaft.

DIE GRENZEN ZWISCHEN IAM UND SOC VERSCHWINDEN

In vielen Organisationen sind Identity-Management und Sicherheitsbetrieb organisatorisch und technisch getrennt. Das IAM verwaltet, das Security Operations Center (SOC) detektiert und reagiert. Doch gerade bei identitätsbasierten Angriffen führt diese Trennung zu blinden Flecken. Ein kompromittiertes Konto ist keine reine Verwaltungsfrage, sondern ein sicherheitskritischer Vorfall. Deshalb muss Threat-aware IAM nahtlos in die operativen Sicherheitsprozesse integriert sein. Zugriffsentscheidungen, Risikoalarme und Verhaltensanomalien müssen in Echtzeit in die Sicherheitsinfrastruktur fließen. Umgekehrt müssen Security-Teams direkt auf Identitäten zugreifen, Rechte sperren, Sitzungen beenden oder Authentifizierungsstufen anpassen können.

Diese Verzahnung erfordert technische Schnittstellen, organisatorische Abläufe und abgestimmte Reaktionsszenarien. SOC-Playbooks müssen identitätszentrierte Eskalationen enthalten. IAM-Systeme müssen APIs für Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) und Threat Intelligence bereitstellen. Nur so entstehen automatisierte Verteidigungsketten, die auf identitätsbasierte Bedrohungen ebenso schnell reagieren wie auf Netzwerkangriffe.

RISIKOKOMBINATIONEN ERKENNEN UND FUNKTIONALE TRENNUNGEN DURCHSETZEN

Ein oft übersehener Aspekt identitätsbasierter Sicherheitsarchitektur ist das Zusammenspiel von Berechtigungen innerhalb eines Kontos.

Nicht jede einzelne Rechtezuweisung birgt Risiko, wohl aber bestimmte Kombinationen. Wenn etwa ein Benutzerkonto gleichzeitig über Zugriffsrechte auf Bestellfreigaben und Buchhaltungsprozesse verfügt, entsteht eine Konstellation, die regulatorisch unzulässig und operativ anfällig ist. Solche sogenannten toxischen Kombinationen unterlaufen das Prinzip der Funktionstrennung und öffnen Tür und Tor für Manipulation, unautorisierte Transaktionen und das Verschleiern von Aktivitäten.

In klassischen IAM-Systemen bleibt dieses Risiko häufig unbemerkt, da Rollen und Rechte modular verwaltet, aber nicht in ihrer Gesamtheit analysiert werden. Threat-aware IAM setzt hier gezielt an. Es modelliert systematische Regelwerke zur Trennung kritischer Aufgaben und überprüft Zugriffsrechte nicht nur isoliert, sondern im Zusammenspiel. Dabei kommen sogenannte Segregation-of-Duties-(SoD)-Matrizen zum Einsatz, die auf Applikationsebene ebenso wie übergreifend über Prozesse und Systeme hinweg toxische Konstellationen identifizieren.

Die Analyse berücksichtigt sowohl formale Rollen als auch faktische Nutzungsmuster und reagiert, wenn eine Regelverletzung entsteht, durch automatisierte Entzugsvorgänge, Eskalation an Governance-Instanzen oder temporäre Rechteblockierung. Diese Form der kontextuellen Rechtebewertung ist besonders in regulierten Sektoren wie der Finanzwirtschaft, dem Gesundheitswesen oder der öffentlichen Verwaltung unverzichtbar, um Transparenz, Integrität und Prüfbarkeit dauerhaft sicherzustellen.

REGULATORISCHER DRUCK UND NACHWEISPFLICHTEN

In Deutschland und der EU verschärfen gesetzliche Vorgaben den Handlungsdruck. Die Datenschutz-Grundverordnung verlangt Nachvollziehbarkeit und Minimierung personenbezogener Zugriffe. Die NIS-2-Richtlinie verpflichtet kritische Infrastrukturen zur kontinuierlichen Risikobewertung und Reaktionsfähigkeit. Klassische IAM-Modelle stoßen hier an Grenzen. Sie erfassen keine Kontexte, kennen keine Prioritäten, bieten keine Echtzeitkontrolle.

Threat-aware IAM hingegen dokumentiert, bewertet und steuert Identitäten als dynamische Risikofaktoren. Es erlaubt revisionssichere Nachweise. Warum wurde Zugriff gewährt, wann wurde eingeschränkt, auf Basis welcher Indikatoren wurde blockiert? Diese Transparenz macht es zum Werkzeug regulatorischer Absicherung.

IMPLEMENTIERUNGSANSÄTZE UND SKALIERBARKEIT

Die Umsetzung eines Threat-aware IAM verlangt mehr als technische Anpassung. Sie erfordert einen strategischen Perspektivwechsel. Identitätssicherheit ist nicht Aufgabe der IT, sondern Teil der Sicherheitsarchitektur. Fachbereiche müssen Verantwortung für Rollen, Berechtigungen und Zugriffskontexte übernehmen. Prozesse müssen Risikoindikatoren berücksichtigen.

Technisch beginnt die Implementierung mit einer strukturierten Erfassung aller Identitäten, ihrer Berechtigungen, Beziehungen und Kontexte. Darauf aufbauend erfolgt die Integration von Verhaltensanalysen, Angriffspfadlogik und automatisierten Eskalationen.

Je nach Größe, Struktur und regulatorischem Umfeld variieren Architektur und Tiefe der Implementierung. Große Organisationen benötigen skalierbare Plattformen, die hohe Datenvolumina in Echtzeit verarbeiten, rollenübergreifende Risiken abbilden und komplexe Eskalationsszenarien steuern können. Mittelständische Unternehmen können pragmatisch starten. Hier helfen die Integration zentraler Identitätsspeicherung, einfache kontextabhängige Regeln und die Anomalieerkennung für privilegierte Konten.

Entscheidend ist nicht der Umfang, sondern die Ausrichtung. Berechtigungen orientieren sich weg von starren Rollen, hin zu dynamischen Bewertungen. So wird die Zugriffssteuerung nicht zur Formalität, sondern zur aktiven Sicherheitsinstanz.

IDENTITÄT ALS STEUERZENTRUM DIGITALER RESILIENZ

Ein Threat-aware IAM verändert das Verständnis von Identität. Es behandelt sie nicht als statisches Objekt mit Zugriffsrechten, sondern als bewegliches Element in einer Bedrohungslage. Es misst Verhalten, bewertet Kontext, erkennt Muster, greift ein.

Daraus entsteht ein Steuerungsinstrument, das nicht nur Zugriff erlaubt, sondern das Risiko steuert. In einer digitalisierten Infrastruktur ohne feste Perimeter ist das kein Zusatznutzen, sondern Voraussetzung für Integrität, Nachvollziehbarkeit und Reaktionsfähigkeit. Wer die Identität nicht als operatives Risiko steuert, verliert sie als Kontrollpunkt. Threat-aware IAM stellt diesen Kontrollpunkt wieder her.

SO GELINGT DIE UMSETZUNG

Unternehmen, die Threat-aware IAM umsetzen wollen, sollten nicht auf einen Big-Bang-Ansatz setzen, sondern schrittweise vorgehen. Der erste Schritt besteht darin, die eigene Identitätslandschaft vollständig zu erfassen, zu konsolidieren und nach Verantwortlichkeiten zu strukturieren. Darauf folgt die Etablierung risikobasierter Zugriffspolitiken, die nicht auf statischen Rollen, sondern auf kontextabhängigen Entscheidungen beruhen.

Parallel dazu müssen Sicherheitsarchitektur, SOC-Prozesse und Governance-Strukturen so verzahnt werden, dass identitätsbezogene Ereignisse nicht isoliert, sondern in Echtzeit analysiert und beantwortet werden können.

Wichtig ist, dass Identitätssicherheit als kontinuierlicher Prozess verstanden wird. Dabei entsteht eine Infrastruktur, die sich mit der Bedrohungslage verändert, mit Nutzungsmustern lernt und mit Angriffen wächst. Wer diesen Wandel strategisch plant, technologisch fundiert umsetzt und organisatorisch absichert, verwandelt Identitäten von einem Risiko in einen Verteidigungspunkt, skalierbar, überprüfbar und resilient. ■

THOMAS JOOS
ist freier Journalist.

No Code IAM für moderne Zugriffskontrolle

Einfaches Berechtigungsmanagement, das mir Ihrer IT wächst.

Mit der No Code Lösung von BAYOOSOFT steuern Unternehmen ihre Berechtigungen, Rollen und Zugriffe sicher, effizient und vollständig nachvollziehbar, ganz ohne Programmieraufwand. Self Service Portale, automatisiertes On und Offboarding sowie transparente Workflows sorgen dafür, dass IT Abteilungen entlastet und Prozesse stabil laufen. Jede Änderung wird lückenlos dokumentiert, sodass Sie jederzeit wissen, wer worauf Zugriff hat und warum. Das schafft Sicherheit, stärkt die Compliance und erleichtert jede Prüfung.

Jetzt mehr erfahren!

bayoosoft.com

Security made in Germany

Trust Seal www.teletrust.de/itsmig

TÜV PROFICERT ® TÜV Hessen

ISO 9001 73 100 7989

www.proficert.de

Wie Unternehmen der strukturierte Umstieg gelingt

IN SIEBEN SCHRITTEN ZUR ZERO-TRUST-UMGEBUNG

Der Zero-Trust-Ansatz stellt vorhandene Sicherheitsarchitekturen auf den Prüfstand: Statt pauschalem Vertrauen überprüft das System jeden einzelnen Zugriff genau – ohne Ausnahme. Für Unternehmen bedeutet das tiefgreifende Veränderungen, die nahezu alle Systeme betreffen. Dieser Wandel will sorgfältig geplant sein. Eine schrittweise Einführung in mehreren Phasen hilft, Risiken zu verringern, Geschäftsprozesse stabil zu halten und Sicherheitslücken systematisch zu schließen.

Für Unternehmen führt derzeit kein Weg an Zero Trust vorbei: Angriffe über kompromittierte Benutzerkonten oder vermeintlich vertrauenswürdige Kanäle zeigen deutlich, dass klassische Schutzmaßnahmen, die auf Netzwerkgrenzen beruhen, nicht mehr ausreichen. Zudem lassen Cloud-Dienste und Remote Work die Grenzen von Unternehmensnetzwerken zunehmend verschwimmen.

An dieser Stelle setzt der Zero-Trust-Ansatz an. Er vertraut keinem Benutzer, Gerät oder Dienst – unabhängig davon, ob sie sich innerhalb oder außerhalb des eigenen Netzwerks befinden. Jeder Zugriff wird kontextabhängig geprüft, basierend auf Identität, Gerätestatus und Risiko.

Das erfordert von Unternehmen nicht nur ein Umdenken in der Sicherheitsarchitektur, sondern auch organisatorische Veränderungen: Zuständigkeiten, Berechtigungen und Prozesse müssen überprüft und neu strukturiert werden. Die Umsetzung von Zero Trust ist daher kein einzelnes Projekt, sondern ein kontinuierlicher Transformationsprozess.

Wer den Wechsel planlos angeht, riskiert Störungen im Betrieb und unnötige Komplexität. Ein schrittweises Vorgehen sorgt dafür, dass technische Maßnahmen, organisatorische Abläufe und Sicherheitsrichtlinien aufeinander abgestimmt bleiben. Ein bewährter Ansatz ist die Einführung in mehreren Phasen – beginnend mit einer klaren Analyse der Ausgangslage bis hin zu kontinuierlicher Überwachung und Kontrolle.

BESTANDSAUFNAHME UND „QUICK WINS“

Am Anfang steht eine gründliche, risikobasierte Bestandsaufnahme: Welche Benutzer, Geräte, Anwendungen und Datenbestände existieren, wie sind sie miteinander verknüpft und wo liegen besonders schützenswerte Informationen, Passwörter oder Token? Darauf aufbauend bewerten die Verantwortlichen Risiken, legen Prioritäten fest und identifizieren erste „Quick Wins“ – also Maßnahmen, die sich mit geringem Aufwand umsetzen lassen und das Risiko deutlich reduzieren.

Ebenso sollten Unternehmen messbare Ziele definieren, etwa deutlich weniger dauerhafte Berechtigungen oder einen schnelleren Entzug von Zugriffsrechten. Das Ergebnis dieser Analyse ist eine Blaupause der künftigen Architektur mit einer priorisierten Maßnahmenliste und einem Plan für die schrittweise Umsetzung.

PHASE 1: IDENTITY GOVERNANCE UND LIFECYCLE MANAGEMENT

In der ersten Phase sollten Unternehmen zwei zentrale Grundlagen schaffen. Erstens ein standardisiertes Identity-Lifecycle-Management mit

automatisierten Prozessen für Eintritt, Rollenwechsel und Austritt von Mitarbeitern. Dabei werden die für eine Rolle notwendigen, möglichst minimalen Berechtigungen automatisch vergeben, angepasst oder entzogen – und zwar über alle Systeme hinweg.

Zweitens sollten IT-Teams Rollen und Attribute vereinheitlichen sowie doppelte oder verwaiste Konten beseitigen – etwa durch rollen- und attributbasierte Zugriffskontrollen. Ein sauberes, konsistentes Identitätsmanagement reduziert die Angriffsfläche erheblich und bildet die Grundlage für alle folgenden Phasen.

PHASE 2: STARKE, ADAPTIVE AUTHENTIFIZIERUNG UND SINGLE SIGN-ON

Im nächsten Schritt steht die Absicherung des Zugriffs im Fokus. Passwortbasierte Verfahren sollten einer Multi-Faktor-Authentifizierung (MFA) mit phishing-sicheren Faktoren weichen. Ergänzend reduziert Single Sign-on die Zahl der Anmeldevorgänge und erleichtert die Umsetzung einheitlicher Richtlinien. Wichtig ist, dass Authentifizierungsanforderungen situationsabhängig angepasst werden – etwa bei ungewöhnlichen Zugriffsorten oder neuen Geräten.

PHASE 3: LEAST-PRIVILEGE-PRINZIP

Anschließend lässt sich die Sicherheit durch die konsequente Umsetzung des Least-Privilege-Prinzips noch einmal deutlich erhöhen: Berechtigungen sollten immer nur für den Zeitraum und Umfang vergeben werden, der tatsächlich erforderlich ist. Ideal sind automatisierte Just-in-time-Freigabe-Workflows, die die für eine Aufgabe erforderlichen Zugriffsrechte erteilen und zum vorher festgelegten Zeitpunkt automatisch wieder entziehen. So lassen sich die Berechtigungen von menschlichen und nichtmenschlichen Identitäten auf die minimal notwendigen Rechte begrenzen.

PHASE 4: SEGMENTIERUNG VON ANWENDUNGEN UND DATEN

Statt ganze Netzsegmente pauschal freizugeben, sollten Unternehmen den Zugriff auf Anwendungs- oder Datenebene steuern. Diese Mikrosegmentierung begrenzt im Ernstfall die Ausbreitung eines Angriffs. Sensible Daten lassen sich zusätzlich mit Attributregeln und kontinuierlicher Autorisierung absichern. Für ältere Anwendungen bieten sich vorgelagerte Sicherheits-Broker an, die Authentifizierung und Zugriffskontrolle übernehmen.

PHASE 5: KONTINUIERLICHES MONITORING UND ANALYSE

Spätestens jetzt sollten sich Unternehmen Gedanken zur Überwachung der eingeführten Maßnahmen machen, um Zero Trust als fortlaufenden Prozess zu etablieren. Monitoring-Systeme sollten Identitäts-, Zugriffs- und Aktivitätsdaten zentral auswerten, um Anomalien wie untypische Datenabfragen oder privilegierte Aktionen zu erkennen. Methoden wie eine Analyse des Benutzerverhaltens (User Behavior Analysis, UBA) helfen, verdächtige Aktivitäten frühzeitig zu identifizieren und automatisierte Gegenmaßnahmen einzuleiten.

PHASE 6: STEUERUNG UND RESILIENZ

Sobald die technischen Grundlagen geschaffen sind, müssen Organisationen diese in stabile Betriebsprozesse überführen. Dazu zählen regelmäßige Überprüfungen von Zugriffsrechten, Notfallmechanismen für privilegierte Konten sowie Testübungen, die die Wirksamkeit der Richtlinien überprüfen. Backups sollten auch Identitäts- und Richtliniendaten einschließen, um zu verhindern, dass sich nach einer Wiederherstellung ungewollte Berechtigungen einschleichen.

PHASE 7: ERWEITERUNG AUF PARTNER UND WORKLOADS

Zero Trust endet nicht an der Unternehmensgrenze, sondern sollte auch für externe Partner, Dienstleister und automatisierte Workloads gelten. Dazu gehören die gemeinsame Nutzung bestehender Identitätssysteme, starke Authentifizierungsfaktoren und minimale Berechtigungen. Ebenso wichtig ist, den Zugriff nach Vertragsende automatisch zu beenden und die Einhaltung der Sicherheitsvorgaben regelmäßig zu prüfen.

FAZIT

Zero Trust ist kein Projekt mit festem Endpunkt, sondern eine langfristige Sicherheitsstrategie. Wer den Ansatz schrittweise umsetzt, kann bestehende Systeme gezielt modernisieren und gleichzeitig die Geschäftskontinuität wahren. Entscheidend ist, Identität, Kontext und Risiko in jeder Phase ins Zentrum der Sicherheitsarchitektur zu stellen – so entsteht ein belastbares Fundament für eine widerstandsfähige IT. ■

SASCHA DEGENHARDT
ist Security Expert und Group Manager Consulting für die ManageEngine-Lösungen bei der MicroNova AG.

Digitales Onboarding

WARUM BANKEN AUF VERSCHIEDENE IDENTIFIKATIONS-VERFAHREN ANGEWIESEN SIND

Durch die Digitalisierung hat die Neukundenaufnahme im Finanzsektor deutlich an Tempo und Effizienz gewonnen – allerdings nur dort, wo Prozesse flexibel genug gestaltet sind, um auf sich wandelnde Vorgaben und Erwartungen reagieren zu können. Regulatorische Anforderungen, Betrugsprävention und Kundenerlebnis müssen heute gleichermaßen berücksichtigt werden. Da sich sowohl Compliance-Vorgaben als auch Kundenbedürfnisse stetig verändern, ist eine einheitliche Vorgehensweise kaum mehr praktikabel. Gefragt sind Onboarding-Prozesse, die sich dynamisch anpassen lassen – und Sicherheit sowie Rechtskonformität von Anfang an fest verankern.

Seit nunmehr knapp zweieinhalb Jahrzehnten haben Neukunden einer Bank die Möglichkeit, sich digital, schnell und unkompliziert ein Konto zu eröffnen, ohne persönlich vor Ort erscheinen und handschriftlich Formulare ausfüllen zu müssen. Seinen Anfang machte das sogenannte digitale Onboarding in den späten 1990er- und frühen 2000er-Jahren – praktisch zeitgleich mit dem Beginn des Onlinebankings.

Den entscheidenden Schub gaben vor allem Neobanken und Fintechs. Mit vollständig digitalen, mobil optimierten Prozessen setzten sie neue Maßstäbe für Geschwindigkeit, Einfachheit und Kundenerlebnis. Traditionelle Finanzinstitute holten aber rasch auf. Ein Wettlauf um die besten Onboarding-Verfahren begann, bei dem es darum ging, alle Prozessschritte – von der Identifizierung über die digitale Signatur bis hin zur Compliance-konformen Risiko- und Betrugsprüfung – möglichst nahtlos in eine einzige digitale Prozesskette zu integrieren.

Im Zuge dieser Entwicklung verlagerte sich der Fokus der Branche von internen Eigenentwicklungen auf skalierbare Software-as-a-Service-(SaaS)-Lösungen. Über standardisierte Schnittstellen ließen sich diese direkt in bestehende Onboarding-Anwendungen einbinden. Dies nicht zuletzt auch mit dem Hintergedanken, dass den Banken der Rückgriff auf externe spezialisierte Dienstleister den flexiblen Aufbau einer agileren Onboarding-Architektur ermöglichen würde.

WARUM DIVERS?

Fähigkeiten wie Flexibilität, Agilität und Souveränität bei digitalen Onboarding-Verfahren bieten Unternehmen der Finanzbranche – und nicht nur diesen – in vielerlei Hinsicht Vorteile. Sie sollen nicht nur die Kundenerfahrung verbessern, sondern auch messbar die Abschlussquote (Konversionsrate) erhöhen. Eine breitere Aufstellung ermöglicht den Aufbau eines Onboarding-Angebots, das sich stärker an den persönlichen Präferenzen der Neukunden und ihrer technischen Ausstattung orientieren kann.

Gleichzeitig lassen sich Kosten und Durchlaufzeiten reduzieren. Denn nicht jedes Identifikationsverfahren bietet das gleiche Maß an Sicherheit, nicht jedes Verfahren erzeugt dieselben Kosten – und nicht für jedes Onboarding, nicht für jedes Onboarding-Risiko und jede Risikogruppe müssen die gleichen Compliance-Anforderungen erfüllt werden. Mit einer angepassten Auswahl lassen sich also Einsparmöglichkeiten realisieren.

Hinzu kommt, dass sich die Onboarding-Technologie stetig weiterentwickelt. Ebenso wie die Vorgaben und Richtlinien der Europäischen Union (EU) sowie der Europäischen Zentralbank, der Bundesregierung und der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) – vom Digital Operational Resilience Act (DORA) bis zur europäischen Anti-Money Laundering Directive (AMLD), vom deutschen Geldwäschegesetz (GWG) – Stichwort Know Your Customer (KYC) –

bis hin zur europäischen Verordnung für Electronic IDentification, Authentication und Trust Services (eIDAS). Je breiter und flexibler sich Banken aufstellen, desto besser können sie mit diesen Entwicklungen Schritt halten.

DIE VIELFALT DER ONBOARDING-VERFAHREN

Der digitale Onboarding-Prozess einer Bank ist darauf ausgelegt, vollständig rechtskonform Neukundenbeziehungen herzustellen. Hierzu sind zwei Schritte erforderlich: die Identifikation des Neukunden nach GwG und der Erwerb einer Qualifizierten Elektronischen Signatur (QES) nach eIDAS.

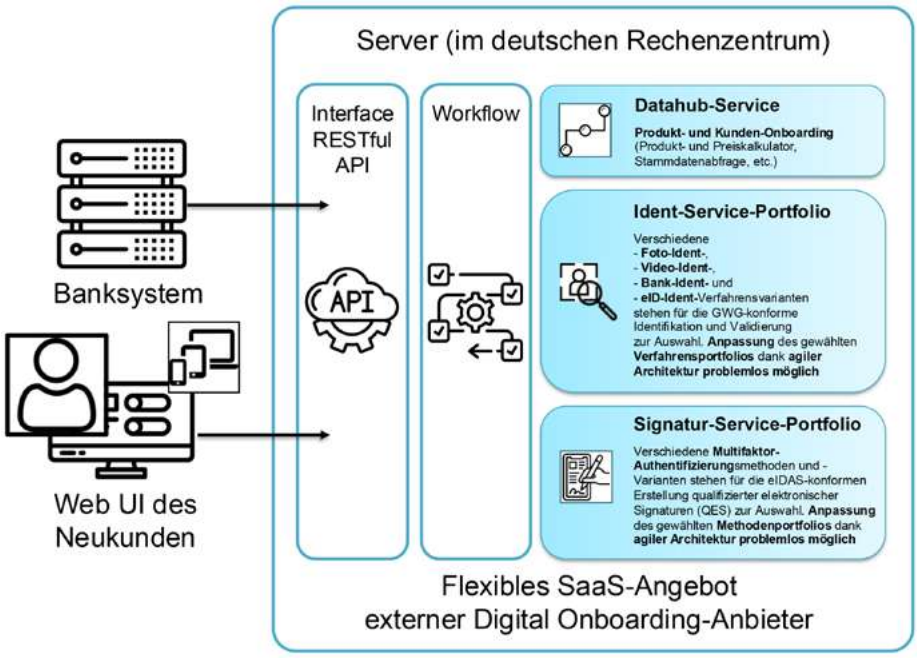
Zur Identifikation kommt in aller Regel eines der folgenden vier Verfahren zur Anwendung:

1. **Videoident-Verfahren:** Der Neukunde führt mit einem geschulten Mitarbeiter eines externen Dienstleisters der Bank ein Live-Videogespräch. Hierbei wird eine Liveness Detection (Prüfung auf Lebendigkeit) durchgeführt. Der Neukunde hält ein Ausweisdokument in die Kamera, lässt es den Mitarbeiter auf dessen Echtheit prüfen (Sicherheitsmerkmale) und mit seinem Gesicht vergleichen.

2. **eID-Ident-Verfahren:** Der Neukunde identifiziert sich unter Zuhilfenahme der Online-Ausweisfunktion (eID) eines Ausweises (etwa seines Personalausweises). Hierzu nutzt er ein Near-Field-Communication-(NFC)-fähiges Smartphone oder Lesegerät sowie seine sechsstellige PIN.

3. **Bank-Ident-Verfahren:** Der Neukunde nutzt seinen bei einer anderen Bank bereits bestehenden Onlinebanking-Zugang. Die neue Bank gleicht die Identitätsdaten des Kunden mit den bereits bei der alten Bank verifizierten Daten ab.

4. **Foto-Ident- beziehungsweise Auto-Ident-Verfahren:** Der Kunde macht Fotos von seinem Ausweisdokument und anschließend ein Selfie oder kurzes Video von sich selbst. Künstliche Intelligenz (KI) und biometrische Software prüfen die Echtheit der Dokumente, vergleichen die Gesichtsmerkmale von Ausweis und Foto beziehungsweise Video und führen dann eine Liveness Detection durch.



Beispiel eines SaaS-Onboarding-Angebots (Quelle: POS Solutions, A PROCILON COMPANY)

Der anschließende Schritt – der Erwerb einer Qualifizierten Elektronischen Signatur als Ersatz für die handschriftliche Unterschrift – ist in der Regel durch eine Zwei-Faktor-Authentifizierung abgesichert. Häufig erfolgt dies über die Übertragung eines eindeutig zugeordneten Signaturzertifikats in Kombination mit einer PIN oder TAN. Alternativ kann die Bestätigung auch per Push-Benachrichtigung auf das Mobilgerät des Neukunden ausgelöst werden.

Alle genannten Verfahren existieren in verschiedenen Varianten und bringen jeweils eigene Stärken und Schwächen mit sich – etwa in puncto Kosten, Nutzererlebnis und Sicherheit. Sie haben für den einen oder anderen Onboarding-Anwendungsfall durchaus ihre Daseinsberechtigung. Welches Verfahren das digitale Onboarding in den kommenden Jahren klar dominieren wird, ist aber schon heute absehbar.

EUDI-WALLET ALS KÜNFTIGER STANDARD

Biometrische Verfahren sind beim digitalen Onboarding derzeit noch weit verbreitet – sowohl bei der Identifikation per Foto- oder Videoident (Analyse von Iris, Stimme oder Gesicht) als auch beim Signaturerwerb per Unterschrift auf Tablet oder Smartphone. Doch der Trend kehrt sich bereits um: Der Einsatz biometrischer Merkmale und der darauf aufbauenden Verfahren nimmt kontinuierlich ab.

Die Zukunft gehört den eID-basierten Identifikationsverfahren. In Deutschland steht derzeit der Personalausweis mit Online-Ausweisfunktion im Mittelpunkt. NFC-fähige Smartphones haben ihm zum Durchbruch verholfen. Seine Vorherrschaft dürfte jedoch nur von kurzer Dauer sein: Mit der Einführung der European Digital Identity Wallet (EUDI-Wallet) dürfte sich das Identitätsmanagement grundlegend verändern.

Finanzdienstleister sollten sich frühzeitig darauf einstellen, die EUDI-Wallet ab 2027/2028 in ihre Onboarding-Prozesse zu integrieren. Eine Möglichkeit dafür besteht in der Zusammenarbeit mit einem SaaS-Anbieter, der flexible Schnittstellen bereitstellt und Anpassungen an neue regulatorische und technologische Anforderungen erleichtert. Ohne entsprechende Flexibilität könnte es für viele Banken schwer werden, mit künftigen Entwicklungen Schritt zu halten. ■

BERNT VOSSEBEIN
ist CEO der POS Solutions, A PROCILON COMPANY.

IAM als Pfeiler der Unternehmenssicherheit in KRITIS

BERECHTIGUNGEN BRAUCHEN KLARE STRUKTUREN

Die Verwaltung von Zugriffsrechten wird für Betreiber kritischer Infrastrukturen (KRITIS) zunehmend komplexer. Tausende Berechtigungen müssen nach dem Sparsamkeitsprinzip vergeben und kontinuierlich überwacht werden – vom Onboarding bis zum Austritt der Mitarbeiter.

Identity- und Access-Management (IAM) stellt Unternehmen aus allen KRITIS-Branchen vor ähnliche Herausforderungen, wenn auch in unterschiedlicher Ausprägung. Die Betriebsabläufe müssen reibungslos funktionieren, während gleichzeitig sichergestellt sein muss, dass Berechtigungen nach dem Least-Privilege-Prinzip vergeben werden – also auf das notwendige Minimum pro Tätigkeit. Diese Anforderung muss vom Onboarding über Versetzungen, Abwesenheiten und Wiedereingliederungen bis hin zum Offboarding durchgängig umgesetzt sein.

Dabei geht es nicht nur darum, alle erforderlichen IT-Berechtigungen zu vergeben. Zusätzlich müssen Verantwortliche dafür sorgen, dass zwischen diesen kein Interessenkonflikt vorliegt. Sie müssen die Trennung toxischer Funktionen (Segregation of Duties) stets gewährleisten. Die digitale Überwachung und Umsetzung gehören zur Erwartungshaltung, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und durch NIS-2 vorgegeben werden.

SECHSSTELLIGE ANZAHL VON BERECHTIGUNGEN IM KRANKENHAUS

Am Beispiel eines Krankenhauses wird schnell ersichtlich, wie umfangreich IAM im Alltag greift. Vom zentralen Krankenhausinformationssystem (KIS) über die elektronische Bildverarbeitung, das Dokumentenmanagementsystem, die Patientenakte, diverse Portalsysteme und die Bettenverwaltung mit RFID-Transpondern bis zur Telemedizin: Unterschiedliche Berechtigungen müssen verwaltet werden. Die IT-Abteilung eines Krankenhauses mittlerer Größe mit 700 Betten muss beispielsweise circa 1.500 mögliche Berechtigungen den richtigen 2.700 Mitarbeitern zuordnen. Bei knapp 50 Berechtigungen pro Benutzer verantwortet die IT damit eine sechsstellige Anzahl von IT-Berechtigungen. Hinzu kommen Zutrittsberechtigungen für sensible Bereiche wie Server- und Technikräume oder Medikamentenarchive.

Doch auch außerhalb der Gesundheitsbranche müssen Unternehmen Energieversorgungsnetze und Energieanlagen schützen. Es sollte zudem klar geregelt sein, welche Führungskräfte über Kompetenzen wie Zeichnungsberechtigungen und Vollmachten, wie Prokura, verfügen.

Bild: Who is Danny - stock.adobe.com

ANGREIFER NUTZEN FEHLBERECHTIGUNGEN AUS

Ein Fehler in der Berechtigungsverwaltung kann hierbei schnell zu wirtschaftlichen Schäden führen. KRITIS-Unternehmen stehen besonders im Fokus von externen Angreifern, für die weitreichende Berechtigungen ein wichtiges Einfallstor darstellen können. Doch auch interne Fehlberechtigungen können zur Verletzung der Vertraulichkeit mit Sanktionierung nach der Datenschutzgrundverordnung (DSGVO) führen. IAM ist somit kein reines IT-Thema – es ist ein wichtiger Pfeiler für die Unternehmenssicherheit und spielt in allen Bereichen eine Rolle.

Neben der präventiven Wirkung des Berechtigungsmanagements bildet die lückenlose Dokumentation von Berechtigungen die Grundlage zur Nachvollziehbarkeit im Ernstfall. Ein regelmäßiger Abgleich der Soll-Vorgaben mit den tatsächlich vergebenen Ist-Berechtigungen ermöglicht die Erkennung und Beseitigung falscher Berechtigungen und stellt gleichzeitig sicher, dass benötigte Berechtigungen nicht erst durch ihr Fehlen im Einsatz auffallen.

Energieversorger können auf diese Weise beispielsweise frühzeitig erkennen, wenn bei der Prüfung einer Person versehentlich Zutrittsberechtigungen für kritische Anlagen erteilt wurden, obwohl diese nur im Verwaltungsbereich tätig ist. Am Beispiel von Cisco, wo im Jahr 2018 ein ehemaliger Mitarbeiter nach seinem Austritt aufgrund weiterhin bestehender Berechtigungen über 400 virtuelle Server löschte und damit erheblichen Schaden für seinen ehemaligen Arbeitgeber verursachte, ist erkennbar, dass eine regelmäßige Prüfung kritischer Zugänge nicht nur eine Anforderung der Aufsicht, sondern aktiver Schutz für das eigene Unternehmen ist.

KRITIKALITÄT DER GESCHÄFTSPROZESSE ALS MAßSTAB

Eine Übersicht der Geschäftsprozesse und ihrer Kritikalität mit einhergehenden Schutzanforderungen für Verfügbarkeit, Vertraulichkeit und Integrität ermöglicht hierbei die Prüfung nach Kritikalität der Berechtigungen zu planen. Eine ganzheitliche Betrachtung von IT-Berechtigungen über alle eingesetzten Anwendungen und Systeme gewährleistet eine vollständige Trennung toxischer oder kritischer Berechtigungskombinationen.

Ist eine strikte Aufgabenteilung nicht möglich, kann im Einklang mit dem IAM ein Vier-Augen-Prinzip eingesetzt werden. Mehrstufige Genehmigungsverfahren, in welchen sichergestellt ist, dass Beantragung und Freigabe durch getrennte Personen erfolgen, gewähren auch bei Überschneidungen eine Freigabe und Prüfung von Berechtigungen frei von Interessenkonflikten. Das Gleichgewicht zwischen Genehmigungsverfahren mit Einbindung organisatorisch und technisch verantwortlicher Stellen sorgt für eine sichere Unternehmensstruktur.

TECHNISCHE IDENTITÄTEN NICHT VERGESSEN

Doch die Berechtigungen der Belegschaft stehen in Zeiten der Digitalisierung schon lange nicht mehr allein. Technische Benutzer und Schnittstellenzugänge bilden mit zunehmender Automatisierung ein weiteres Einfallstor für böswillige und fahrlässige Vorfälle. Die klare Zuordnung der technischen Identitäten zu fachlich Verantwortlichen und die Berücksichtigung dieser Identitäten im Rahmen der Steuerung und Überprüfung dienen dem Schutz des Unternehmens.

Eine klare Organisationsstruktur mit wiederverwendbaren Stellen und Berechtigungspaketen rund um die Geschäftsprozesse stellt nicht nur die Grundlage für das IAM dar, sondern bildet gleichzeitig die Basis für eine solide IT-Planung und Unternehmensstrategie. Geregelte Berechtigungsvergaben verhindern Fehler und schützen vor den Folgen, während regelmäßige Überprüfungen sicherstellen, dass Schwachstellen durch weitreichende Zugriffsrechte und Störungen durch fehlende Berechtigungen der Vergangenheit angehören.

Die Bündelung vergleichbarer Rechte in einheitlichen Stellen, Paketen und Rollen garantiert hierbei, dass auch umfangreiche Veränderungen – zum Beispiel durch den Einsatz neuer Systeme – einmalig erfasst werden und über die Organisationsstruktur den richtigen Personen zugeordnet werden.

STADTVERWALTUNG ALS BEISPIEL FÜR HETEROGENE STRUKTUREN

Gerade in Unternehmen mit umfangreichen und unterschiedlichen Aufgabenfeldern, von der Verwaltung bis zum Einsatz beim Kunden, liegen teilweise sehr unterschiedliche Berechtigungen vor. Am Beispiel einer Stadtverwaltung wird schnell erkennbar, dass für die verschiedenen Ämter – von der Schulverwaltung bis zur Pressestelle – ein gemeinsamer Umfang an Berechtigungen benötigt wird. Gleichzeitig unterscheiden sich die bereichsspezifischen Berechtigungen von der Führerscheinstelle über das Amt für Brand-, Zivilschutz und Rettungsdienst bis hin zum Büro des Bürgermeisters deutlich.

Während gewährleistet sein muss, dass alle Mitarbeiter der Kfz-Zulassungsstelle auf die Kfz-Daten zugreifen können und im Amt für Brand- und Zivilschutz auf Rettungspläne der ansässigen Unternehmen zugegriffen werden kann, steuert eine klare Organisationsstruktur, dass keine sensiblen Unternehmensdaten von Mitarbeitern der Zulassungsstelle aus den Systemen des Brand- und Zivilschutzes abgefragt werden können.

FAZIT

IAM ist kein einmaliges Projekt. Es begleitet jeden Unternehmensprozess und schützt alle Beteiligten. Geplante Vergaben, regelmäßige Überprüfungen, eine nachvollziehbare Berechtigungshistorie und die Einbindung aller Verantwortlichen – gemeinsam stellen diese Teile des Identity- und Access-Managements mit der richtigen Kombination aus Flexibilität, Organisation und Transparenz sicher, dass Unternehmen Audits zur IT-Sicherheit gelassen entgegensehen können. ■

ROLAND HEIN
ist Geschäftsführer der bit Informatik GmbH.

Berechtigungsmanagement: Die unterschätzte Herausforderung der digitalen Transformation

Bild: juststock/Getty Images

Wenn aus einfachen Zugriffsrechten ein Sicherheitsrisiko wird

Es ist Montagmorgen im IT-Support. Die neue Kollegin aus dem Vertrieb sollte arbeiten können, aber ihr fehlen die Zugriffe auf drei Systeme. Der Kollege aus der Produktion ist vor vier Wochen gewechselt, hat aber immer noch die Berechtigungen seiner alten Abteilung. Und die Rezertifizierung? Liegt zwischen Excel-Listen und einem halbfertigen Ticket.

So sieht die Realität in vielen Unternehmen aus. Solche Berechtigungsfehler führen zu Verzögerungen, Supportaufwand oder Sicherheitslücken. Nicht weil IT-Teams schlecht arbeiten, sondern weil klassische Ansätze mit der Dynamik moderner Organisationen nicht mehr Schritt halten können.

Das Dilemma: Sicherheit vs. Agilität

Die Anforderungen sind paradox: Berechtigungen sollen wasserdicht sein, aber nicht zur Bremse werden. Jede Änderung muss nachvollziehbar sein, ohne bürokratischen Overhead. Und natürlich Audit-sicher dokumentiert, idealerweise automatisch.

Viele IAM-Systeme versprechen das. In der Praxis: Die Implementierung dauert Monate, die Systeme sind überladen, und die IT arbeitet trotzdem manuell nach. Das größte Problem: Irgendwann driften Soll- und Ist-Zustand auseinander. Hier entsteht das eigentliche Sicherheitsrisiko.

Was moderne IAM-Lösungen anders machen

Der entscheidende Unterschied: Statt auf punktuelle Prüfungen zu setzen, vergleichen moderne Systeme kontinuierlich den Soll-Zustand mit der Realität und greifen bei Abweichungen automatisch ein. Wird ein Konto versehentlich verändert, stellt das System den korrekten Zustand eigenständig wieder her.

Automatisierte Workflows übernehmen Routineaufgaben: Rechtevergabe, Rezertifizierungen, Rollenwechsel oder Entzug ungenutzter Zugriffe. Standardisierte Profile sorgen dafür, dass neue Mitarbeitende vom ersten Tag an genau die Berechtigungen haben, die sie brauchen – versioniert, nachvollziehbar, revisionssicher.

Onboarding: Wo sich der Unterschied zeigt

Besonders beim Onboarding wird das Potenzial automatisierter Prozesse deutlich. Moderne Systeme setzen auf No-Code-Ansätze: Ein Ereignis im HR-System löst automatisch die passenden Workflows aus. Konten, Gruppen und Lizenzen werden auf Basis von Rolle, Abteilung und Standort erstellt.

Das Ergebnis: Neue Kolleg:innen sind ab dem ersten Arbeitstag produktiv, ohne dass die IT manuell tätig wird. Schnellere Bereitstellung, weniger Fehler, deutlich weniger Support-Tickets.

Praxisbeispiel: Integration, die funktioniert

Der BAYOOSOFT Access Manager zeigt, wie dieser Ansatz in der Praxis aussieht. Die Lösung dockt an Active Directory, Entra, HR-Systeme und Fachapplikationen an. Ändert sich das Organigramm oder das Rollenmodell, zieht das System nach – ohne Entwicklungszyklen und manuelle Nacharbeit.

Automatisierte Standardaufgaben und Self-Service-Funktionen reduzieren den operativen Aufwand spürbar. IT-Teams gewinnen Zeit für strategische Projekte, Fachbereiche bekommen Transparenz. Wichtig: Entwicklung und Support laufen vollständig in Deutschland, DSGVO-konform und nah an europäischen Regularien.

Fazit: Wenn Berechtigungsmanagement endlich einfach wird

Modernes IAM ist keine Frage der Feature-Liste, sondern der konsequenten Umsetzung. Der Unterschied: Soll und Ist werden kontinuierlich synchron gehalten, Prozesse nicht nur definiert, sondern automatisiert. Compliance entsteht als Ergebnis guter Automatisierung.

Das Ergebnis: maximale Sicherheit, volle Nachvollziehbarkeit und echte Effizienzgewinne genau da, wo es zählt. Und vielleicht das Wichtigste: IT-Teams, die endlich Zeit für das haben, was wirklich wichtig ist. ■

Mehr dazu hier

BAYOOSOFT
Kontaktinfos:
Europaplatz 5
64293 Darmstadt
+49 (0) 6151 - 86 18-700
info@bayoosoft.com
www.bayoosoft.com

BAYOOSOFT

secunet

When there are more bots than robots.

Industrie 4.0 braucht Premium-Cybersecurity.
Wir bieten das passende Set-up modernster Technologie. Von der Edge bis in die Cloud.

secunet macht souveräne Digitalisierung möglich.

secunet.com

Modularer GRC-Ansatz für IT-Sicherheit

bit Informatik erweitert GRC-Lösung für NIS-2-Compliance

Die bit Informatik GmbH aus Trier positioniert ihre Software bit-Compliance als modulare Lösung für Unternehmen mit kritischer Infrastruktur, die die Anforderungen der NIS-2-Richtlinie umsetzen müssen.

Mit bit-Compliance bietet die bit Informatik GmbH eine modulare Lösung für Governance, Risikomanagement und Compliance (GRC) an. Aufbauend auf mehreren Jahrzehnten Erfahrung mit den Anforderungen aus MaRisk und dem Digital Operational Resilience Act (DORA) an die Kredit- und Finanzwirtschaft, verfügt die Software ein ausgereiftes Set an Funktionen und Werkzeugen zur Bewältigung der NIS-2-Anforderungen von Unternehmen mit kritischer Infrastruktur (KRITIS). Neben der Finanzbranche nutzen staatliche Akteure wie Behörden und Verwaltungen, Krankenhäuser und Stadtwerke das Produkt.

Erfahrung und Flexibilität

Die Erfahrung der bit Informatik GmbH und die Flexibilität von bit-Compliance sind zwei ausschlaggebende Faktoren für den Einsatz der Lösung. Über drei Jahrzehnte hinweg hat die das Unternehmen das notwendige Know-how erarbeitet, um sicherzustellen, dass Anforderungen schnell und einfach umgesetzt werden können. Millionen Berechtigungen, Tausende Mitarbeiter und heterogene IT-Landschaften stellen mit bit-Compliance keine Hürde mehr dar.

Mit zehn flexibel konfigurierbaren Modulen bietet bit-Compliance eine passende Lösung für jede regulatorische Herausforderung. Dank der Unterstützung unterschiedlicher Datenbanksysteme und eines DSGVO-konformen On-Premises-Betriebs lässt sich die Browser-Anwendung bit-Compliance mit wenigen Handgriffen einsetzen. Der Fokus liegt hierbei stets auf den zu bewältigenden Herausforderungen, sodass Module und technische Schnittstellen je nach Bedarf eingesetzt und jederzeit erweitert werden können.

Workflow und Dokumentation

Ein umfangreiches Spektrum an Standardfunktionen – wie eine hochflexible Workflow-Engine mit integrierten Benachrichtigungs- und Eskalationsfunktionen – ermöglicht die Gestaltung individueller Prozesse. Unbegrenzte Bearbeitungsstufen sowie die Möglichkeit zur Steuerung der sichtbaren und bearbeitbaren Angaben je Bearbeitungsschritt leiten Anwender durch die Prozesse und beschränken die Bearbeitungsdauer auf das Wesentliche. Eine durchgehende Protokollierung sämtlicher Änderungen – über Verträge, Informationsverbundobjekte, Anweisungen, Notfallpläne, Berechtigungen und so weiter hinweg – führt zum Aufbau eines nachvollziehbaren Archivs – die Grundlage für erfolgreiche IT-Audits.

Automatisierte Prozesse für NIS-2-Umsetzung

Durch eine optimale Verknüpfung der Geschäftsprozesse, Verträge, Anwendungen et cetera wird die Umsetzung von NIS-2 erleichtert. bit-Compliance erkennt automatisiert Änderungen mit Auswirkungen auf andere Objekte und generiert entsprechende Vorlagen. Regelmäßige Überprüfungen, etwa Business-Impact-Analysen zur Bestimmung kritischer Geschäftsprozesse, werden automatisch angestoßen und verteilt. Die zuständigen Bearbeiter werden per E-Mail sowie direkt in der Anwendung informiert und können die Auslöser der Veränderungen nachvollziehen.

Bild: decorator | Jubxvect - stock.adobe.com

Schnittstellen zu Drittsystemen übernehmen wiederkehrende Routinearbeiten und entlasten so die Fachkräfte. Automatisierte Berechtigungsveränderungen in Active Directory, Teams oder Microsoft Entra erhöhen hierbei nicht nur die Effizienz, sondern reduzieren gleichzeitig die Fehlerquote durch den Wegfall manueller Übertragungen.

Die bit Informatik GmbH steht durchgehend mit ihren Kunden und Partnern im Austausch und behält Veränderungen der nationalen und europäischen Anforderungen im Blick. Erforderliche Anpassungen werden zeitnah in die Software integriert, damit sich Kunden auf die Umsetzung fokussieren können. Von der Datenschutz-Grundverordnung (DSGVO) und der NIS-2-Richtlinie bis zum AI-Act – die bit Informatik stellt Umsetzungshilfen bereit.

Beratung und Datenübernahme aus Altsystemen

Beim Einsatz von bit-Compliance unterstützen Experten für Datenanalyse und -aufbereitung die Überführung von Daten aus Altsystemen. Dabei werden verschiedene Stände aus unterschiedlichen Quellen abgeglichen und zusammengeführt. Erfahrene Berater begleiten bei der Anpassung der Standardfunktionalität an die Unternehmensanforderungen und greifen hierbei auf Praxiserfahrungen aus verschiedenen Branchen zurück.

Unternehmen, die bereits unterschiedliche (Excel-)Lösungen für verschiedene Problemstellungen rund um Notfall-, Berechtigungs-, Drittparteien- und Infrastrukturmanagement im Einsatz haben und nicht wieder bei

Null beginnen möchten, erhalten Unterstützung: Die bit Informatik GmbH übernimmt die Analyse und Aufbereitung und bit-Compliance unterstützt anschließend bei der regelmäßigen und anlassbezogenen Prüfung.

Made in Germany

Mit Sitz in Trier bietet die bit Informatik eine in Deutschland entwickelte Lösung für GRC-Anforderungen. Neben dem klassischen Support per E-Mail und Telefon schult und berät das Team der bit Informatik GmbH sowohl digital als auch vor Ort. Dabei stellt die bit Informatik GmbH als IKT-Dienstleister rund um Datenschutz, IT-Sicherheit, Revision, Notfallmanagement und Nachhaltigkeit alle erforderlichen Berichte zur Verfügung, um eine transparente Dienstleistersteuerung zu ermöglichen. Mit einer IDW-PS-880-Zertifizierung wird zudem nachgewiesen, dass sämtliche technische und fachliche Anforderungen von bit-Compliance fachgerecht umgesetzt werden. ■

Weitere Informationen zur Anwendung bit-Compliance:

Interessierte können eine unverbindliche Präsentation der relevanten Module unter **info@bit-Informatik.de** vereinbaren oder sich über die verfügbaren Module unter **www.bit-informatik.de** informieren.

Mehr dazu hier

bit Informatik GmbH
Geschäftsführer Herr Roland Hein
Am Wissenschaftspark 32
54296 Trier

Tel.: +49 651 966 29-0
E-Mail: info@bit-informatik.de

bit-Compliance

Einklang zwischen Sicherheit, Compliance und Benutzerfreundlichkeit

Relevante Puzzleteile eines modernen Identitätsmanagements in Unternehmen

Digitale Identitäten stehen im Zentrum nahezu aller modernen Geschäftsmodelle. Ihre sichere und effiziente Verwaltung entwickelt sich zunehmend zur Herausforderung für Unternehmen und öffentliche Einrichtungen. Wer Nutzer zuverlässig authentifizieren will, muss sensible Informationen schützen und gleichzeitig eine reibungslose Anwendererfahrung ermöglichen. Vor allem im Customer Identity and Access Management (CIAM) spielen deshalb zukunftsfähige Authentifizierungsverfahren eine Schlüsselrolle: Sie helfen, Sicherheitsrisiken zu minimieren und das Nutzererlebnis spürbar zu verbessern.

Die Anforderungen an das Identitäts- und Zugriffsmanagement sind vielfältiger denn je, während sich die aktuelle Bedrohungslage dynamisch weiterentwickelt. Somit ist es für Unternehmen essenziell, ihre Authentifizierungsstrategien kontinuierlich zu überprüfen und entsprechend zu adaptieren. Damit dies sicher gelingen kann, braucht es Klarheit über die wichtigsten Herausforderungen und Trends im IAM-Umfeld. Nur so lässt sich erkennen, welche Fähigkeiten ein CIAM-System von morgen bereits heute bieten muss.

Digitale Identitäten: Vielfalt und Verantwortung

Die Zahl digitaler Identitäten wächst exponentiell, und längst sind es nicht mehr nur menschliche Nutzer. Non-Human Identities (NHI) wie IoT-Geräte, Microservices oder KI-Agenten agieren als privilegierte Entitäten und benötigen ein ebenso stringentes Identitäts- und Zugriffsmanagement. Studien sprechen von einem Verhältnis von 1:50 zwischen Human und Non-Human Identities. Die Herausforderung: Transparenz, Lifecycle-Management und sichere Authentifizierung trotz fehlender biometrischer Merkmale, dafür mit Zertifikaten, Token und automatisierter Rotation. Gleichzeitig explodiert die Vielfalt an Identity Providern (IdP). Unternehmen müssen mit lokalen Directories, Cloud-Diensten, Behördenportalen und Wallet-basierten Identitäten wie EUDI oder E-ID umgehen. Ohne Multi-IdP-Fähigkeit drohen Brüche in der User Journey, regulatorische Hürden und Sicherheitslücken.

Neue Bedrohungen: Phishing, KI und Quantencomputing

Cyberkriminelle nutzen die Komplexität der Authentifizierung gezielt aus. Phishing bleibt dabei das Einfallstor Nummer eins. KI-gestützte Angriffe simulieren biometrische Merkmale, lösen Captchas und generieren täuschend echte Phishing-Mails. Gleichzeitig entstehen durch Schatten-IT und unkontrollierte Nutzung von KI-Tools neue Risiken innerhalb der Organisation. Auch das Quantencomputing stellt eine reale Bedrohung dar. Der Shor-Algorithmus kann klassische Verschlüsselung wie RSA oder ECC in Minuten brechen. Angreifer speichern heute verschlüsselte Daten, um sie später zu entschlüsseln. Unternehmen sind somit dringend angehalten, ihre Infrastruktur auf Post-Quanten-Kryptografie (PQC) vorzubereiten. Hybride Modelle, algorithmische Agilität und NIST-konforme Standards sind hier von entscheidender Bedeutung.

Sicherheit trifft Benutzerfreundlichkeit

Technische Komplexität darf nicht zulasten der Nutzerfreundlichkeit gehen. Denn was nützt höchste Sicherheit, wenn Kunden und Mitarbeitende Prozesse abbrechen oder umgehen? Moderne CIAM-Systeme benötigen daher adaptive Authentifizierungsverfahren: Sicherheitsstufen werden kontextsensitiv angepasst, zusätzliche Prüfungen nur bei erhöhtem Risiko durchgeführt.

Passwortlose Verfahren wie FIDO2 bieten eine elegante Lösung. Sie sind Phishing-resistent, geräteübergreifend nutzbar und verbessern die User Experience signifikant. Doch auch FIDO2 stößt an Grenzen – etwa bei Maschinenidentitäten oder Legacy-Systemen. Eine starke Orchestrierung, flexible Flows und fallback-fähige Alternativen sind daher unverzichtbar, um Sicherheit und Usability zu vereinen.

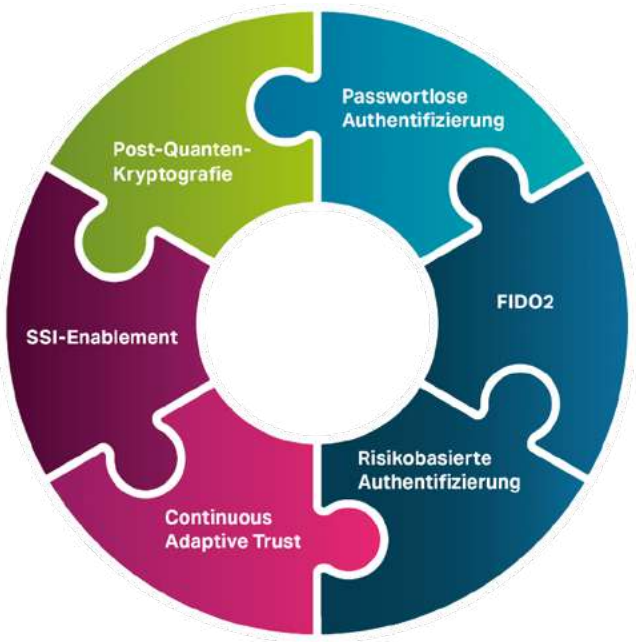
SSI-Enablement: Die Zukunft beginnt jetzt

Mit der Einführung der Europäischen Digitalen Identität (EUDI) und Self-Sovereign Identity (SSI) entstehen neue Vertrauensmodelle. Nutzer behalten die Kontrolle über ihre Daten, Unternehmen müssen sich auf dezentrale Identitätsnachweise einstellen. SSI ermöglicht rechtsverbindliche Transaktionen ohne zentrale Register – ein Paradigmenwechsel, der CIAM-Systeme vor neue Aufgaben im SSI-Enablement stellt und ein ganzheitliches, agiles Prozessverständnis verlangt.

„Puzzeln mit Methode": Airlock als strategischer Partner

Der Security-Experte Airlock bietet eine Plattform, die weit über klassische IAM-Funktionalität hinausgeht und aktuellen wie künftigen Herausforderungen konsequent Rechnung trägt. Besondere Stärke beweist die Architektur dabei vor allem in der methodischen Zusammensetzung verschiedensten Security-Komponenten und Services zu einem konsistenten, flexiblen Sicherheitsmodell. Die Plattform ist modular aufgebaut und erlaubt es, Sicherheitsbausteine wie Web Application Firewall, API-Security, Identity and Access Management, Anomaly Detection und WAAP nicht nur nebeneinander zu betreiben, sondern sie funktional und logisch miteinander zu verzahnen.

Für maximale Flexibilität im Einsatz basiert die Lösung von Airlock auf einem mehrschichtigen Sicherheitsmodell, das sich bedarfsgerecht an die Anforderungen unterschiedlicher IT-Landschaften anpasst – ob On-Premises, hybrid oder vollständig cloudbasiert. Containerisierte Anwendungen lassen sich ebenso integrieren wie klassische Backend-Systeme.



Im Zuge steigender Anforderungen müssen unterschiedlichste Puzzleteile sinnvoll zusammengesetzt werden.

Dabei steht nicht nur die technische Interoperabilität im Vordergrund, sondern auch die strategische Skalierbarkeit: Unternehmen können neue Sicherheitsmechanismen schnell etablieren, bestehende Prozesse flexibel anpassen und regulatorische Anforderungen zuverlässig erfüllen. Ein zentrales Element dieser Methodik ist die Fähigkeit zur dynamischen Risikoanalyse. Über konfigurierbare Authentifizierungsflüsse, fein steuerbare Trust-Scores und kontinuierliche Verhaltensanalysen entsteht eine adaptive Umgebung. Somit können Unternehmen zügig auf neue Bedrohungslagen und Nutzungsmuster reagieren. Gleichzeitig bleibt die Benutzerfreundlichkeit gewahrt – durch kontextbasierte Authentifizierung, passwortlose Verfahren und Self-Service-Funktionen, die den Helpdesk entlasten und die Akzeptanz auf Anwenderseite erhöhen.

Praxisbeispiele zeigen die Leistungsfähigkeit:

- **Johanniter-Unfall-Hilfe** nutzt Airlock für flexible Authentifizierungsflüsse mit über 60.000 Mitarbeitenden. Unterschiedliche Compliance-Vorgaben werden zuverlässig erfüllt.
- **Frankfurter Bankgesellschaft** ersetzte RSA-Token durch passwortlose OneTouch-Authentifizierung.
- **Schweizerische Bundesbahnen** integrieren hunderte Serviceanbieter über Token Exchange. Segmentierung und zentrale Steuerung sorgen für Skalierbarkeit und Sicherheit für über fünf Millionen Anwender.

„Puzzeln mit Methode" bedeutet bei Airlock also nicht nur technologische Vielfalt, sondern vor allem strategische Kohärenz. Jede Komponente erfüllt eine klar definierte Aufgabe im Gesamtsystem und trägt dazu bei, digitale Identitäten sicher, effizient und benutzerfreundlich zu verwalten. Airlock Secure Access Hub liefert somit ein agiles Fundament für digitale Souveränität, regulatorische Konformität und nachhaltige Innovationsfähigkeit. ■

Im Whitepaper *„Die Puzzleteile moderner Authentifizierung"* werden die Herausforderungen, denen die Verantwortlichen für Identitäts- und Zugriffsmanagement gegenüberstehen, im Detail beschrieben. Zudem liefert das Whitepaper konkrete Handlungsempfehlungen zur Umsetzung moderner Authentifizierungsprozesse. Unternehmen erhalten hilfreiche Tipps, worauf bei der Auswahl einer geeigneten Lösung unbedingt geachtet werden sollte.

Zum kostenlosen Download:

Mehr dazu hier

AIRLOCK®
SECURE ACCESS HUB

Schwachstelle Identitäten:

Warum Zero Trust ohne intelligentes Identity-Management nicht funktioniert

Viele Zero-Trust-Initiativen scheitern am Identitätsmanagement. Ohne zentrale Steuerung lassen sich Berechtigungen kaum nachvollziehen und Risiken nur schwer erkennen. Gerade in hybriden IT-Umgebungen sind durchgängige Prozesse für die Provisionierung, Authentifizierung und Überwachung von Benutzerkonten entscheidend, um Sicherheitslücken zu vermeiden. Moderne Identity-und-Access-Management-(IAM)-Lösungen wie ManageEngine AD360 automatisieren die Verwaltung von Identitäten, ermöglichen eine kontextabhängige Authentifizierung und setzen Sicherheitsrichtlinien konsequent um. So schaffen sie die Basis für eine konsistente Zero-Trust-Strategie.

Identitäten sind das Herzstück jeder Zugriffskontrolle - und damit ein entscheidender Faktor für den Erfolg einer Zero-Trust-Strategie. Nur wenn bekannt ist, wer unter welchen Bedingungen auf welche Ressourcen zugreift, lassen sich Risiken zuverlässig steuern.

Ein leistungsfähiges IAM schafft dafür die notwendige Transparenz und Kontrolle. Es bildet die Grundlage, um Benutzerkonten konsistent zu verwalten, Berechtigungen rollenbasiert zu vergeben und Zugriffe kontinuierlich zu überwachen. Ein IAM-System sollte dafür automatisierte Identitätsprozesse, kontextabhängige Zugriffskontrollen, eine adaptive Multi-Faktor-Authentifizierung (MFA) sowie umfassendes Auditing bieten.

ManageEngine AD360 vereint all diese Funktionen in einer Plattform und hilft IT-Teams, Access Management und Identitätssicherheit in hybriden Umgebungen weitestgehend zu automatisieren. So wird aus manuellem Verwaltungsaufwand ein zentraler Sicherheitsmechanismus – und Identitätsmanagement zum Fundament jeder Zero-Trust-Architektur.

Automatisiertes Identity Lifecycle Management über Systemgrenzen hinweg

Werden Benutzerkonten manuell erstellt, geändert oder gelöscht, sind Fehler – und im schlimmsten Fall Sicherheitslücken – vorprogrammiert. AD360 eliminiert diese manuellen Schritte: Identitäten lassen sich über den gesamten Lebenszyklus hinweg automatisiert verwalten – von der Erstellung bis zur Deprovisionierung. Auch das Gewähren oder Widerrufen von Zugriffsrechten kann über ereignisgesteuerte Automatisierungsrichtlinien ohne manuelle Eingriffe erfolgen.

Mithilfe zentraler, individuell anpassbarer Vorlagen lassen sich Benutzerkonten und Postfächer in Active Directory, Microsoft 365, Exchange Server und Google Workspace konsistent anlegen und synchronisieren. Durch die Integration von HR-Systemen wird das On- und Offboarding neuer Mitarbeitender zusätzlich vereinfacht. Gleichzeitig sorgt AD360 für konsistente Zugriffsrichtlinien, die sicherstellen, dass Nutzer nur die Berechtigungen

erhalten, die sie für ihre jeweilige Rolle benötigen – ein zentraler Schritt hin zu einer konsequent umgesetzten Zero-Trust-Strategie.

Adaptive Authentifizierung und flexible Zugriffssteuerung

Starke Authentifizierungsmechanismen gehören zu den wichtigsten Säulen von Zero Trust. AD360 unterstützt 19 Authentifizierungsmethoden, darunter biometrische Verfahren, Hardware-Token und zeitbasierte Einmalpasswörter (Time-based one-time password, TOTP). Administratoren können Richtlinien definieren, die sich an Benutzergruppen, Gerätekontext oder Standort orientieren – beispielsweise, um bei ungewöhnlichen Anmeldeversuchen automatisch zusätzliche Faktoren anzufordern.

Mit der adaptiven Multi-Faktor-Authentifizierung lässt sich das Sicherheitsniveau dynamisch anpassen, ohne die Benutzerfreundlichkeit zu beeinträchtigen. Ergänzend sorgt Single Sign-on (SSO) für einen komfortablen Zugriff auf lokale und Cloud-Anwendungen, während Richtlinien sicherstellen, dass jede Anmeldung den vorgegebenen Sicherheitsstandards entspricht.

Früherkennung durch User Behavior Analytics

Ein entscheidender Bestandteil von AD360 ist die User Behavior Analytics (UBA), die auf Machine Learning (ML) basiert. Dazu analysiert die Lösung typische Nutzeraktivitäten, erstellt ein Profil des normalen Verhaltens und erkennt Abweichungen automatisch – etwa eine ungewöhnlich hohe Zahl von Dateiabrufen oder Anmeldeversuche außerhalb der Arbeitszeiten.

Mithilfe von Echtzeit-Benachrichtigungen lassen sich Insider-Bedrohungen und kompromittierte Konten frühzeitig erkennen, bevor Schaden entsteht. Durch die Kombination von ML-gestützter Analyse, adaptiver Authentifizierung und Echtzeit-Auditing bietet AD360 eine Sicherheitsarchitektur, die Angriffe aktiv erkennt und auf Anomalien reagiert.

Transparenz und Kontrolle durch Auditing und Reporting

Eine Zero-Trust-Strategie endet nicht bei der Authentifizierung – sie setzt kontinuierliches Monitoring voraus. AD360 bietet dazu detaillierte Auditing- und Reporting-Funktionen, mit denen sich alle Änderungen an Benutzerkonten, Gruppenmitgliedschaften und Berechtigungen nachvollziehen lassen.

Echtzeitbenachrichtigungen informieren über sicherheitsrelevante Ereignisse wie das Anlegen privilegierter Konten oder das Ändern kritischer Gruppenrechte. Darüber hinaus stehen vorkonfigurierte Compliance-Berichte für Standards wie die Datenschutzgrundverordnung (DSGVO), den Sarbanes-Oxley Act (SOX) oder den Payment Card Industry Data Security Standard (PCI DSS) zur Verfügung. So können Unternehmen Sicherheitsvorfälle schneller erkennen, Richtlinienverstöße dokumentieren und Audits effizient vorbereiten.

Fazit: Kontrolle über Identitäten als Voraussetzung für Zero Trust

Zero Trust setzt ein Identitätsmanagement voraus, das weit über klassische Benutzerverwaltung hinausgeht. Nur wenn Identitäten konsequent verwaltet, Berechtigungen dynamisch gesteuert und Zugriffe kontinuierlich überwacht werden, lässt sich Sicherheit wirksam durchsetzen.

Mit ManageEngine AD360 steht Unternehmen eine Plattform zur Verfügung, die genau diese Anforderungen erfüllt – von der automatisierten Provisionierung über adaptive Authentifizierung bis hin zur ML-basierten Anomalie-Erkennung. Damit wird Identitätsmanagement zu einem aktiven Bestandteil der Sicherheitsarchitektur – und Zero Trust von der Strategie zur gelebten Praxis. ■

Digital Onboarding – Agilität kann man auch outsourcen

Mit externer Hilfe beim Digital Onboarding zu mehr Agilität und Flexibilität bei der Neukundengewinnung

Viele Unternehmen setzen zur Abwicklung ihrer Neukundengewinnung mittlerweile auf digitale Onboarding-Verfahren. Längst nicht immer bringen ihnen ihre Bemühungen aber auch den erhofften Erfolg. Nicht selten bleiben die Konversionsraten hinter den Erwartungen zurück. Zu viele potenzielle Neukunden brechen das Onboarding vorzeitig ab, da der Prozess sich zu sehr in die Länge zieht, zu kompliziert gestaltet ist oder Beschränkungen ihrer technischen Ausstattung nicht ausreichend berücksichtigt – kurz: ihnen einfach nicht ausreichend Optionen bei der Auswahl eines für sie passenden Verfahrens bietet. Um bei der Neukundengewinnung maximal erfolgreich zu sein, benötigen Unternehmen ein möglichst flexibles und breites Onboarding-Verfahrensportfolio, aus dem ihre potenziellen Kunden ein für sie geeignetes Verfahren auswählen können. Die beste Möglichkeit dazu stellt das Outsourcing des Digital Onboardings an einen spezialisierten Anbieter mit möglichst breiter Verfahrenspalette dar.

Autor: Bernt Vossebein,
CEO von POS Solutions, A PROCILON COMPANY

Digitales Onboarding ermöglicht es potenziellen Neukunden, sich bequem und schnell bei einem Unternehmen zu registrieren sowie für einen Dienst anzumelden oder ein Produkt zu erwerben. Ausgestattet mit einer geeigneten Auswahl von Digital-Onboarding-Verfahren können Unternehmen ihre Neukundengewinnung deutlich optimieren. Doch muss die genutzte Onboarding-Lösung, um den erhofften Erfolg zu bringen, neben einer einfachen und hohen Skalierbarkeit und einer möglichst nahtlosen und einfachen Integration in die bestehenden Customer-Relationship-Management-(CRM-) Systeme auch ein immer entscheidenderes Feature beinhalten: Sie muss es Unternehmen ermöglichen, ihre Onboarding-Verfahren möglichst flexibel zu handhaben. Intern – viele kleine und mittlere Unternehmen (KMU) sowie Großunternehmen stellen dies gerade fest – lässt sich diese Fähigkeit in aller Regel nur schwer und verbunden mit erheblichen Kosten realisieren. Immer mehr Unternehmen gehen deshalb mittlerweile dazu über, hier auf Lösungen spezialisierter externer Anbieter zu setzen. Unter Zuhilfenahme modular aufgebauter Plattformlösungen können diese die für eine erfolgreiche Digital-Onboarding-Architektur erforderliche Flexibilität und Agilität realisieren – ohne den Unternehmen dabei etwas von ihrer Souveränität zu nehmen.

Warum sich Flexibilität und Agilität beim Digital Onboarding auszahlen

Flexibilität und Agilität werden für ein erfolgreiches und Compliance-konformes Digital Onboarding dringend benötigt – etwa um eine zufriedenstellende Customer Experience zu generieren. Neukunden haben unterschiedliche Bedürfnisse, Produktwünsche und technische Ausstattungen. Eine agile Onboarding-Architektur ermöglicht es Unternehmen, genau darauf einzugehen und den Onboarding-Prozess an spezifische gesetzliche Rahmenbedingungen, Kundensegmente, Nutzungsfälle und Endgerätpräferenzen anzupassen. Dies sorgt für eine höhere Conversion

Rate und eine kürzere Time-to-Value. Oder um Onboarding-Verfahren an Umstellungen im Geschäftsmodell sowie Produkt- und Serviceupdates anzupassen. Oft müssen hier einzelne Schritte, Instruktionen und Informationen nachjustiert werden. Ein weiteres Einsatzgebiet: Kommen neue, passendere Onboarding-Verfahren auf den Markt, sollen sie so schnell wie möglich in das bestehende Portfolio integriert werden können. Oder: Es gibt Änderungen in der Applikationswelt des Unternehmens (CRM, DMS, ERP etc.). Anpassungen der Onboarding-Verfahren werden erforderlich, um weiterhin eine nahtlose Integration und Investitionssicherheit gewährleisten zu können. Schließlich kommt es auch bei den gesetzlichen Rahmenbedingungen, bei Datenschutz- und Compliance-Anforderungen immer wieder zu Anpassungen und Änderungen. Um in all diesen Fällen möglichst rasch die gewünschte Justierung vornehmen zu können, ist die Sicherstellung einer ausreichenden Agilität der Onboarding-Architektur zwingend erforderlich.

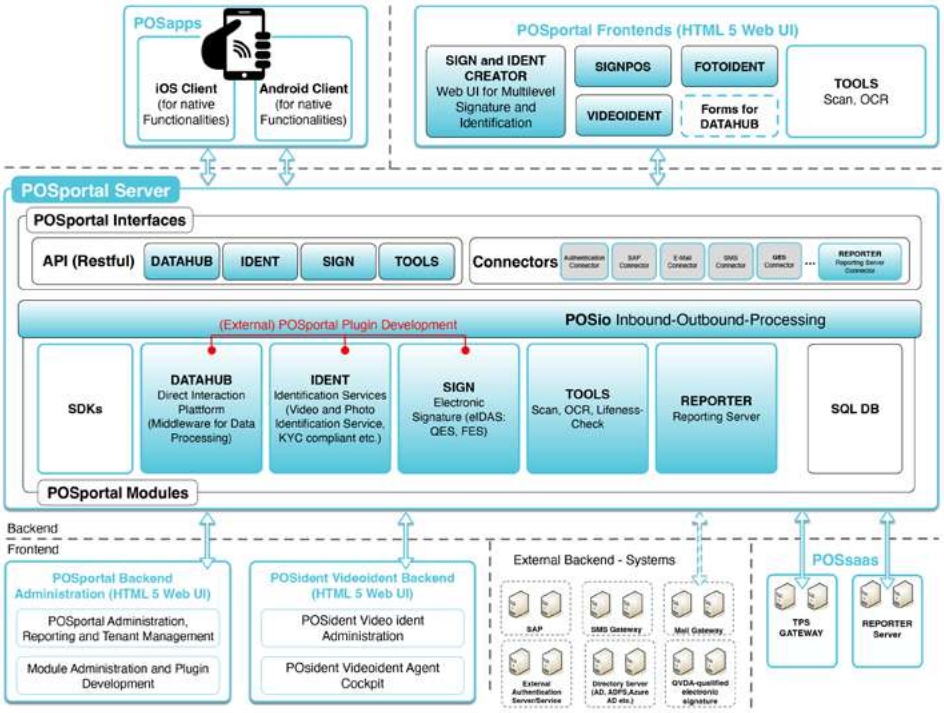


Schaubild: *Beispiel für eine agile, Compliance-konforme Digital Onboarding-Architektur, die über einen externen Onboarding-Spezialisten bezogen werden kann (Quelle: POS Solutions, A PROCILON COMPANY)*

Moderne externe Digital-Onboarding-Lösungen – modular und doch aus einem Guss

Genau die lässt sich mit einer modernen externen Onboarding-Lösung schnell und unkompliziert realisieren. Moderne externe Onboarding-Lösungen sind als modular aufgebaute Plattformlösungen konzipiert. Über eine offene API/SDK-Schnittstelle lassen sich die Plattformen schnell und unkompliziert an die eigenen CRM-Systeme und den übrigen Tech-Stack anbinden – was die Time-to-Market sowie die Kosten eines Onboardings erheblich reduziert. Ihr modulares Baukasten-Prinzip ermöglicht es Anwendern, sich einzelne Services, Funktionen und Produkte genauso zusammenzustellen, wie sie sie für einen spezifischen Anwendungsfall benötigen. Zur Auswahl stehen:

- **Methoden zur Datenpersistierung –** für eine strukturierte Datenerfassung, -verteilung und -abfrage
- **Identifikationsmethoden –** zur rechtskonformen digitalen Identifizierung via Foto-Ident-, Video-Ident-, Access-to-Account- und E-Ident-Verfahren
- **E-Signatur-Methoden –** zur rechtskonformen digitalen Signierung mit fortgeschrittenen und qualifizierten elektronischen Signaturen gemäß eIDAS
- **Reporting- und Monitoring-Services –** zur vollständigen Überwachung und Berichterstattung aller Onboarding-Verfahren
- **Zusatzfunktionalitäten –** über die API-Schnittstelle lassen sich weitere Funktionen integrieren, etwa zusätzliche Scans von Dokumenten, eine Optical Character Recognition (OCR) oder auch ein Liveness-Check

Einmal integriert können die gewählten Onboarding-Bausteine und -Services bei Bedarf schnell und unkompliziert abgeändert werden – ohne dass es hierzu erforderlich wird, selbst Code zu generieren oder das Hauptprodukt zu deployen. Dadurch können auch Mitarbeiter der Marketing- oder einer Produkt-Abteilung die erforderlichen A-/B-Tests und Optimierungsschritte übernehmen. Alle zur Verfügung stehenden Identifikations- und Signatur-Verfahren sind EU-weit rechtskonform – etwa im Hinblick auf eIDAS, KYC, GWG, AML und DSGVO. Eine moderne Onboarding-Plattform kann damit die erforderlichen Trusted-Services, wie sie in stark regulierten Branchen – etwa der Finanz- und Gesundheitsbranche – vorgeschrieben sind, problemlos zum Einsatz bringen.

Externe modular aufgebaute Plattformlösungen schaffen genau die Agilität und Flexibilität, die Unternehmen beim Onboarding benötigen, um zielgerichtet zu den für sie richtigen Onboarding-Verfahren zu gelangen und diese kontinuierlich zu optimieren. Um in der heutigen dynamischen Onboarding-Landschaft erfolgreich zu bestehen, um den eigenen Erfolg bei der Neukundengewinnung zu maximieren, sind sie die derzeit wohl beste Wahl.

Sie möchten sich gern einmal persönlich mit dem vollen Einsatzpotenzial einer externen Onboarding-Plattform für Ihr Unternehmen vertraut machen? Nehmen Sie hier Kontakt zu uns auf und buchen Sie einen Termin für einen Test. Gern helfen wir Ihnen, die für Sie passenden Onboarding-Verfahren und -Module zu ermitteln. ■

Mehr dazu hier

A PROCILON COMPANY

Ohne Runtime-Einblicke bleibt Sicherheit Stückwerk

CLOUD-NATIVE SECURITY: WARUM LAUFZEITSICHTBARKEIT ENTSCHEIDEND IST

Container, Kubernetes und serverlose Architekturen fördern Agilität und Effizienz, vergrößern aber auch die Angriffsflächen. Klassische Sicherheitsmodelle stoßen hier an ihre Grenzen. Der Schlüssel zu mehr Resilienz liegt in der Laufzeitsichtbarkeit: Sie macht Angriffe und Fehlverhalten dort sichtbar, wo sie entstehen – im laufenden Betrieb. Dadurch lassen sich Risiken nicht nur identifizieren, sondern nach Relevanz bewerten und gezielt entschärfen. Erst wer versteht, was wirklich passiert, kann wirksam schützen – und Sicherheitsstrategien an die Dynamik moderner Umgebungen anpassen.

Mit der zunehmenden Nutzung von Containern, Kubernetes und serverlosen Architekturen wächst nicht nur das Tempo der Softwareentwicklung, sondern auch die Komplexität der IT-Umgebungen. Sicherheitsteams stehen vor der Aufgabe, dynamische, teils hybride Landschaften zu überwachen, Warnmeldungen zu priorisieren und Systeme zu schützen, die sich laufend verändern. Die entscheidende Frage lautet daher längst nicht mehr, wie sich Risiken frühzeitig erkennen lassen, sondern wie man sie in Echtzeit bewerten und wirksam eindämmen kann.

Cloud-Native Application Protection Platforms (CNAPPs) gelten in der Branche als eine Möglichkeit, diese Lücke zu schließen, indem sie Sichtbarkeit, Compliance-Überwachung, Bedrohungserkennung und Incident Response in einer integrierten Umgebung bündeln. Der entscheidende Unterschied zu bisherigen Ansätzen liegt dabei in der Konzentration auf Runtime-Daten.

VOM RAUSCHEN ZUR RELEVANTEN INFORMATION

Über viele Jahre stützte sich Cloud-Sicherheit vor allem auf präventive Maßnahmen wie Code-Scans, Konfigurationsprüfungen oder Compliance-Kontrollen. Diese bleiben wichtig, erfassen jedoch nur einen Teil der Realität. Sie weisen auf mögliche Schwachstellen hin, sagen aber nichts darüber aus, ob diese im laufenden Betrieb tatsächlich ausgenutzt werden oder überhaupt relevant sind.

Hier setzt die Laufzeitsichtbarkeit an: Sie zeigt, welche Workloads tatsächlich aktiv sind und wie sie sich im Betrieb verhalten. So erhalten Sicherheitsteams belastbare Anhaltspunkte, um Bedrohungen richtig einzuordnen und gezielt zu priorisieren. Der Laufzeitkontext liefert Antwor-

ten auf zentrale Fragen: Ist eine Schwachstelle in einer laufenden Workload überhaupt erreichbar? Entsteht durch eine Fehlkonfiguration ein realer Angriffsweg? Wird eine Workload aktuell aktiv ausgenutzt?

Ohne diesen Einblick riskieren Unternehmen, Fehlalarmen hinterherzulaufen, während echte Angriffe unbemerkt bleiben. Laufzeitsichtbarkeit schafft hier Klarheit: Sie trennt Wichtiges von Unwichtigem, reduziert überflüssigen Alarmverkehr und hilft, die tatsächliche Angriffsfläche deutlich zu verkleinern.

VON PRÄVENTION ZU PRIORISIERUNG

Moderne Unternehmen sehen sich einer Flut von Warnmeldungen ausgesetzt – von Schwachstellenscannern über Cloud-Posture-Tools bis hin zu Application-Security-Plattformen. Die schiere Menge ist kaum noch zu bewältigen. Sicherheitsteams verbringen oft mehr Zeit damit, Meldungen zu prüfen und zu priorisieren, als tatsächliche Schwachstellen zu beheben.

Wirksam wird Sicherheit jedoch erst, wenn Schwachstellen und Fehlkonfigurationen eindeutig zugeordnet werden:

- zu den Workloads, die tatsächlich im Betrieb laufen;
- zu den Geschäftsanwendungen, die sie tragen;
- zu den Teams, die für die Behebung verantwortlich sind.

Diese Transparenz ist entscheidend, um die Lücke zwischen Sicherheits- und Entwicklungsteams zu schließen. Für Entwickler wirken viele Befunde ohne Kontext wie Störfaktoren; Sicherheitsteams wiederum fehlt oft der Überblick über Zuständigkeiten und tatsächliche Auswirkungen. Laufzeitsichtbarkeit liefert den gemeinsamen Kontext: Sie ermöglicht eine gezielte Priorisierung, sodass die richtigen Teams die relevanten Probleme zum richtigen Zeitpunkt beheben können.

KÜNSTLICHE INTELLIGENZ ALS VERSTÄRKER

Selbst bei klaren Prioritäten bleibt die Größe und Dynamik moderner Cloud-Umgebungen eine Herausforderung. Zunehmend rückt hier auch künstliche Intelligenz (KI) in den Fokus – sie soll nach Einschätzung vieler Anbieter das Verständnis und die Funktionsweise von CNAPPs grundlegend verändern.

KI entlastet Sicherheitsteams auf drei Ebenen:

- **Signal-Korrelation:** Ereignisse aus Logs, Netzwerkverkehr und Workload-Verhalten werden zusammengeführt, sodass sich versteckte Angriffskampagnen erkennen lassen.
- **Reduktion von Fehlalarmen:** Mustererkennung und Sprachmodelle filtern irrelevante Meldungen heraus und machen nur die wirklich wichtigen sichtbar.
- **Beschleunigte Reaktion:** Automatisierte Analysen schlagen konkrete Gegenmaßnahmen vor oder leiten in definierten Low-Risk-Szenarien selbst Schritte ein.

Besonders wertvoll ist die Fähigkeit von KI-gestützten Systemen, komplexe Angriffsmuster durch mehrstufige Schlussfolgerungen zu erkennen – oft mit Ergebnissen, die klassischen Tools entgehen. Für überlastete Security Operations Center bedeutet das kürzere Reaktionszeiten und weniger Fehlalarme.

Die Technologie ersetzt dabei keine Sicherheitsteams, verändert aber deren Arbeitsweise grundlegend. Statt im Rauschen unzähliger Alerts zu versinken, können sich Analysten auf die wirklich wichtigen Vorfälle konzentrieren und fundierte Entscheidungen in deutlich kürzerer Zeit treffen.

VERANTWORTUNG UND ZUSAMMENARBEIT

Ein weiteres Kernproblem vieler Organisationen ist die unklare Verantwortlichkeit. Sicherheitswarnungen entfalten nur dann Wirkung, wenn sie beim richtigen Team ankommen – und zwar mit dem nötigen Kontext. In der Praxis bleibt jedoch häufig offen, wer sich tatsächlich um eine Schwachstelle kümmern muss.

Darum ist es entscheidend, die Meldungen eindeutig auf Quellcode, Zuständigkeiten und den Einsatzkontext zurückzuführen. So lassen sich Schwachstellen, die im Betrieb sichtbar werden, direkt dem verantwortlichen Team zuordnen. Sicherheit kann dadurch stärker als gemeinsame Aufgabe aller Beteiligten verstanden werden – und nicht zu einer isolierten Last einzelner Abteilungen.

Partnerschaften und Integrationen spielen dabei eine zentrale Rolle. Wenn Sicherheitsplattformen mit Anbietern von Codeanalyse- oder Application-Security-Testing-Lösungen zusammenarbeiten, lassen sich Laufzeitschwachstellen direkt dem zugrunde liegenden Quellcode zuordnen. Das verringert den Abstimmungsaufwand und beschleunigt die Behebung deutlich, zumindest in der Theorie.

KONSOLIDIERUNG IST UNVERMEIDLICH

Viele Unternehmen setzten lange auf Best-of-Breed-Ansätze – also auf spezialisierte Einzellösungen für jeden Teilbereich der Sicherheit. So kamen getrennte Tools für Schwachstellenscans, Compliance-Prüfungen oder Cloud-Posture-Monitoring zum Einsatz. Dieser Ansatz bot zunächst klare Vorteile: spezialisierte Funktionen, hohe Flexibilität. In der dynamischen Cloud-Welt jedoch wird genau diese Vielfalt zunehmend zur Belastung – durch komplexe Integrationen, redundante Daten und fehlende Übersicht.

Die Folgen dieser Fragmentierung zeigen sich in der Praxis deutlich. Häufig melden mehrere Tools dieselbe Schwachstelle, ohne dass klar ist, welche Information tatsächlich relevant ist. Wichtiger Kontext geht dabei verloren, weil jedes Werkzeug nur einen Ausschnitt der Realität abbildet und Zusammenhänge zwischen einzelnen Befunden unklar bleiben. Gleichzeitig steigt der Betriebsaufwand: Teams müssen verschiedene Plattformen parallel bedienen, pflegen und in bestehende Workflows einbinden. Hinzu kommen Reibungsverluste durch Silostrukturen – Sicherheits-, Entwicklungs- und Betriebsteams arbeiten oft mit unterschiedlichen Datengrundlagen, was zu Verzögerungen und Missverständnissen führt.

CNAPPs werden daher als die nächste Stufe der Konsolidierung gesehen. Sie vereinen zentrale Sicherheitsfunktionen in einer integrierten Plattform und schaffen damit einheitliche Sicht und Steuerung über die gesamte Cloud-Umgebung. Dazu gehören das Schwachstellenmanagement zur Erkennung und Priorisierung von Sicherheitslücken, die Posture-Bewertung zur Überwachung von Konfigurationen und Compliance-Vorgaben, die kontinuierliche Laufzeitanalyse

zur Erkennung von Bedrohungen sowie klar definierte Prozesse für eine schnelle und koordinierte Incident Response im Ernstfall.

Befürworter sehen in der Konsolidierung mehrere Vorteile: Silos werden abgebaut, weil alle Teams auf derselben Datengrundlage arbeiten und einen gemeinsamen Überblick erhalten. Der Wildwuchs an Einzellösungen geht zurück – eine zentrale Plattform ersetzt zahlreiche spezialisierte Tools, senkt Kosten und reduziert Komplexität. Zudem entsteht eine einheitliche Quelle der Wahrheit: Risiken werden in einem konsistenten Kontext über alle Ebenen hinweg dargestellt. Und schließlich rückt der Betrieb mehr in den Fokus – Bedrohungen werden nicht im Rauschen unzähliger Alarme übersehen, sondern dort erkannt, wo sie tatsächlich wirksam werden. Kritiker weisen allerdings darauf hin, dass der tatsächliche Nutzen stark von der Integrationstiefe und den vorhandenen Prozessen abhängt.

Damit werden CNAPPs nach Ansicht vieler Fachleute zu einem zentralen strategischen Baustein moderner Cloud-Sicherheit. Unternehmen gewinnen nicht nur an Transparenz und Effizienz, sondern vor allem an Reaktionsfähigkeit – sie können echte Angriffe schneller erkennen und gezielt abwehren.

VORBEREITUNG AUF DIE ZUKUNFT

Die Verbreitung von Containern und cloudnativen Anwendungen wird weiter stark wachsen. Schätzungen zufolge wird bis zum Ende des Jahrzehnts rund die Hälfte aller Unternehmensanwendungen containerbasiert betrieben. Damit wächst auch der Druck auf Sicherheitsteams: Ihre Strategien müssen skalierbar, automatisiert und so gestaltet sein, dass sie mit der Dynamik moderner Entwicklungs- und Betriebsmodelle Schritt halten.

Die Zukunft der Cloud-Sicherheit konzentriert sich dabei auf drei Schwerpunkte:

- **Laufzeitsichtbarkeit:** Sicherheitsmaßnahmen müssen zeigen, welche Risiken im Betrieb tatsächlich relevant sind.
- **KI-Unterstützung:** Intelligente Systeme helfen, Warnmeldungen schneller zu bewerten und in Maschinengeschwindigkeit zu reagieren.
- **Konsolidierte Plattformen:** Statt vieler Einzellösungen sorgt ein zentrales System für einen einheitlichen Überblick über alle Cloud-Risiken.

Unternehmen, die diesen Weg einschlagen, handeln schneller, verringern ihre Angriffsfläche und bleiben Angreifern einen Schritt voraus. Wer dagegen auf isolierte Tools und rein reaktive Prozesse setzt, läuft Gefahr, den Anschluss zu verlieren.

FAZIT

Die Cloud hat die Entwicklung und den Betrieb von Anwendungen grundlegend verändert – und damit auch die Maßstäbe für ihre Absicherung. Laufzeitsichtbarkeit, KI-gestützte Priorisierung und integrierte Plattformansätze sind 2025 keine Zusatzoptionen mehr, sondern zentrale Bestandteile einer wirksamen Sicherheitsstrategie.

Die Botschaft ist klar: Es geht nicht darum, jedem einzelnen Alert hinterherzulaufen. Entscheidend ist, den Blick auf das zu richten, was wirklich zählt – reale Bedrohungen in laufenden Workloads. Nur so lassen sich Cloud-Anwendungen zuverlässig absichern, widerstandsfähig machen und langfristig zukunftsfest betreiben. ■

THN/SYSDIG/STEFAN MUTSCHLER (FREIER JOURNALIST)

DEFINITION: CLOUD-NATIVE APPLICATION PROTECTION PLATFORM

Eine Cloud-Native Application Protection Platform (CNAPP) bezeichnet einen integrierten Ansatz zur Absicherung cloud-nativer Anwendungen über ihren gesamten Lebenszyklus hinweg. Sie kombiniert verschiedene Sicherheitsfunktionen – etwa Schwachstellenmanagement, Konfigurations- und Compliance-Überwachung sowie Laufzeit- und Berechtigungskontrolle – in einer zentralen Plattform.

Ziel ist es, Risiken konsistent zu erkennen, zu bewerten und zu beheben – von der Entwicklung (Shift-Left) bis zum Betrieb (Runtime). Typischerweise vereint eine CNAPP Funktionen aus Bereichen wie

- *CSPM (Cloud Security Posture Management) für die Überprüfung von Cloud-Konfigurationen,*
- *CWPP (Cloud Workload Protection Platform) für den Schutz laufender Workloads,*
- *CIEM (Cloud Infrastructure Entitlement Management) zur Verwaltung von Zugriffsrechten sowie*
- *Container- und Kubernetes-Sicherheit.*

Durch diese Zusammenführung entsteht eine einheitliche Sicht auf Sicherheitsrisiken über unterschiedliche Cloud-Dienste und Anbieter hinweg. CNAPPs sollen so die Komplexität reduzieren, die durch isolierte Einzellösungen entsteht.

(Quelle: nach Gartner, „Market Guide for Cloud-Native Application Protection Platforms", 2025)

Bild: Mega - stock.adobe.com

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

Raus aus der Abhängigkeit

CLOUD-EXIT: WIE UNTERNEHMEN IHRE DIGITALE SOUVERÄNITÄT ZURÜCKGEWINNEN

US-Hyperscaler dominieren den Cloud-Markt, doch für europäische Unternehmen wachsen die Risiken. Unsere Autoren zeigen, wie sich Exit-Strategien und souveräne Cloud-Architekturen risikobasiert entwickeln lassen: von bewährten Portabilitäts-Mustern über Multi- und Sovereign-Cloud-Modelle bis hin zu durchdachten Governance-Mechanismen, die Sicherheit, Compliance und unternehmerische Handlungsfähigkeit miteinander verknüpfen.

Die Nutzung von Cloud-Diensten großer US-Anbieter entwickelt sich für europäische Unternehmen und Behörden zunehmend zum Problem. Geopolitische Spannungen, gesetzliche Zugriffsmöglichkeiten wie der Cloud Act und strenge Datenschutz-Vorgaben machen deutlich: Cloud bedeutet nicht mehr nur Skalierbarkeit und Effizienz, sondern auch Kontrollverlust.

Digitale Souveränität wird damit zur Schlüsselanforderung. Organisationen müssen sicherstellen, dass sie über ihre Daten und Infrastruktur selbstbestimmt verfügen können – unabhängig von externen politischen oder regulatorischen Einflüssen.

RECHTLICHE RAHMENBEDINGUNGEN VERSCHÄRFEN DEN DRUCK

Die rechtliche Lage im Cloud-Umfeld hat sich in den vergangenen Jahren mehrfach verschoben. Besonders das Schrems-II-Urteil sorgt bis heute für Unsicherheit: Mit dem Beschluss hob der Europäische Gerichtshof das frühere Privacy Shield auf. Standardvertragsklauseln bleiben zwar ein wichtiges Instrument, verlangen jedoch zusätzliche technische und organisatorische Schutzmaßnahmen. In der Folge führen das EU-US Data Privacy Framework und die Executive Order 14086 neue Garantien ein – etwa Redress-Mechanismen (Beschwerdeverfahren) und Grundsätze der Verhältnismäßigkeit bei Geheimdienstzugriffen. Diese Regelungen mindern Risiken, schaffen aber keine vollständige Rechtssicherheit und ersetzen keine individuelle Prüfung einzelner Workloads.

Weiterhin bleibt der CLOUD Act ein zentraler Unsicherheitsfaktor: US-Behörden dürfen unter bestimmten Bedingungen auf Daten von US-Anbietern zugreifen, auch wenn diese physisch in der EU liegen. Entscheidend dafür sind Besitz, Verwahrung oder Kontrolle. Gleichzeitig erhöhen NIS-2 und DORA den Druck auf Unternehmen: Beide Regularien verschärfen die Anforderungen an Governance, Lieferkettenmanagement und Drittparteikontrolle sowie an Exit-Fähigkeit und Resilienz – vor allem für Betreiber kritischer Infrastrukturen und Akteure im Finanzsektor.

WENN TRANSPARENZ AN GRENZEN STÖßT

Die Nutzung von US-Hyperscalern schafft vor allem für Betreiber kritischer Infrastrukturen eine komplexe Risikolandschaft. Politische und regulatorische Unsicherheiten – etwa durch den CLOUD Act oder mögliche Handelsrestriktionen – können dazu führen, dass Behörden auf Daten zugreifen oder Cloud-Dienste eingeschränkt werden, selbst wenn die Informationen physisch in Europa liegen. Solche extraterritorialen Zugriffspflichten untergraben die Rechtssicherheit und gefährden die Integrität sensibler Systeme.

Ein Beispiel aus der Praxis: Ein europäisches Unternehmen betreibt geschäftskritische Anwendungen in der Public Cloud eines großen US-Anbieters. Zwar liegt eine Testierung nach dem Cloud Computing Compliance Criteria Catalogue (C5) – eine Testierung nach ISAE-3000-Auditstandard des Bundesamts für Sicherheit in der Informationstechnik (BSI), keine Zertifizierung im engeren Sinne – vor und belegt definierte Sicherheits- und Compliance-Kontrollen, doch die tatsächliche Transparenz bleibt begrenzt. Der Katalog bestätigt das Vorhandensein definierter Kontrollen, ersetzt jedoch nicht die individuelle Einsicht in Betriebsprozesse oder Speicherorte. Für hochsensible Workloads braucht es deshalb einen eigenen Transparenz- und Evidenzpfad – mit Nachweisen zu Replikation, Zugriffsketten und eingebundenen Drittparteien.

Selbst detaillierte Audit-Anfragen stoßen in der Praxis an Grenzen, wenn Anbieter nur standardisierte Reports bereitstellen und keine tieferen technischen Details offenlegen. Diese Intransparenz erschwert es, die Einhaltung europäischer Datenschutzanforderungen vollständig zu prüfen und Risiken aus extraterritorialen Gesetzen realistisch zu bewerten. Gleichzeitig drohen Lock-in-Effekte: Proprietäre Schnittstellen und enge Dienstabhängigkeiten machen den Anbieterwechsel aufwendig und riskant. Im Ernstfall – etwa bei geopolitischen Konflikten oder regulatorischen Änderungen – kann das die Geschäftskontinuität unmittelbar gefährden.

Ohne eigene Architekturentscheidungen bleibt „digitale Souveränität“ ein theoretisches Konzept, kein praktischer Vorteil.

Die Kombination aus politischem Druck, rechtlichen Unsicherheiten und technologischen Abhängigkeiten macht deutlich: Strategische Exit-Optionen und souveräne Cloud-Architekturen sind keine theoretische Überlegung, sondern eine sicherheitsrelevante Notwendigkeit für Organisationen, die kritische Dienste bereitstellen.

EXIT-STRATEGIE IM KONTEXT DIGITALER SOUVERÄNITÄT

Eine Exit-Strategie bedeutet nicht die sofortige Migration aller Systeme, sondern die Fähigkeit, jederzeit handlungsfähig zu sein. Sie schafft die Grundlage, um im Fall regulatorischer Änderungen, geopolitischer Spannungen oder technischer Risiken schnell reagieren zu können.

Ohne eine definierte Exit-Option bleibt Entscheidungsfreiheit häufig theoretisch, da technische und organisatorische Abhängigkeiten den Wechsel erschweren. Erst die aktive Vorbereitung – etwa durch Migrationspläne, Daten- und Log-Portabilität sowie Notfallkonzepte – macht Souveränität praktisch umsetzbar. Ein Missverständnis ist, „Exit" mit passivem Abwarten gleichzusetzen. Wirksam ist nur ein proaktiver Ansatz: Analyse der Workloads, Identifikation von Lock-in-Risiken und Aufbau alternativer Plattformen.

Open-Source-basierte und standardisierte Komponenten sowie containerbasierte Portabilität senken Wechselkosten und verringern Abhängigkeiten. Dadurch lassen sich Workloads flexibel auf Hyperscalern, europäischen Cloud-Plattformen oder auf unternehmenseigenen Infrastrukturen (On-Premises) betreiben. Ergänzend sichern vertragliche Exit-Optionen – etwa die Portabilität von Daten und Protokollen, klare Service Level Agreements (SLA) und festgelegte Audit-Rechte – die Handlungsfähigkeit langfristig ab.

PRAGMATISCHER ANSATZ ZUR WORKLOAD-KLASSIFIKATION

Ein entscheidendes Element für jede Exit-Strategie ist die Priorisierung der Workloads. Ein bewährter Weg ist die Klassifikation nach Daten- und Systemkritikalität:

- **Unternehmenskritisch:** Systeme, deren Ausfall die Geschäftskontinuität unmittelbar gefährdet, zum Beispiel Enterprise Resource Planning (ERP) oder Produktionssteuerung
- **Kritisch:** Anwendungen mit hohem Einfluss auf Compliance oder Sicherheit, aber ohne sofortige Betriebsunterbrechung, zum Beispiel Human-Resources-(HR)-Systeme oder die Finanzbuchhaltung
- **Intern:** Workloads für interne Prozesse mit begrenztem Risiko, zum Beispiel Kollaborationstools
- **Öffentlich:** Systeme mit offenen Daten oder geringer Sensibilität, zum Beispiel Marketing-Websites

Diese Klassifikation ermöglicht eine schrittweise Exit-Planung: Zuerst Backups und Disaster-Recovery für unternehmenskritische Workloads, dann Migration kritischer Systeme, während weniger sensible Anwendungen später folgen. So entsteht ein realistischer, priorisierter Migrationspfad, der Handlungsfähigkeit sichert, ohne operative Stabilität zu gefährden. Ergänzend sollte je Klasse der Schutzbedarf – also Vertraulichkeit, Integrität, Verfügbarkeit und rechtliche Anforderungen – sowie die Exit-Tiefe (von reinen Sicherungskopien bis zu vollständig redundanten Disaster-Recovery- und aktiv-aktiv-Szenarien) mit konkreten Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) verknüpft werden.

ERFOLGSFAKTOREN FÜR DEN STRATEGISCHEN EXIT

Eine wirksame Exit-Strategie verlangt mehr als technische Maßnahmen. Sie beginnt mit einer klaren strategischen Ausrichtung und endet in einer umsetzbaren Praxis. Eine einheitliche Lösung gibt es jedoch nicht. Der konkrete Weg hängt immer vom Geschäftsmodell, von regulatorischen Anforderungen und von der technischen Ausgangslage ab. Fünf Faktoren bestimmen, ob eine Exit-Strategie in der Praxis trägt:

- **Strategische Verankerung:** Jede Exit-Strategie braucht Rückendeckung aus der Geschäftsleitung. Sie ist Teil der Risiko- und Compliance-Strategie und muss in die Unternehmensplanung integriert sein.
- **Transparenz und Analyse:** Abhängigkeiten müssen sichtbar werden. Das gelingt durch Abstraktionsschichten zwischen Anwendung und Plattformdiensten sowie durch die konsequente Vermeidung proprietärer Schnittstellen.
- **Offenheit und Portabilität:** Offene Standards und containerbasierte Architekturen bilden das Rückgrat einer souveränen Cloud-Strategie. Organisationen sollten früh festlegen, welche Kernkomponenten portabel und interoperabel bleiben müssen.
- **Wirtschaftlichkeit:** Eine realistische Kalkulation entscheidet über den Erfolg. Investitionen in Migration, neue Plattformen und Schulungen müssen den Gesamtbetriebskosten (Total Cost of Ownership, TCO) gegenübergestellt werden. Der Wettbewerb zwischen Anbietern wirkt dabei als Optimierungshebel.
- **Architektonische Absicherung:** Schlüsselherrschaft, Zugriffsentkopplung, Datenlokalisierung und die regelmäßige Testbarkeit der Zielplattform schaffen technische Flexibilität und organisatorische Resilienz.

ARCHITEKTURPRINZIPIEN FÜR SOUVERÄNE CLOUD-UMGEBUNGEN

Darüber hinaus gilt es, die technische Architektur konsequent auf Portabilität auszurichten. Ein zentrales Prinzip lautet Portability by Design: Standardisierte Containerformate nach Open Container Initiative (OCI), Infrastruktur als Code und automatisierte Plattformtests gewährleisten, dass Workloads unabhängig von einzelnen Anbietern betrieben werden können.

Ebenso wichtig ist eine konsequente Kryptografie- und Schlüsselherrschaft. Unternehmen sollten ihre Schlüssel selbst kontrollieren – etwa über Hardware-Sicherheitsmodule (HSM) oder externe Key-Management-Systeme (KMS) – und deren Rotation dokumentieren. Masterkeys dürfen dabei grundsätzlich nicht exportierbar sein.

Auch die Zugriffsentkopplung spielt eine zentrale Rolle. Strikte Least-Privilege-Modelle, getrennte Administrator-Domänen, Just-in-Time-Berechtigungen und revisionssichere Protokollierung in einer separaten Vertrauensdomäne erhöhen die Sicherheit und Nachvollziehbarkeit.

Nicht zuletzt trägt eine klare Datenlokalisierung zur Souveränität bei: Sensible Workloads sollten ausschließlich innerhalb der Europäischen Union verarbeitet werden. Remote-Administrationszugriffe von außerhalb des europäischen Rechtsraums sind bei kritischen Infrastrukturen (KRITIS) zu vermeiden.

Ergänzend gehört zu einer souveränen Cloud-Architektur ein durchgängiger Transparenz- und Audit-Pfad. Vertraglich zugesicherte Auskunfts- und Prüfungsrechte, klar definierte Disclosure-Prozesse und technische Nachweise – etwa in

Reifegrad	Merkmale
Basic	Backups vorhanden, kein dokumentierter Migrationspfad, minimaler Portabilitätsnachweis
Prepared	Restore-/Migrationstests dokumentiert, getrennte Admin-Domänen und Schlüsselhaltung, Verträge mit Portabilitätsklauseln
Portable	automatisierte Migration auf Alternativplattformen, Container/Infrastrucure-as-Code, externe Schlüsselherrschaft etabliert
Resilient	regelmäßige Trockenübungen, nachweisbares Full-Failover, Logs in separater Trust-Domäne, definierte und geprüfte RTO/RPO-Ziele

Tabelle 1: Checkliste Reifegradmodell Exit-Fähigkeit

Form von Attestierungen oder Protokollen – ermöglichen eine unabhängige Überprüfung, ohne Betriebsgeheimnisse zu gefährden.

Abschließend gilt: Ein Exit bleibt nur dann wirksam, wenn er regelmäßig getestet wird. Organisationen sollten Wiederherstellungs- und Migrationsübungen fest einplanen, Zielplattform-Runbooks dokumentieren und messbare Kennzahlen für Wiederanlaufzeiten und Datenverluste definieren. Nur so lässt sich die Exit-Fähigkeit im Ernstfall verlässlich nachweisen.

REIFEGRADMODELL ALS ORIENTIERUNG

Um den Stand der eigenen Exit-Fähigkeit bewerten zu können, lässt sich der Fortschritt anhand eines Reifegradmodells mit vier Stufen einordnen (siehe Tabelle 1). Basic steht für die Ausgangsstufe: Backups sind vorhanden, ein dokumentierter Migrationspfad oder belastbarer Nachweis der Portabilität jedoch nicht. Prepared beschreibt Organisationen, die bereits Restore- und Migrationstests dokumentiert haben, getrennte Administrator-Domänen und eine eigene Schlüsselhaltung betreiben sowie über Verträge mit Portabilitätsklauseln verfügen.

Portable kennzeichnet Umgebungen, in denen Workloads automatisiert auf alternative Plattformen migriert werden können – mit containerisierten Anwendungen, Infrastruktur als Code und einer etablierten externen Schlüsselverwaltung. Resilient schließlich bezeichnet die höchste Stufe: Regelmäßige Wiederherstellungsübungen, ein nachweisbares vollständiges Failover, Protokolle in separaten Vertrauensdomänen sowie definierte und geprüfte Wiederanlauf- und Wiederherstellungsziele sichern die Exit-Fähigkeit auch im Ernstfall.

EU DATA ACT SCHAFFT NEUE CHANCEN

Ein deutliches Signal für Überlegungen zu Exit-Szenarien sind neue Rahmenbedingungen, die durch die europäischen Institutionen gesetzt werden. Der EU Data Act (VO (EU) 2023/2854) ist seit 2024 in Kraft; der Großteil der Pflichten gilt ab 12. September 2025 und bringt für Unternehmen einen entscheidenden Vorteil: verbindliche Wechselrechte für Cloud-Kunden. Damit wird der Anbieterwechsel nicht mehr nur eine technische, sondern auch eine rechtlich abgesicherte Option. Ein weiterer Meilenstein folgt bis zum 12. Januar 2027, wenn sogenannte Egress-Gebühren vollständig entfallen müssen – also Entgelte, die Anbieter bislang für das Herausleiten oder Übertragen von Daten an andere Plattformen verlangten.

Diese Regelungen senken die finanziellen Hürden für Datenmigration erheblich und stärken die Position europäischer Unternehmen gegenüber Hyperscalern. Wer jetzt eine Exit-Strategie plant, sollte diese neuen Rechte aktiv nutzen – etwa durch die Aufnahme entsprechender Klauseln in Verträge und die Vorbereitung auf einen Anbieterwechsel ohne zusätzliche Kosten.

Der neue Rechtsrahmen stärkt die digitale Souveränität, doch nur Unternehmen, die frühzeitig handeln und ihre Architektur entsprechend ausrichten, können die Vorteile tatsächlich nutzen.

FAZIT

Für alle Organisationen, die sich mit einem Exit-Szenario beschäftigen, ist digitale Souveränität kein abstraktes Ideal, sondern ein strategischer Imperativ. Wer heute die Kontrolle über Daten, Systeme und Plattformen sichern will, muss den Exit nicht als Rückschritt begreifen, sondern als Gestaltungsoption. Der EU Data Act liefert dafür neue rechtliche Hebel – doch ohne technische und organisatorische Vorbereitung bleiben sie wirkungslos.

Jetzt ist der richtige Zeitpunkt, die Exit-Fähigkeit gezielt zu planen und zu bewerten. Welche Workloads sind kritisch? Wo bestehen Lock-in-Risiken? Welche Architekturentscheidungen ermöglichen echte Portabilität? Wer diese Fragen heute beantwortet, sichert morgen die Handlungsfreiheit seines Unternehmens – und schafft die Grundlage für Resilienz, Innovationsfähigkeit und regulatorische Sicherheit in einer zunehmend fragmentierten digitalen Welt. ■

MICHAEL BERTKO
ist Sales Consultant bei OPITZ CONSULTING und begleitet Unternehmen bei der Entwicklung und Umsetzung ganzheitlicher Cloud- und Infrastrukturstrategien. Sein Schwerpunkt liegt auf digitaler Souveränität, Multi-Cloud-Architekturen und Exit-Szenarien, die Kontrolle, Sicherheit und Wirtschaftlichkeit miteinander verbinden.

JEREMY SMEETS
ist Senior System Engineer und strategischer Technologieberater bei OPITZ CONSULTING. Seit über einem Jahrzehnt begleitet er Unternehmen und öffentliche Institutionen bei der Architektur, Integration und Transformation komplexer Infrastrukturen – mit besonderem Fokus auf digitale Souveränität, Open-Source-Ecosysteme und nachhaltige Plattformstrategien.

OT-Segmentierung als Schutzschild der vernetzten Produktion

SICHERHEIT IN ZONEN

Die Digitalisierung und Vernetzung industrieller Anlagen vergrößert die Angriffsflächen erheblich. Gelangen Kriminelle einmal ins System, können sie sich oft ungehindert durch das Produktionsnetz bewegen – mit gravierenden Folgen bis hin zum Stillstand ganzer Fertigungslinien. OT-Segmentierung setzt hier an: Sie kontrolliert die Verbindungen innerhalb vernetzter Systeme und schützt so vor der Ausbreitung von Angriffen.

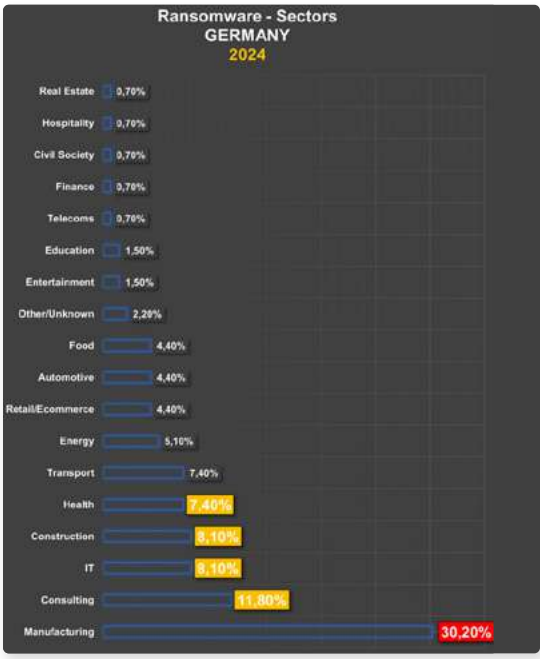
Ein einziger Cyberangriff kann genügen – und die Fertigung steht still. Besonders in der Industrie ist dieser Dominoeffekt längst keine Ausnahme mehr: Laut dem *„Länderbericht zur Cyberbedrohungslandschaft: Deutschland 2024“* der Var Group war die Fertigungsindustrie mit 30,2 Prozent aller beobachteten Ransomware-Angriffe die am stärksten betroffene Branche. Auch Distributed-Denial-of-Service-(DDoS)- und Web-Defacement-Attacken treffen Produktionsbetriebe regelmäßig. Schon kurze Ausfälle führen zu massiven Verlusten und machen die Branche zum bevorzugten Ziel für Angreifer.

Wie drastisch die Folgen sein können, zeigte jüngst der Serviettenhersteller Fasana: Nach einem Ransomware-Angriff kam die Produktion vollständig zum Erliegen, am Ende blieb nur der Gang in die Insolvenz. Der Fall verdeutlicht, wie eng Office-IT und Produktionsnetze heute verzahnt sind – und wie wichtig es ist, beide Bereiche gleichermaßen abzusichern. Ein zentraler Baustein dafür ist die Operational-Technology-(OT)-Segmentierung: Sie begrenzt die Ausbreitung eines Angriffs und hält kritische Anlagen funktionsfähig.

KONTROLLIERTE KOMMUNIKATION STATT KOMPLETTE ABSCHOTTUNG

OT-Segmentierung bezeichnet die strategische Unterteilung industrieller Infrastrukturen in separate logische oder physische Zonen mit kontrollierten Grenzen, die den Kommunikationsfluss zwischen Geräten oder Gerätegruppen regulieren. Anders als bei der klassischen IT-Segmentierung, die primär der Netzwerkoptimierung dient, zielt OT-Segmentierung darauf ab, im Fall eines Angriffs laterale Bewegungen zu begrenzen und die potenziellen Auswirkungen eines Sicherheitsvorfalls einzudämmen.

In der Praxis bedeutet OT-Segmentierung den Aufbau von auf Whitelists basierenden Sicherheitsbarrieren zwischen verschiedenen funktionalen Bereichen – wie etwa zwischen der



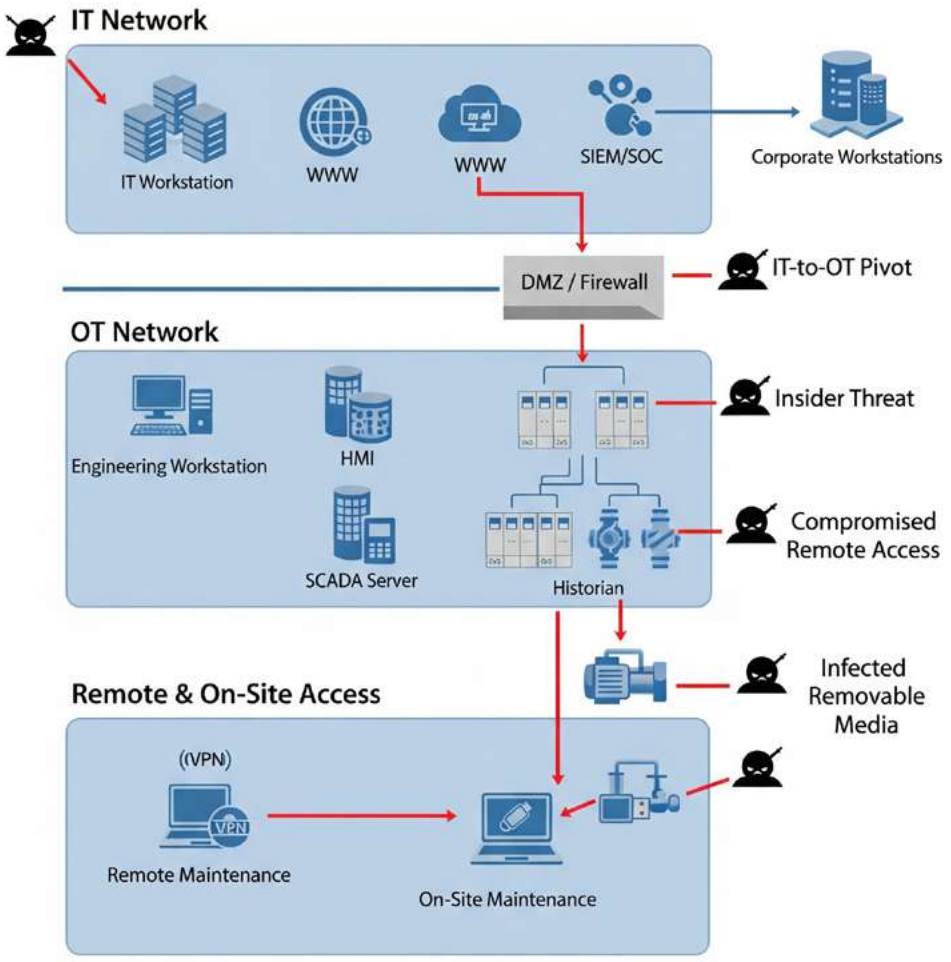
Ransomware-Angriffe 2024: Die Fertigungsindustrie in Deutschland ist mit 30,2 Prozent am häufigsten betroffen, gefolgt von Beratung (11,8 Prozent) und IT (8,1 Prozent). (Bild: Var Group)

Überwachungsebene und der Maschinensteuerungsebene. Der Zugriff zu jedem Funktionsbereich wird von Richtlinien geregelt, die durch Protokolle, Adressen oder Verhaltensmuster definiert sind. Entscheidend ist dabei, dass Kommunikation nicht blockiert wird, sondern kontrolliert, sichtbar und nachverfolgbar gestaltet wird.

Die Vorteile einer OT-Segmentierung sind eindeutig: Sie verringert die Angriffsfläche und trägt wesentlich zur Aufrechterhaltung des laufenden Betriebs bei. So lassen sich ungeplante Stillstände vermeiden und zugleich Prozessdaten, Anlagen und Arbeitsplätze wirksam schützen. Darüber hinaus unterstützt die Segmentierung die Einhaltung regulatorischer Anforderungen – etwa durch die Begrenzung von Schadensausbreitung, die Kontrolle von Zugriffs- und Autorisierungsrechten sowie die schnellere Erkennung von Sicherheitsvorfällen. Angesichts der wachsenden Bedrohungslage entwickelt sich OT-Segmentierung zunehmend zu einem strategischen Wettbewerbsfaktor – besonders in der Fertigungsindustrie, die in Deutschland zu den am häufigsten von Cyberangriffen betroffenen Branchen zählt.

WEIT VERBREITETE FEHLEINSCHÄTZUNGEN IN DER PRAXIS

Ein häufiger Irrglaube in der industriellen Praxis ist die Annahme, OT-Segmentierung bestehe lediglich darin, Netzwerke mit Firewalls oder Virtual Local Area Networks (VLANs) zu trennen. Aus diesem Grund werden bei der Implementierung oft die tatsächlichen Kommunikationsflüsse und Abhängigkeiten zwischen den OT-Geräten nicht in Betracht gezogen – obwohl das die Grundlage einer sicheren OT-Umgebung ist. Diese vereinfachte Sichtweise führt oft zu Fehlkonzeptionen, die im schlimmsten Fall wirkungslos oder sogar kontraproduktiv sind.



Cyberbedrohungen können sich über verschiedene Pfade ausbreiten. Ohne geeignete Segmentierung und Zugriffskontrollen lassen sich solche Angriffsketten kaum wirksam unterbrechen. (Bild: Var Group)

EMPFEHLUNGEN FÜR ENTSCHEIDER

Damit OT-Segmentierung nicht nur technisch funktioniert, sondern auch im Betriebsalltag standhält, braucht es ein klares, praxisnahes Vorgehen. Die folgenden Empfehlungen zeigen, worauf es bei erfolgreicher Implementierung ankommt:

- ***Bestandsaufnahme als Basis:*** *Bevor Unternehmen in Segmentierungstechnologien investieren, sollten sie sich Klarheit über ihre OT-Assets und deren Kommunikationsbeziehungen verschaffen. Eine passive Netzwerkanalyse liefert die notwendigen Daten, ohne den Betrieb zu stören.*
- ***Planung auf Basis realer Kommunikationsflüsse:*** *Zonen und Conduits sollten entsprechend der tatsächlichen betrieblichen Logik der Anlagen definiert werden. Eine zu starke Orientierung an IT-Konzepten, die in industriellen Umgebungen oft nicht praktikabel sind, gilt es zu vermeiden.*
- ***Gezielter Schutz von Drittzugriffen:*** *Mindestsicherheitsanforderungen sollten vertraglich mit externen Lieferanten definiert werden, im Einklang mit den Grundsätzen der NIS-2-Richtlinie, einschließlich kontrolliertem Zugang, Rückverfolgbarkeit und Update-Management.*
- ***Organisatorische Resilienz mitdenken:*** *Ergänzend zur technischen Segmentierung sollten Unternehmen Incident-Response-Pläne entwickeln, Mitarbeitende regelmäßig schulen und eine Kommunikationsmatrix für den Krisenfall vorbereiten. Security-Gap-Analysen und Forensik-Readiness-Checks helfen, Schwachstellen frühzeitig zu erkennen und Meldepflichten nach NIS-2 sicher einzuhalten.*

Zonen-ID	Zonen-Name	Ebene	Asset Typ(en)	Protokolle	Risikostufe	Kommunikation mit	Security Level Target	Anmerkungen
Z1	Business LAN	4	ERP, AD, Mailserver	TCP/IP	Mittel	Z2	SL1	aus IT-Netz, keine eingehenden Verbindungen
Z2	DMZ	3,5	Historian, Jump Server	OPC UA, RDP	Hoch	Z1, Z3	SL2	Gateways
Z3	Kontroll-netzwerk	3	SCADA-Server	Modbus TCP	Hoch	Z2, Z4	SL2	Zugang aus der DMZ
Z4	SPS-Zone	2	Siemens S7-Steuerungen	Profinet	Sehr hoch	Z3, Z5	SL3	Whitelists-Regelungen
Z5	Feldebene	1	Sensoren, Aktoren	Analog, HART	Hoch	Z4	SL3	kein Fernzugriff

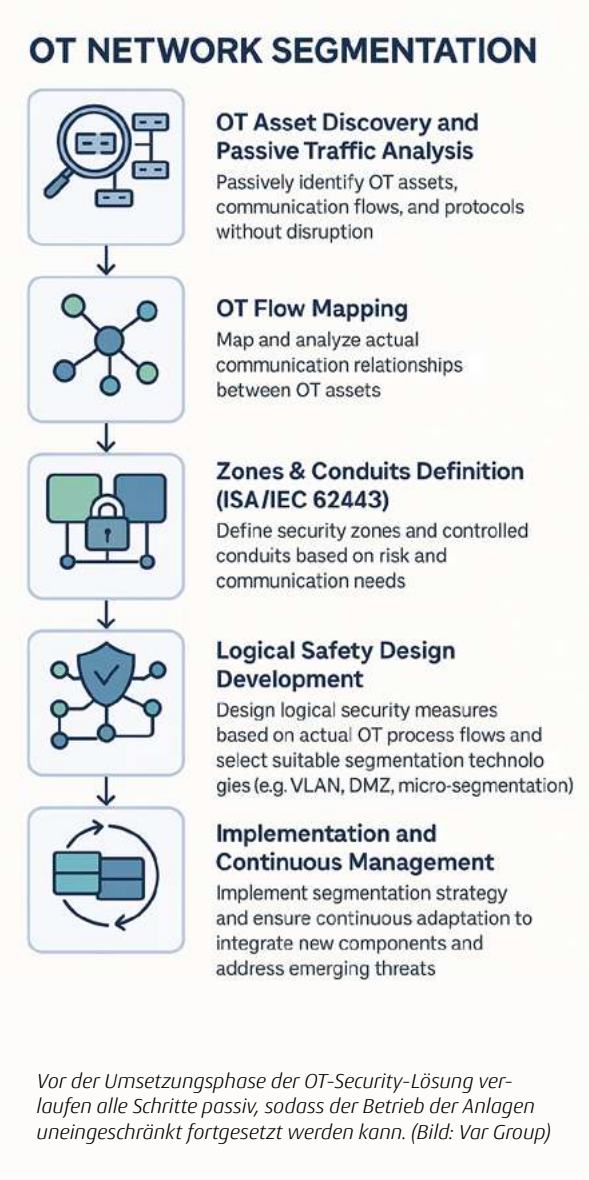
Tabelle 1: Beispielhafte Zuordnung industrieller Systeme

Ein weiterer verbreiteter Mythos betrifft die Auswirkungen auf die Betriebsabläufe: Viele Unternehmen befürchten, dass OT-Segmentierung die Effizienz industrieller Prozesse beeinträchtigen könnte. In Wirklichkeit jedoch sichert eine richtig konzipierte Segmentierung die Prozesskontinuität, da sie die Widerstandsfähigkeit der Anlagen erhöht und den Schaden im Angriffsfall eindämmt. Statt Prozesse zu stören, schützt sie diese vor unerwünschten Eingriffen und Störungen.

Nicht zuletzt wird Segmentierung häufig als einmalige Aufgabe betrachtet, während es sich in Wahrheit um einen kontinuierlichen Prozess handelt, der mit der Evolution des Netzwerks Schritt halten muss. Gerade in der Industrie, wo Anlagen oft über Jahrzehnte betrieben werden und immer wieder neue Komponenten hinzukommen, ist ein dynamisches Segmentierungskonzept unerlässlich.

SYSTEMATISCHES VORGEHEN NACH INTERNATIONALEN STANDARDS

Am Anfang jeder wirksamen OT-Segmentierung steht eine präzise Bestandsaufnahme. Ohne eine passive Asset-Discovery riskieren Unternehmen, ihr Netzwerk auf Grundlage unvollständiger oder falscher Annahmen zu strukturieren. Im ersten Schritt sollten daher mittels passiver Verkehrsanalyse sämtliche Geräte, Kommunikationsbeziehungen und Protokolle erfasst werden – idealerweise, ohne den laufenden Betrieb zu beeinträchtigen.



Vor der Umsetzungsphase der OT-Security-Lösung verlaufen alle Schritte passiv, sodass der Betrieb der Anlagen uneingeschränkt fortgesetzt werden kann. (Bild: Var Group)

Mit diesen Informationen erfolgt das Flow Mapping: die systematische Erfassung und Analyse der tatsächlichen Kommunikationsbeziehungen zwischen den OT-Asstes. Darauf aufbauend lassen sich Zonen und Conduits nach dem ISA/IEC-62443-Standard festlegen, dem zentralen Referenzrahmen für industrielle Cybersicherheit. Zonen fassen dabei Assets mit vergleichbarer Risikostufe und ähnlichen Schutzanforderungen zusammen, während Conduits die kontrollierten Übergänge zwischen diesen Bereichen bilden. Für jede Zone wird ein Ziel-Sicherheitsniveau (Security Level Target, SL-T) definiert, das den erforderlichen Mindestschutz beschreibt – abhängig von ihrer Relevanz für die Produktion und dem möglichen Schaden im Ernstfall.

Wie ein solches Modell in der Praxis aussehen kann, zeigt Tabelle 1: Sie veranschaulicht beispielhaft, wie industrielle Systeme wie Enterprise-Resource-Planning-(ERP)-Server, Historian, Supervisory-Control-and-Data-Acquisition-(SCADA)-Server, speicherprogrammierbare Steuerungen (SPS) oder Feldgeräte in funktionale Zonen (Z1–Z5)

TYPISCHE SEGMENTIERUNGSFORMEN IN DER OT

- ***VLANs:*** *kurz für Virtual Local Area Network, ein logisches Teilnetzwerk innerhalb eines physischen lokalen Netzwerks (LAN). Es ermöglicht, ein einzelnes LAN in mehrere, voneinander getrennte logische Netzwerke zu unterteilen, ohne dass zusätzliche Hardware benötigt wird.*
- ***DMZ:*** *kurz für Demilitarisierte Zone; Sicherheitszonen zwischen IT und Produktion. Sie dienen als Zwischenpuffer, um Maschinen vor direkten Zugriffen zu schützen.*
- ***Industrielle Gateways:*** *Geräte, die in industriellen Steuerungssystemen eingesetzt werden, um die Kommunikation zwischen verschiedenen Netzwerksegmenten zu ermöglichen, oft auch zwischen IT- und OT-Netzwerken.*
- ***Zonen und Conduits:*** *nach dem internationalen Standard der International Society of Automation/International Electrotechnical Commission (ISA/IEC 62443) definierte Sicherheitsbereiche mit kontrollierten Übergängen. Strukturierter Ansatz: Produktionsbereiche werden getrennt und der Datenaustausch zwischen ihnen wird kontrolliert. Vergleichbar mit Sicherheitsbereichen im Werk.*
- ***Mikrosegmentierung:*** *feinste Unterteilung bis auf Geräte- oder Anwendungsebene. Besonders sinnvoll in sensiblen oder stark vernetzten Anlagen.*

eingeteilt und mit spezifischen Protokollen, SL-Anforderungen und Übergängen versehen werden. Solche Tabellen dienen als wichtige Grundlage für die technische Umsetzung – zum Beispiel für die Konfiguration von Firewalls, das Whitelisting von Verbindungen oder das Einrichten sicherer Fernzugänge.

HERAUSFORDERUNGEN IN HETEROGENEN PRODUKTIONSUMGEBUNGEN

In der Umsetzung werden je nach Netzstruktur und Komplexität unterschiedliche Formen der Segmentierung eingesetzt: von physischer Trennung über VLANs bis hin zu industriellen Demilitarisierten Zonen (DMZ) und Mikrosegmentierung auf Anwendungsebene. Welcher technische Ansatz gewählt wird, hängt maßgeblich vom konkreten Umfeld ab – zum Beispiel von der Heterogenität der Anlage, der verfügbaren Dokumentation oder der Anforderungsdichte im Produktionsprozess.

Darauf aufbauend lässt sich ein logisches Sicherheitsdesign entwickeln, das sich eng an den realen Prozessflüssen orientiert – ein wesentlicher Erfolgsfaktor, um Sicherheit und Betriebsstabilität in Einklang zu bringen. Besonders ältere, heterogene Umgebungen erfordern dabei besondere Sorgfalt: Lückenhafte Dokumentation, proprietäre oder veraltete Protokolle und begrenzte Skalierbarkeit erhöhen das Risiko unbeabsichtigter Störungen. In solchen Fällen wird der Projekterfolg maßgeblich durch eine gründliche Erkundung und vorausschauende Migrationsplanung bestimmt.

Ein Beispiel aus der Chemieindustrie zeigt, wie OT-Segmentierung als Teil einer übergreifenden Modernisierungsstrategie wirken kann. Ein international tätiges Unternehmen führte die Maßnahme nicht reaktiv nach einem Sicherheitsvorfall ein, sondern gezielt, um Wettbewerbsfähigkeit und Resilienz zu stärken. Die zweijährige Umsetzung umfasste neben der technischen Realisierung auch die Schulung und Einbindung aller relevanten Gruppen – von der lokalen OT-Mannschaft über die IT bis hin zu Ingenieurteams und Anlagenleitern. Dieser ganzheitliche Ansatz erwies sich als Schlüssel zum Erfolg: Das Werk erreichte ein deutlich höheres Schutzniveau, beschleunigte die Einhaltung kommender EU-Vorgaben wie der Cyberresilience-Act-Verordnung und positionierte sich als Vorreiter in Sachen Sicherheit und regulatorischer Vorbereitung.

STRATEGISCHE WEICHENSTELLUNG

Mit der fortschreitenden Vernetzung entwickelt sich OT-Segmentierung zunehmend zu einem zentralen Baustein für Resilienz und langfristige Betriebskontinuität. Der Trend geht klar in Richtung Integration: Segmentierung wird heute mit kontinuierlichem Monitoring, starker Authentifizierung, Privileged-Access-Management und Zero-Trust-Konzepten verknüpft, die speziell auf industrielle Umgebungen zugeschnitten sind. Damit wird sie nicht als Endpunkt, sondern als Ausgangsbasis auf dem Weg zur cyberindustriellen Reife verstanden. Angesichts geopolitischer Spannungen, globaler Lieferkettenrisiken und der beschleunigten Digitalisierung gewinnt der Schutz industrieller Anlagen strategische Bedeutung. Er ist längst keine rein technische Aufgabe mehr, sondern eine unternehmerische Pflicht. OT-Segmentierung markiert dabei einen der ersten praxisnahen Schritte zu mehr Widerstandsfähigkeit. ■

WICHTIGE OT-SICHERHEITSSTANDARDS

- ***ISA/IEC 62443:*** *internationale Normenreihe für die Cybersicherheit industrieller Automatisierungssysteme*
- ***NIS-2-Richtlinie:*** *EU-Richtlinie zur Netz- und Informationssicherheit mit erweiterten Anforderungen für kritische Infrastrukturen*
- ***ISO 27001/27002:*** *allgemeine Standards für Informationssicherheits-Managementsysteme, zunehmend auch für OT relevant*
- ***NIST Cybersecurity Framework:*** *Rahmenwerk des US-amerikanischen National Institute of Standards and Technology*

ALESSANDRO ZUECH
ist Head of OT Security bei Yarix, einer Marke der Var Group für Cyber Security.

Von der Norm zur Wirkung (3):
Risiken erkennen, priorisieren, beherrschen –
ISO 31000 als Basis für Resilienz und Compliance.

VOM BAUCHGEFÜHL ZUR METHODE

Risikomanagement als Brücke zwischen Strategie und Umsetzung

Gute Entscheidungen entstehen nicht aus dem Bauch heraus, sondern basieren auf einem System: Im dritten Teil unserer Serie zeigen unsere Autoren, wie sich mithilfe der ISO 31000 Unsicherheit in steuerbare Größen übersetzen lässt – mit einem klaren Prozess, definierten Rollen und Kennzahlen, die Management und Auditoren überzeugen. Der Fokus verlagert sich von der reinen Dokumentation in Listen und Heatmaps hin zu einer aktiven Steuerung, die Risiken gezielt entlang der definierten Risikobereitschaft und der strategischen Unternehmensziele priorisiert.

Jedes Unternehmen steht täglich vor Entscheidungen, deren Ausgang ungewiss ist – egal, ob es um Investitionen, Lieferanten oder Sicherheitsmaßnahmen geht. Oft verlässt man sich dabei auf Erfahrung und Intuition: „Das Risiko ist gering, das wird schon nicht passieren." Dieses Bauchgefühl mag im Tagesgeschäft funktionieren, stößt jedoch in einem zunehmend regulierten Umfeld schnell an seine Grenzen.

Mit wachsenden Anforderungen aus der ISO 27001, der Network and Information Security-Directive 2 (NIS-2), dem Digital Operational Resilience Act (DORA) und weiteren Regularien steigt der Druck, Risiken nicht nur zu erkennen, sondern auch nachvollziehbar zu bewerten und systematisch zu steuern. Es genügt nicht mehr, Gefahren zu erahnen – sie müssen quantifizierbar, priorisierbar und in Steuerungsprozesse eingebettet sein. Genau hier setzt das Risikomanagement nach ISO 31000 an: Es schafft Struktur in einem Umfeld, das oft von Unsicherheit geprägt ist, und liefert den methodischen Rahmen, um Risiken messbar zu machen und Entscheidungen auf Fakten zu stützen.

Dabei versteht die ISO 31000 den Begriff Risiko nicht ausschließlich als Bedrohung. Risiko bedeutet hier jede Abweichung vom Ziel – positiv wie negativ. Das heißt: Neben den klassischen Gefahren (Threats) berücksichtigt das Risikomanagement auch Chancen (Opportunities), die aus bewussten Entscheidungen entstehen können. Dieses Verständnis erweitert den Blick: Es geht nicht nur darum, Risiken zu vermeiden, sondern Potenziale aktiv zu gestalten.

In der ISO 9001 ist dieses Chancenmanagement als integraler Bestandteil der kontinuierlichen Verbesserung verankert. Richtig umgesetzt, sorgt es dafür, dass Unternehmen nicht nur auf Störungen reagieren, sondern gezielt günstige Entwicklungen fördern – etwa durch Innovationen, Prozessoptimierungen oder neue Partnerschaften. Wer diese positiven Risiken ignoriert, läuft Gefahr, sie unbewusst in Bedrohungen zu verwandeln: Was heute eine Chance ist, kann morgen durch mangelnde Steuerung zum Risiko werden.

Ein ganzheitliches Risikomanagement nach ISO 31000 verbindet daher Sicherheitsdenken mit unternehmerischer Gestaltungskraft. Wer Risiken versteht, kann sie nicht nur kontrollieren, sondern auch nutzen – zur Stärkung von Resilienz, Vertrauen und Wettbewerbsfähigkeit. So wird Risikomanagement vom Pflichtprogramm zum Führungsinstrument, das Unsicherheit in Handlungsfähigkeit und Zukunftssicherheit verwandelt.

PROBLEMBESCHREIBUNG: RISIKEN OHNE METHODE BLEIBEN UNSICHTBAR

Gerade beim Management von Risiken ist es gefährlich, Entscheidungen nur auf Basis von Erfahrung und Intuition zu treffen. Denn Intuition kann trügen, besonders in komplexen Organisationen. Erfahrung ersetzt Wahrnehmung schnell durch Annahme. Wer glaubt, alles unter Kontrolle zu haben, unterliegt leicht der „Illusion der Kontrolle". Diese kognitive Verzerrung führt dazu, dass Risiken unterschätzt und Zufälle überschätzt werden. Methodisches Risikomanagement dient daher nicht nur regulatorischen Anforderungen, sondern schützt auch das Unternehmen selbst und die Menschen, die darin Entscheidungen treffen.

Mit Normen wie ISO 27001, NIS-2 oder DORA verlangen Aufsichtsbehörden und Auditoren heute den Nachweis, dass Risiken strukturiert identifiziert, bewertet und gesteuert werden. Subjektive Einschätzungen reichen längst nicht mehr aus. Ohne objektive Methode fehlt die Grundlage, um Risiken nachvollziehbar zu dokumentieren, ihre Eintrittswahrscheinlichkeit realistisch zu bewerten und die Wirksamkeit von Maßnahmen nachzuweisen.

Fehlt ein solches System, treten regelmäßig dieselben Muster auf:

1. **Intransparenz:** Risiken werden unsystematisch gesammelt, wichtige Zusammenhänge bleiben verborgen, Doppelungen und Lücken entstehen.

2. **Fehlende Priorisierung:** Ressourcen fließen in „gefühlte" Gefahren, während echte Bedrohungen übersehen werden.

3. **Illusion der Kontrolle:** Gerade erfahrene Personen überschätzen ihre Fähigkeit, Risiken intuitiv einschätzen zu können, und unterschätzen gleichzeitig die Wirkung unerkannter Abhängigkeiten.

4. **Geringe Steuerungswirkung:** Ohne Kennzahlen und belastbare Analysen fehlt die

Bild: Eigene Darstellung, generiert mit ChatGPT (SORA)

Grundlage für faktenbasierte Entscheidungen in Management und Aufsicht.

Das Ergebnis ist ein Teufelskreis aus reaktiven Maßnahmen, steigendem Auditaufwand und schwindendem Vertrauen – intern wie extern. Wo Risikoanalysen nur als Pflichtübung verstanden werden, bleibt die Organisation blind für strukturelle Schwächen. Ein professionelles, methodisch fundiertes Risikomanagement dagegen schafft Klarheit: Es übersetzt Unsicherheit in steuerbare Größen und macht Risiken sichtbar, bevor sie wirken.

VERGLEICHSMATRIX: ISO 31000, ISO 27005, NIST SP 800-30 UND ISO 9001

Risikomanagement ist ein altbewährtes Konzept – doch die Herangehensweisen unterscheiden sich je nach Norm und Zielsetzung deutlich. Während ISO 31000 den übergeordneten strategischen Rahmen für alle Organisationstypen liefert, vertieft ISO 27005 das Thema speziell für Informationssicherheitsrisiken. Das amerikanische Pendant NIST SP 800-30 ergänzt diesen Ansatz durch praxisnahe Methoden, Szenarien und Beispiele aus dem IT-Umfeld.

Als vierter Baustein kommt ISO 9001 ins Spiel. Sie betrachtet Risiken und Chancen im Kontext von Qualität und kontinuierlicher Verbesserung. Anders als die drei anderen Normen versteht sie Risikomanagement nicht als separates System, sondern als Bestandteil der gesamten Unternehmenssteuerung. Damit liefert sie den operativen Anknüpfungspunkt für ein integriertes Managementsystem, das Qualität, Sicherheit und Resilienz verbindet.

Tabelle 1 zeigt, wie sich diese vier Standards ergänzen und welche Rolle sie jeweils im Zusammenspiel moderner Governance-Strukturen spielen. Gemeinsam bilden die vier Normen den Werkzeugkasten für modernes Risikomanagement und integrierte Steuerung:

- **ISO 31000** liefert den strategischen Rahmen,
- **ISO 27005** vertieft den Informationssicherheitsaspekt,
- **NIST SP 800-30** macht Risikoanalysen praktisch anwendbar
- und **ISO 9001** verankert das Ganze in den operativen Prozessen und der kontinuierlichen Verbesserung.

Wer diese Ansätze kombiniert, schafft eine einheitliche Sprache für Risiko und Qualität – und damit eine Basis, auf der Sicherheit, Resilienz und Leistungsfähigkeit gemeinsam wachsen können.

METHODISCHE UMSETZUNG: RISIKOPROZESS IN SECHS SCHRITTEN

Ein wirksames Risikomanagement folgt einer klaren Logik. Die ISO 31000 definiert dafür einen durchgängigen Prozess, der sich an der PDCA-Systematik (Plan – Do – Check – Act, PDCA) orientiert – bekannt aus ISO 9001 und ISO 27001. Dieser Regelkreis verbindet strategische Ausrichtung, operative Umsetzung und kontinuierliche Verbesserung zu einem lebendigen Steuerungssystem, das Risiken nicht nur dokumentiert, sondern aktiv managt.

Abbildung 1: Risikoprozess (Bild: SECaaS.IT, generiert mit ChatGPT (SORA))

1. Kontext festlegen

Am Anfang steht die Festlegung des Kontexts. Organisationen müssen verstehen, in welchem Umfeld sie agieren: Welche Ziele verfolgen sie, welche regulatorischen Anforderungen gelten, welche internen und externen Faktoren prägen ihre Risikolandschaft?

Dieser Schritt ist weit mehr als ein formaler Auftakt. Er schafft nicht nur die Grundlage für die Bewertung einzelner Risiken, sondern liefert auch direkten Mehrwert für das Unterneh-

Norm/Richtlinie	Zweck	Methodischer Fokus	Stärken	Einsatzbereich
ISO 31000 (2018)	übergreifendes Rahmenwerk für Risikomanagement	Kontext – Identifikation – Analyse – Bewertung – Behandlung – Monitoring	ganzheitlich, strategisch, organisationsweit	für alle Organisationstypen, branchenübergreifend
ISO 27005 (2022)	Spezialisierung für Informationssicherheitsrisiken	Bedrohung – Schwachstelle – Auswirkung (Szenario-Ansatz)	Detailtiefe für IT/IS, Anbindung an ISMS nach ISO 27001	Informationssicherheits- und IT-Risikomanagement
NIST SP 800-30 (2022 Rev. 1)	Leitfaden für Risikoanalyse im IT-Umfeld	System-/Asset-Fokus; Eintrittswahrscheinlichkeit × Schadenshöhe	praktische Beispiele, Heatmaps, enge Verbindung zu Controls	besonders relevant für US-Organisationen, KRITIS und Behörden
ISO 9001 (2015)	Qualitäts- und Chancenmanagement im Rahmen integrierter Systeme	Risiken und Chancen in Prozessen, PDCA-Zyklus, kontinuierliche Verbesserung	Verbindung von Risiko, Qualität und Performance	Qualitäts-, Prozess- und Integrationsmanagement

Tabelle 1: Vergleich zentraler Normen und Leitlinien für das Risikomanagement

men: Wer sich mit dem eigenen Kontext kritisch auseinandersetzt, gewinnt ein realistisches Bild seiner Stärken, Schwächen und Abhängigkeiten – und legt damit die Basis für strategische Entscheidungen. Gleichzeitig führt diese Reflexion zu einem besseren Verständnis der eigenen Prozesse und Schnittstellen.

2. Risiken identifizieren

Im zweiten Schritt werden potenzielle Bedrohungen und Chancen systematisch erfasst – entlang der gesamten Wertschöpfungskette und über alle Unternehmensbereiche hinweg. Dabei kommen Methoden wie Workshops, Szenarioanalysen, Incident-Reviews oder externe Quellen zum Einsatz, zum Beispiel ENISA Threat Landscape oder BSI-Standard 200-3.

Entscheidend ist, Risiken nicht isoliert, sondern auf unterschiedlichen Ebenen zu betrachten. Zwar gibt ISO 31000 keine formale Taxonomie vor, doch in der Praxis hat sich eine dreistufige Einteilung bewährt – in Anlehnung an das COSO-Enterprise-Risk-Management-Framework (COSO ERM):

1. **Strategische Ebene (Entity Level):** Risiken, die das gesamte Unternehmen betreffen, etwa Marktveränderungen, Governance-Fragen oder externe Schocks.
2. **Operative Ebene (Process Level):** Risiken innerhalb von Prozessen, Projekten oder Funktionen – sie betreffen die tägliche Wertschöpfung und Servicequalität.
3. **Projekt- oder Asset-Ebene:** Risiken, die spezifisch einem Projekt, Produkt oder Asset zugeordnet sind, etwa technische Störungen, Lieferverzögerungen oder Systemausfälle.

Diese Kategorisierung hilft, Risiken zielgerichtet zu analysieren und Verantwortlichkeiten klar zuzuordnen.

3. Risiken analysieren

Die Analyse quantifiziert die ermittelten Risiken. Eintrittswahrscheinlichkeit und Schadenshöhe werden typischerweise auf einer Skala von 1 bis 5 bewertet; ihr Produkt ergibt einen Risikowert von 1 bis 25. Eine Heatmap visualisiert diese Werte und zeigt auf einen Blick, wo akuter Handlungsbedarf besteht (siehe Abbildung 2). Die Analyse sollte zudem qualitative Aspekte wie Reputationsschäden, Lieferkettenstörungen oder regulatorische Auswirkungen berücksichtigen.

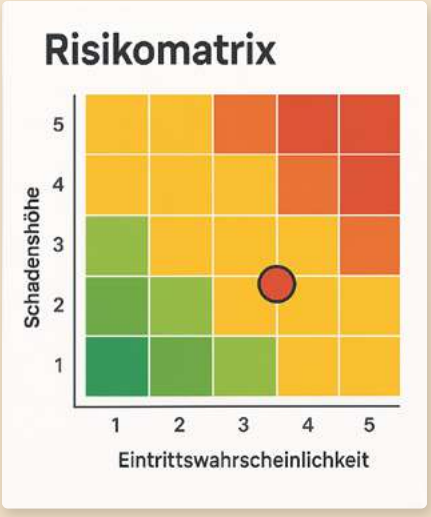


Abbildung 2: Risikomatrix (Bild: SECaaS.IT, generiert mit ChatGPT (SORA))

4. Risiken bewerten und priorisieren

Im nächsten Schritt erfolgt die Bewertung: Welche Risiken überschreiten den definierten Risikoappetit und welche liegen innerhalb der akzeptablen Toleranzgrenzen? Diese Priorisierung

Bild: Nuthawut - stock.adobe.com

entscheidet, wo Ressourcen zuerst eingesetzt werden. Moderne Risiko-Dashboards kombinieren qualitative und quantitative Kennzahlen, um Managemententscheidungen faktenbasiert zu unterstützen.

5. Risiken behandeln

Die Behandlung der Risiken umfasst vier Grundstrategien: vermeiden, vermindern, übertragen oder akzeptieren. Jede Maßnahme wird mit Verantwortlichkeiten, Fristen und Wirksamkeitskriterien im Risikoregister dokumentiert. Dabei ist entscheidend, dass Maßnahmen mit anderen Managementsystemen (zum Beispiel Informationssicherheit, Qualität, Umwelt, Business Continuity) abgestimmt sind – ein Kernelement integrierter Governance-Strukturen.

6. Monitoring und Review

Da sich Risiken ständig verändern, bildet das Monitoring den Abschluss und zugleich den Neubeginn des Zyklus. Risikoparameter werden regelmäßig überprüft, Leistungskennzahlen (Key Performance Indicators, KPIs) wie Mean Time to Recovery (MTTR), Restrisiko oder Anteil kritischer Risiken im roten Bereich dienen als Frühwarnindikatoren. Automatische Benachrichtigungen bei Schwellenwertüberschreitungen helfen, das Management rechtzeitig einzubinden.

Damit wird Risikomanagement zu einem lebendigen Steuerungsprozess, der sich laufend anpasst und verbessert – ganz im Sinne des PDCA-Prinzips. In Verbindung mit dem COSO ERM erhält dieser Prozess zusätzlich strategische Tiefe: COSO verknüpft Risiko, Performance und Berichterstattung zu einem einheitlichen System. So entsteht ein unternehmensweites Risikomanagementsystem (RMS), das sowohl operative als auch regulatorische Anforderungen abdeckt – von ISO über NIS-2 bis hin zu Financial-Audits – und Risiko als integralen Bestandteil moderner Unternehmensführung versteht.

ROLLENBEZUG: WER TRÄGT DIE VERANTWORTUNG?

Ein Risikomanagementsystem lebt nicht von Tabellen oder Tools, sondern von klaren Verantwortlichkeiten. Die besten Methoden bleiben wirkungslos, wenn sie nicht in Rollen und Entscheidungsstrukturen verankert sind. ISO 31000 betont daher den Führungsbezug: Risikomanagement ist keine Stabs- oder Auditfunktion, sondern eine Führungsaufgabe, die das gesamte Unternehmen betrifft.

Die oberste Leitung definiert den Risikoappetit – also das Maß an Risiko, das das Unternehmen bereit ist zu tragen – und legt die Toleranzgrenzen fest. Sie entscheidet über Budgets, Ressourcen und Maßnahmenprioritäten und verankert das Risikomanagement in der strategischen Unternehmensplanung. Regelmäßige Management-Reviews und Dashboards schaffen Transparenz: Sie zeigen Trends, offene Risiken, deren Restwert und die Wirksamkeit von Maßnahmen. So wird Risikomanagement zum Steuerungsinstrument, das Entscheidungen auf Basis objektiver Daten ermöglicht.

Der CISO oder Compliance-Lead sorgt nicht für den operativen Inhalt des Risikoregisters, sondern stellt den Rahmen und die Qualitätssicherung bereit. Er definiert die Methodik, betreut das Risikomanagement-System, prüft die Konsistenz der Bewertungen und unterstützt die Fachbereiche bei der Umsetzung. Die operative Verantwortung für einzelne Risiken verbleibt bei den jeweiligen Risikoverantwortlichen in den Fachabteilungen. Der CISO agiert somit als methodischer Enabler und Qualitätsmanager, der sicherstellt, dass Risiken nach einheitlichen Kriterien erfasst, bewertet und überwacht werden. Er fungiert als Brücke zwischen Management, Compliance und Technik – und sorgt für die Integration mit anderen Governance-Systemen wie Informationssicherheit, Datenschutz oder Lieferantenmanagement.

Die Fachbereiche übernehmen die „First Line of Defense". Sie sind die tatsächlichen Risikoverantwortlichen. Hier entstehen, verändern und materialisieren sich Risiken. Die Fachabteilungen erkennen Schwachstellen und Vorfälle frühzeitig, bewerten deren Auswirkungen auf Prozesse oder Projekte und setzen Maßnahmen um. Ihre Verantwortung reicht von der Risikoidentifikation über die Umsetzung bis zur Dokumentation der Evidenzen – idealerweise direkt im Workflow, etwa über Tickets, Logs oder Abnahmeprotokolle. So entsteht eine durchgängige Beweiskette („Minimal Viable Evidence"), die Nachvollziehbarkeit schafft und Audits erheblich vereinfacht.

Aktivität	Vorstand	CISO/Compliance	Fachabteilungen
Risikobereitschaft festlegen	A/R	C	I
Risikoregister führen	I	A/R	C
Maßnahmen umsetzen	I	C	A/R
Evidenz dokumentieren	I	R	A/R

Tabelle 2: Rollenverteilung im Risikomanagement, A = Accountable, R = Responsible, C = Consulted, I = Informed

Erfolgreiches Risikomanagement ist immer teamübergreifend:

- Die Geschäftsführung legt den Rahmen und die strategische Richtung fest,
- der CISO oder Compliance-Lead steuert die Methodik und die Qualität,
- und die Fachbereiche tragen die Verantwortung für ihre operativen Risiken.

Diese klare Trennung der Verantwortlichkeiten stärkt die Wirksamkeit des Systems und verhindert, dass Risiken in der Organisation „hängen bleiben".

FUNKTIONSTRENNUNG UND DIE „THREE LINES OF DEFENSE"

Nach ISO 31000 und internationalen Best Practices, besonders dem Three-Lines-Modell des Institute of Internal Auditors (IIA), ist es entscheidend, zwischen operativer Verantwortung, methodischer Steuerung und unabhängiger Prüfung zu unterscheiden. Diese Funktionstrennung stellt sicher, dass niemand sein eigenes System prüft oder Risiken bewertet, für die er operativ verantwortlich ist. Besonders in der IT ist dies essenziell, da technische Expertise zwar notwendig, aber nicht automatisch objektiv ist.

Durch die Trennung von Verantwortung, Steuerung und Kontrolle entsteht ein robustes Vier-

Linie	Rolle/Funktion	Hauptaufgabe	Beispiel (IT-Kontext)
1. First Line	Operatives Management/ Fachbereiche	Risiken erkennen, bewerten, Maßnahmen umsetzen	Systemverantwortliche, Projektleiter, Administratoren
2. Second Line	Risiko-, Compliance-, ISMS- oder Datenschutzfunktion	Methoden und Prozesse definieren, Umsetzung begleiten, Qualität sicherstellen	CISO, Compliance Lead, ISB
3. Third Line	interne Revision/Audit	unabhängige Wirksamkeitsprüfung	interne Revision, externer Auditor

Tabelle 3: Die „Three Lines of Defense" im Risikomanagement

Augen-Prinzip, das kognitive Verzerrungen wie Overconfidence oder die Illusion of Control reduziert. Damit wird die Risikobewertung nachvollziehbar, transparent und prüfungssicher – und entspricht zugleich den Erwartungen von Aufsicht, Auditoren und Regulatoren.

PRAXISBEISPIEL: RISIKOANALYSE EINER KRITISCHEN APPLIKATION

Wie sich die zuvor beschriebenen Prinzipien praktisch anwenden lassen, zeigt ein Beispiel aus dem Umfeld einer geschäftskritischen IT-Anwendung. Ein mittelständisches Fertigungsunternehmen betrieb ein zentrales Manufacturing Execution System (MES) zur Steuerung seiner Produktionslinien. Dieses System war der digitale Taktgeber der gesamten Fertigung. Ohne es stand die Produktion still.

Im Rahmen eines systematischen Risikomanagement-Prozesses wurde das Szenario „Ransomware-Angriff auf das MES" analysiert. Die Risikoanalyse erfolgte bewusst nicht intuitiv, sondern methodisch nach ISO 31000: Zunächst wurde das Risiko in den Kontext der Geschäftsziele eingeordnet. Anschließend bewertete das Team gemeinsam mit der IT- und Produktionsleitung die Eintrittswahrscheinlichkeit als mittel (3 von 5) und die Schadenshöhe als sehr hoch (5 von 5) – Produktionsstillstand, Lieferverzug und Vertragsstrafen waren die absehbaren Folgen. Das Ergebnis war ein Risikowert von 15, der deutlich über der definierten Risikobereitschaft des Unternehmens lag.

Damit war klar, es besteht sofort Handlungsbedarf. Das Unternehmen entschied sich für ein Bündel präventiver und reaktiver Maßnahmen. Ein Offsite-Backup wurde eingerichtet, die Netzsegmente der Produktionssysteme voneinander getrennt und gezielte Awareness-Trainings für Administratoren durchgeführt. Ergänzend entstand ein Incident-Response-Playbook, das im Ernstfall Verantwortlichkeiten und Kommunikationswege festlegte.

Diese Schritte wurden nicht als einmalige Aktion verstanden, sondern in das laufende Risikoregister integriert. Der CISO übernahm das Monitoring und definierte den KPI „maximale Wiederanlaufzeit ≤ 12 Stunden". Die Fortschritte und Statusberichte flossen quartalsweise in das Management-Review ein.

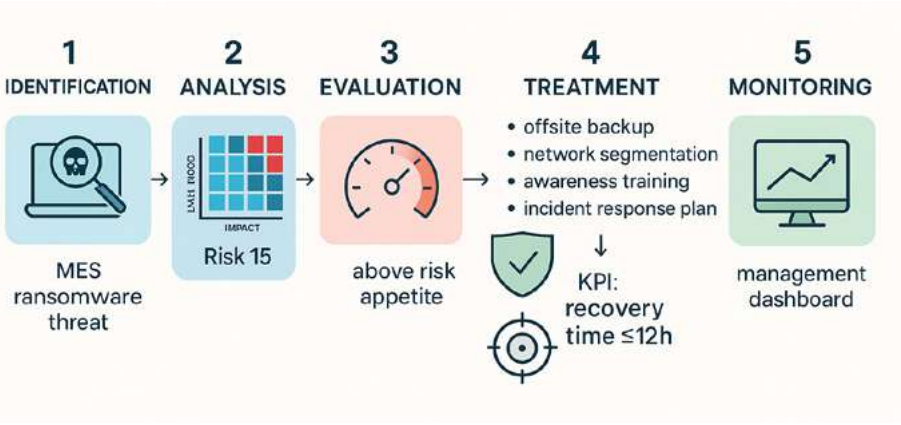


Abbildung 3: ISO 31000 Risk Management Process (Bild: SECaaS.IT, generiert mit ChatGPT (SORA))

Das Ergebnis überzeugte: Das Unternehmen konnte seine Investitionen gezielter priorisieren, den Nachweis gegenüber Auditoren und Kunden strukturiert führen – und vor allem das Vertrauen der Produktionsteams stärken. Das Risiko wurde nicht länger als Bedrohung empfunden, sondern als gesteuerte Größe, die Sicherheit und Planbarkeit schafft.

FAZIT: VOM BAUCHGEFÜHL ZUR STEUERBAREN WIRKUNG

Risikomanagement ist weit mehr als ein Pflichtprogramm für Auditoren. Es ist ein Führungsinstrument. Wer Risiken strukturiert erfasst, bewertet und steuert, gewinnt nicht nur Sicherheit, sondern auch Entscheidungsfähigkeit. ISO 31000 liefert dafür den strategischen Rahmen, der Intuition in Methode verwandelt und Unsicherheit in Handlungsspielräume übersetzt. Statt auf das Bauchgefühl zu vertrauen, schafft ein methodisches Vorgehen Transparenz und Priorität. Risiken werden vergleichbar, Maßnahmen messbar, und die Steuerung wird zur kontinuierlichen Aufgabe. Ergänzend liefern ISO 27005 und NIST SP 800-30 die nötige operative Tiefe, um Informationssicherheits- und IT-Risiken nahtlos einzubetten.

Ein wirksames Risikomanagement beruht auf fünf zentralen Prinzipien:

1. **Rahmen schaffen:** ISO 31000 bildet die strategische Grundlage für Sicherheit, Resilienz und Compliance.
2. **Methode statt Intuition:** Erst systematische Analyse macht Risiken sichtbar und beherrschbar.
3. **Integration statt Insellösung:** ISO 27005 und NIST SP 800-30 ergänzen sich zu einem konsistenten Werkzeugkasten.

4. **Verantwortung leben:** Klare Rollen und Evidenzen sichern die Wirksamkeit – vom Vorstand bis ins Operations-Team.

5. **Risiken steuern, nicht verwalten:** Kennzahlen, Reviews und Eskalationen machen Risiko zum echten Managementinstrument.

So entsteht ein Verständnis von Governance, das Risiken nicht nur mindert, sondern als Impuls für Lernen und Verbesserung nutzt.

Der nächste Artikel der Serie zeigt, wie sich dieses Prinzip weiterdenken lässt – wenn Governance, Internes Kontrollsystem (IKS), Environmental, Social and Governance (ESG) und DORA in einem integrierten Managementsystem zusammengeführt werden. Nur so lassen sich Synergien heben, Aufwände reduzieren und Steuerung wirklich ganzheitlich gestalten. ■

Literatur (Auswahl)

[1] *ISO (2018): ISO 31000:2018 – Risk management — Guidelines. Geneva: International Organization for Standardization. (Bestätigung 2023). www.iso.org/standard/65694.html*

[2] *ISO (2022): ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: International Organization for Standardization. www.iso.org/standard/80585.html*

[3] *NIST (2012): Special Publication 800-30 Rev.1 – Guide for Conducting Risk Assessments. Gaithersburg, MD: National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/30/r1/final*

[4] *ISO (2015): ISO 9001:2015 – Quality management systems — Requirements. Geneva: International Organization for Standardization.*

[5] *ENISA (2025): NIS2 Technical Implementation Guidance. Athens: European Union Agency for Cybersecurity. (Version 1.0, 26 June 2025). www.enisa.europa.eu/publications/nis2-technical-implementation-guidance*

[6] *BSI (2021): IT-Grundschutz-Kompendium – Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz. Bonn: Bundesamt für Sicherheit in der Informationstechnik.*

[7] *IIA (2020): The IIA's Three Lines Model – An update of the Three Lines of Defense. Lake Mary, FL: The Institute of Internal Auditors. www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/*

[8] *COSO (2017): Enterprise Risk Management – Integrating with Strategy and Performance. Durham, NC: Committee of Sponsoring Organizations of the Treadway Commission.*

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

[10] *European Commission (2022): Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA). Brussels: European Commission.*

[11] *ENISA (2023): Threat Landscape 2023 – Cybersecurity Challenges and Trends. Athens: European Union Agency for Cybersecurity.*

[12] *Gartner (2023): Market Guide for Integrated Risk Management. Stamford, CT: Gartner Research.*

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.***

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

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

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.

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

An der Mensch-KI-Schnittstelle entscheidet sich die Zukunft der Cybersicherheit

LERNEN GEGEN DIE LÜCKE

KI-Agenten ziehen in den Arbeitsalltag ein – und erweitern die Angriffsfläche an der Schnittstelle von Mensch und Maschine. Wer Sicherheit strategisch denkt, trainiert deshalb beide Ebenen: Anwender und Agenten. So entsteht eine belastbare Doppelverteidigung, die technische Kontrollen und Verhalten zusammenführt.

Die Cybersicherheitslandschaft steht vor dem größten Umbruch seit den Anfängen des Internets. Künstliche Intelligenz (KI) ist heute fester Bestandteil betrieblicher Abläufe. Laut Schätzungen von Goldman Sachs werden agentische KI-Systeme (AI agents) bis 2030 rund 60 Prozent des Software-Marktwerts ausmachen. Gartner prognostiziert, dass bis 2026 etwa 40 Prozent der Unternehmensanwendungen spezialisierte KI-Agenten integrieren werden – nach weniger als fünf Prozent im Jahr 2024. Damit entsteht eine neue Angriffsfläche, die Sicherheitsstrategien jenseits bekannter Modelle erfordert.

Seit Jahren gilt in der Cybersicherheit ein Grundsatz: Der Mensch ist das schwächste Glied der Kette. Mehr als 60 Prozent aller Sicherheitsvorfälle gehen auf menschliches Fehlverhalten zurück – Phishing und Social Engineering zählen dabei zu den effektivsten Angriffsmethoden.

Mit dem Einzug von KI-Agenten in den Arbeitsalltag verlagert sich nun der Fokus. Sicherheitsverantwortliche müssen nicht mehr nur menschliche Schwächen adressieren, sondern auch die neuen Risiken aus der Interaktion zwischen Mensch und KI berücksichtigen – eine Angriffsfläche, die Cyberkriminelle bereits gezielt ausnutzen.

NEUE ANGRIFFSVEKTOREN DURCH KI-SYSTEME

KI zeigt in der Cybersicherheit eine spannende Doppelrolle: Einerseits ist sie ein mächtiges Verteidigungsinstrument, das Anomalien erkennt, Reaktionen automatisiert und Bedrohungsinformationen mit übermenschlicher Geschwindigkeit verarbeitet. Andererseits nutzen Angreifer dieselbe Technologie, um komplexe Attacken zu entwickeln, und machen KI-Systeme selbst zu lohnenden Zielen.

So setzen sie KI beispielsweise gezielt ein, um täuschend echte Phishingmails zu erstellen, Deepfakes für Social-Engineering-Kampagnen zu generieren oder Aufklärungsaktivitäten zu automatisieren. Gleichzeitig entstehen neue Angriffsmethoden, die speziell darauf abzielen, KI-Systeme selbst zu manipulieren – etwa durch Prompt-Injection, Model Poisoning oder adversarielle Eingaben.

Klassische Sicherheitsansätze konzentrieren sich traditionell auf den Perimeterschutz , also auf Firewalls, Intrusion-Detection-Systeme und

Endpunktschutz. Diese Maßnahmen bleiben relevant, reichen jedoch für die KI-durchdrungene Arbeitsumgebung von heute und morgen nicht mehr aus, denn die entscheidende Sicherheitslücke entsteht an der Schnittstelle zwischen Mensch und KI-Agent. Hier trifft Social Engineering auf künstliche Intelligenz – und es treten Verwundbarkeiten auf, für die bestehende Sicherheitsrahmen bislang keine Antworten bieten.

Beispiele für diese neuen Bedrohungsszenarien sind:

- **Prompt-Injection-Angriffe:** Angreifer gestalten gezielt Eingaben, um KI-Agenten zu manipulieren. Diese können dadurch unautorisierte Aktionen ausführen, Sicherheitskontrollen umgehen oder vertrauliche Informationen preisgeben.
- **Imitation von KI-Agenten:** Cyberkriminelle schleusen gefälschte Agenten in Unternehmensumgebungen ein, die sich als legitime Tools ausgeben und Zugangsdaten oder sensible Informationen abgreifen.
- **Human-AI-Social-Engineering:** Komplexe Täuschungsversuche, die das Vertrauensverhältnis zwischen Mitarbeitenden und KI-Systemen ausnutzen – etwa indem kompromittierte Agenten als interne Quellen oder Kolleginnen und Kollegen auftreten.

DOPPELTE VERTEIDIGUNGSLINIE ERFORDERLICH

Der Einzug von KI-Systemen in die Arbeitswelt beseitigt den Faktor Mensch nicht, sondern er verstärkt ihn. Daher richtet sich der Fokus künftig auf zwei zentrale und besonders anfällige Ebenen der Sicherheit: Die menschliche Ebene erfordert, dass Beschäftigte befähigt werden, KI-Systeme sicher zu nutzen, Manipulationsversuche zu erkennen und KI-generierte Ergebnisse kritisch zu prüfen. Die Agentenebene verlangt, dass KI-Agenten selbst gegen schädliche Eingaben, Datenabflüsse und unautorisierte Aktionen geschützt werden.

Eine wirksame Sicherheitsstrategie verbindet beide Schichten zu einem dualen Schutzkonzept, das Training und technische Absicherung gemeinsam weiterentwickelt. So wie Unternehmen ihre Mitarbeiter über Jahre darin geschult haben, Phishingmails und verdächtige Links zu erkennen, gilt es nun, eine neue Kompetenz aufzubauen: KI-Kompetenz. Diese umfasst nicht nur den sicheren Umgang mit KI-Werkzeugen, sondern auch das Erkennen, wenn solche Systeme fehlgeleitet, manipuliert oder missbraucht werden.

Ein wirksames KI-Sicherheitstraining muss mehrere zentrale Kompetenzen abdecken:

- **Überwachung von Agenten:** Mitarbeiter sollten lernen, Ausgaben von KI-Agenten zu prüfen und zu validieren, besonders bei sicherheitsrelevanten oder geschäftskritischen Entscheidungen.
- **Sichere Eingaben („Prompts“) formulieren:** Teams müssen verstehen, wie sichere Prompts gestaltet werden und welche Eingaben potenziell riskant sind, weil sie das Verhalten eines Agenten manipulieren könnten.
- **Erkennen von Anomalien im Agentenverhalten:** Beschäftigte sollten in der Lage sein, abweichendes oder unerwartetes Verhalten eines KI-Systems zu identifizieren und entsprechend zu reagieren.

ERWEITERTE RISIKOBEWERTUNG NOTWENDIG

Der Aufbau solcher Fähigkeiten ist jedoch nur die eine Seite der Medaille. Ebenso wichtig ist es, bei Risikobewertungen künftig KI-spezifische Schwachstellen mit einzubeziehen. Während klassische Modelle sich auf Nutzerverhalten, Gerätesicherheit und Netzwerkaktivität konzentrieren, erweitert sich der Blick in KI-gestützten Arbeitsumgebungen um neue Kriterien: die Anfälligkeit einzelner Personen für KI-gestützte Angriffe, das Sicherheitsniveau der genutzten KI-Agenten, die Sensitivität der Daten in Mensch-KI-Interaktionen sowie die Auswirkungen eines kompromittierten Agentenverhaltens auf Geschäftsprozesse und Compliance.

Technologie allein löst keine Sicherheitsprobleme. Der menschliche Faktor bleibt – ob im Umgang mit klassischen Systemen oder mit KI-Agenten – entscheidend für die Sicherheitskultur eines Unternehmens. Organisationen sollten daher eine Kultur fördern, die KI aktiv integriert, zugleich aber kritisches Denken und gesunde Skepsis bewahrt. Das bedeutet, Innovation mit KI-Tools zu ermöglichen, ohne den Anspruch aufzugeben, Ergebnisse zu prüfen, zu hinterfragen und zu verifizieren – besonders in sicherheitskritischen Anwendungen.

DIE ZUKUNFT LERNT MIT

Cyberbedrohungen entwickeln sich rasant weiter, und KI beschleunigt sowohl Angriffs- als auch Verteidigungsstrategien. Erfolgreich werden jene Unternehmen sein, die anpassungsfähige, lernende Sicherheitsprogramme etablieren.

Dazu gehört, starre Schulungskonzepte durch dynamische und individuell ausgerichtete Trainings zu ersetzen, die sich kontinuierlich an die Bedrohungslage anpassen. Gleichzeitig sollten Unternehmen KI-Technologien zur Abwehr KI-gestützter Angriffe nutzen und ihre Mitarbeiter befähigen, als kompetente Partner in diesem technologischen Wettlauf zu agieren.

Die Grenze zwischen Mensch und KI in der Cybersicherheit wird zunehmend verschwimmen. Unternehmen, die diese Entwicklung frühzeitig erkennen und in ein umfassendes Training an der Mensch-KI-Schnittstelle investieren, sichern sich eine resiliente Sicherheitsposition in einer Zeit tiefgreifender technologischer Veränderungen.

Die Botschaft ist klar: Cybersicherheit im KI-Zeitalter bedeutet nicht mehr, Systeme vor Menschen oder Menschen vor Systemen zu schützen – sondern die Interaktion zwischen beiden sicher zu gestalten. Denn in dieser Verbindung liegt zugleich die größte Schwachstelle und das größte Potenzial zur Verteidigung. ■

STUART CLARK
ist ein erfahrener Sicherheitsexperte mit über 25 Jahren Berufserfahrung. Als Vice President Product Strategy bei KnowBe4 treibt er die Weiterentwicklung der Produkte im Bereich Künstliche Intelligenz und Human Risk Management+ (HRM+) sowie darüber hinaus voran.

Mehr Bedrohungen, weniger Personal, neue Werkzeuge

SECURITY OPERATIONS UNTER DRUCK

Steigende Bedrohungslagen, zunehmender Personalmangel und komplexe IT-Landschaften setzen viele Security-Teams unter Druck. Der Einsatz von künstlicher Intelligenz (KI) soll Abhilfe schaffen. Doch nur im Zusammenspiel mit standardisierten Prozessen und realistischen Erwartungen entstehen belastbare Ergebnisse.

Security Operations (SecOps) gelten als Taktgeber der digitalen Unternehmenssicherheit. Gleichzeitig stehen sie exemplarisch für den Druck, unter dem die Branche heute arbeitet. Die Angriffslage wird komplexer, die Infrastruktur verteilt sich auf Rechenzentren, Public-Cloud und Edge, während die Personaldecke dünn bleibt. In dieser Situation gelten Automatisierung und künstliche Intelligenz als Hebel, um Reaktionszeiten zu verkürzen, Fehlalarme einzuhegen und Entscheidungen datenbasiert zu treffen.

Laut Studien aus den Jahren 2024 und 2025 prägen drei Entwicklungen die Agenda in den Security Operations Centern (SOCs): Konsolidierung von Werkzeugen, KI-Einsatz in Verteidigung und Angriff sowie cloudzentrierte Betriebsmodelle. Die Wirksamkeit dieser Ansätze hängt allerdings vom Zusammenspiel aus Technologie, Standardisierung der Abläufe und realistischem Erwartungsmanagement ab.

DIE LAGE IM SOC

In hybriden Umgebungen vervielfachen sich Sichtfelder und Meldewege. Sicherheitsereignisse entstehen in Identitätssystemen, Endpunkten, Cloud-Control-Planes, Software-as-a-Service-(SaaS)-Applikationen und industriellen Netzen. Die Folge sind heterogene Daten und inkonsistente Arbeitsweisen zwischen Teams. Viele Führungskräfte reagieren darauf mit der Konsolidierung von Plattformen, um Daten schneller zusammenzuführen und den Betrieb überschaubar zu halten.

Analysen raten ausdrücklich dazu, zentrale Funktionen zu bündeln und Lücken gezielt mit Speziallösungen zu schließen, damit Organisationen anpassungsfähig bleiben und kein riskantes Abhängigkeitsverhältnis zu einzelnen Herstellern entsteht. Diese Position verbindet technologische und betriebswirtschaftliche Perspektiven, da Umstiegs- und Schulungskosten bei Wechseln realistisch zu kalkulieren sind.

KI: BESCHLEUNIGER MIT HAUSAUFGABEN

Ferner entsteht durch künstliche Intelligenz eine neue Dynamik im operativen Alltag. Sie wirkt sich im SOC auf drei Ebenen aus: Erstens priorisiert sie Vorfälle anhand historischer Muster, Kontextdaten und Angriffstaktiken. Zweitens strukturiert sie die Bearbeitung mit Vorschlägen für Untersuchung, Eindämmung und Wiederherstellung, inklusive automatischer Dokumentation. Drittens hilft sie, Wissenslücken zu schließen, indem sie Anreicherungen aus Threat Intelligence, Asset-Kontext und Identitätsrisiken zusammenführt. Das spart Zeit, reduziert Kontextwechsel und entlastet besonders kleine Teams.

Gleichzeitig wandert KI als Angriffsvektor in die Bedrohungslandschaft. Generative Werkzeuge senken Einstiegshürden für Phishing-Kampagnen, Social Engineering und das Zusammenspiel mehrstufiger Angriffe. Analysten empfehlen deshalb, Reaktionsverfahren zeitlich zu verdichten und die Automatisierungstiefe zu erhöhen, damit Verteidigungsschritte mit KI-gestützten Angriffsgeschwindigkeiten Schritt halten können.

VON CLOUD-NATIV BIS API-SICHERHEIT

Während KI die operative Effizienz steigert, verändert sich auch der technische Unterbau der Security Operations. Cloudnative SOC-Services bieten Skalierbarkeit und ermöglichen den Betrieb über Standorte und Zeitzonen hinweg. Das ist eine große Hilfe bei Personalmangel. Parallel steigt die Relevanz von Security Orchestration, Automation and Response (SOAR), weil Playbooks Routinearbeiten übernehmen und die Fehleranfälligkeit senken. Zero-Trust-Prinzipien wandern aus Strategiepapieren in die Umsetzung, besonders mit Blick auf Identitäten, Gerätezustände und Zugriffsentscheidungen in Echtzeit.

Bild: YAREN | LiliGraphie - stock.adobe.com

Auch Anwendungsteams stehen vor neuen Aufgaben: Der anhaltende API-Boom erhöht die Angriffsfläche. Entsprechend müssen Organisationen ihre Reifegrade in API-Inventarisierung, Authentisierung, Ratenbegrenzung und Laufzeitüberwachung ausbauen.

Prognosen sehen zusätzlich den Umgang mit Prompt-Injection-Risiken in KI-Schnittstellen sowie die Vorbereitung auf Post-Quantum-Kryptografie auf der Roadmap vieler Unternehmen. Diese Entwicklungslinien sind industrieübergreifend sichtbar und betreffen sowohl klassische IT als auch produktionsnahe Umgebungen.

MESSBARE VERBESSERUNGEN STATT HEILSVERSPRECHEN

Nach der strukturellen und technologischen Neuausrichtung stellt sich die Frage, wie sich deren Wirksamkeit belegen und dauerhaft steigern lässt. Entscheider erwarten von Investitionen in Security Operations nachweisbare Verbesserungen – etwa bei mittleren Erkennungs- und Reaktionszeiten, beim Anteil falsch positiver Meldungen und bei der Wiederherstellungsfähigkeit kritischer Dienste. Gleichzeitig wächst der Druck, Tool-Landschaften zu konsolidieren. Studienergebnisse aus dem Jahr 2025 zeigen eine hohe Dynamik in der Plattformvereinheitlichung und eine breite Nutzung KI-gestützter Sicherheitsfunktionen im Alltag.

Diese Entwicklungen sind kein Heilsversprechen, sondern ein Hinweis darauf, dass Organisationen messbare Fortschritte erzielen, wenn Governance, Prozesse und Technologie gemeinsam betrachtet werden. Besonders wirkungsvoll ist es, wenn Sicherheits-, IT- und Fachbereiche Konsolidierungsentscheidungen abgestimmt treffen und Qualifizierungsprogramme parallel zur Plattformstrategie laufen. Ohne kontinuierliches Upskilling bleibt der Produktivitätsgewinn neuer Werkzeuge begrenzt.

VIER BAUSTEINE FÜR ROBUSTE SOC-BETRIEBE

Damit Security Operations dauerhaft wirksam bleiben, braucht es jedoch mehr als Konsolidierung und Automatisierung. Erstens ist Datenzugang entscheidend: Telemetrie aus Identität, Endpunkten, Netz, Cloud-Protokollen und Geschäftsanwendungen muss zusammengeführt werden, damit Erkennung, Korrelation und forensische Nachvollziehbarkeit funktionieren.

Zweitens braucht es klare Verfahren. Standardisierte Playbooks für Triage, Eindämmung und Wiederherstellung verkürzen Einarbeitungszeiten und machen Ergebnisse reproduzierbar.

Drittens ist Kontext Pflicht. Asset-Kritikalität, Compliance-Verpflichtungen und Geschäftsprozesse beeinflussen Prioritäten erheblich, weshalb reine Alarmzahlen wenig aussagekräftig sind.

Viertens muss Automatisierung sicher eingeführt werden. Jede automatisierte Maßnahme erfordert testbare Freigabekriterien, Rollback-Pläne und Transparenz darüber, wann ein Mensch die Kontrolle übernimmt. Diese vier Bausteine erhöhen die Robustheit von SOC-Betrieben stärker als zusätzliche Einzellösungen.

PRODUKTAUSWAHL NACH WERTSCHÖPFUNGSKETTE

Bei der Produktauswahl lohnt sich ein nüchterner Blick auf die Wertschöpfungskette des SOC. Erfassungs- und Integrationsschicht, Analytik und Korrelation, Orchestrierung und Reaktion sowie Wissensmanagement sind die zentralen Leitplanken. Unternehmen fahren gut damit, Kernfunktionen auf einer Plattform zu konsolidieren und Spezialbedarfe wie industrielle Netzwerke, Hochsicherheitszonen oder branchenspezifische Compliance mit Zusatzlösungen abzudecken.

Ebenso wichtig ist die Migrationsfähigkeit. Wer heute konsolidiert, sollte Umstiegsszenarien und Exit-Klauseln von Beginn an planen, damit technologische und vertragliche Pfade offenbleiben. Diese Vorgehensweise wird in strategischen Leitfäden für 2025 ausdrücklich empfohlen, um Flexibilität, Kostenkontrolle und Resilienz auszubalancieren.

RESILIENZ ALS UNTERNEHMENSZIEL

Technologie beschleunigt, löst aber nicht automatisch strukturelle Probleme. Deshalb gehört zu jeder technischen Transformation ein Lernpfad für Analystinnen und Analysten, ein Steuerungsmodell für Kennzahlen und ein klarer Auftrag an die Führung, Reaktionsfähigkeit als Unternehmensziel zu verankern.

Resilienz bedeutet in diesem Kontext, dass Unternehmen Störungen antizipieren, absorbieren, sich anpassen und schnell wiederherstellen können. Dieser Anspruch ist erreichbar, wenn das SOC nicht als isolierte Technikzelle agiert, sondern als Teil einer unternehmensweiten Betriebsstrategie. Branchenverbände ordnen diese Entwicklung als „Megatrend" ein, der sich in den kommenden Jahren weiter verstärken dürfte.

Sicherheitsabteilungen brauchen heute mehr als zusätzliche Tools. Sie benötigen Datenzugang ohne Reibungsverluste, klar definierte Abläufe und Automatisierung, die nachvollziehbar und sicher greift. KI kann hier ein tragender Baustein sein. Sie priorisiert besser, strukturiert Reaktionen und dokumentiert fundiert. Die fachliche Verantwortung bleibt dennoch beim Menschen.

Organisationen, die technologische Innovation mit konsolidierten Plattformen, gezielter Weiterbildung und messbaren Zielen verbinden, erhöhen ihre Resilienz spürbar und bleiben auch in einer beschleunigten Bedrohungslage handlungsfähig. ■

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.

Relativer Personenbezug, USA-Transfers, Schadensersatz

DREI EU-URTEILE VERSCHÄRFEN DATENSCHUTZPFLICHTEN FÜR UNTERNEHMEN

Anfang September haben europäische Gerichte den rechtlichen Rahmen für personenbezogene Daten präzisiert. Die Entscheidungen haben direkte Folgen für datenintensive Branchen wie Krankenhäuser, Medizintechnik, Forschung, Versicherungen und Banken.

In der ersten Septemberwoche 2025 haben der Europäische Gerichtshof (EuGH) und das Gericht der Europäischen Union (EuG) eine Reihe von Grundsatzurteilen zum Datenschutzrecht gefällt. Sie betreffen den gesamten Lebenszyklus personenbezogener Daten – von der Erhebung und Verarbeitung über internationale Datentransfers bis hin zur Haftung bei Datenschutzverstößen. Die Entscheidungen schaffen zwar teilweise rechtliche Klarheit in zentralen Fragestellungen, verschärfen zugleich aber die Anforderungen an Verantwortliche und Auftragsverarbeiter.

Besonders betroffen sind Organisationen mit umfangreicher Datenverarbeitung und sensiblen Informationen, etwa Krankenhäuser, Medizintechnik (MedTech), Forschungseinrichtungen sowie Versicherer und Banken. Für sie stellt sich vor allem die Frage, welche bestehenden Prozesse, Verträge und Risikobewertungen jetzt pragmatisch anzupassen sind.

Wir fassen die wichtigsten Kernaussagen zusammen und analysieren, welche praktischen Konsequenzen sich daraus für die datenintensiven Branchen ergeben.

RELATIVER PERSONENBEZUG: PERSPEKTIVE DES EMPFÄNGERS ENTSCHEIDET

Im Verfahren des Einheitlichen Abwicklungsausschusses (Single Resolution Board, SRB), der als europäische Behörde für die Abwicklung von großen Kreditinstituten zuständig ist, ging es um die Frage, wann Daten als personenbezogen einzustufen sind und aus wessen Perspektive dies zu beurteilen ist (EuGH, Urt. v. 04.09.2025 – Az. C-413/23 P). Der SRB hatte Fragebögen an Anteilseigner und Gläubiger einer europäischen Bank verteilt und die Antworten pseudonymisiert an eine Wirtschaftsprüfungsgesellschaft übermittelt. Betroffene beschwerten sich, weil sie nicht über die Weitergabe informiert wor-

den waren. Der SRB argumentierte, die pseudonymisierten Daten seien für den Wirtschaftsprüfer keine personenbezogenen Daten.

Entscheidend sei die Sicht des Verantwortlichen. Solange der Empfänger keine Mittel habe, die nach allgemeinem Ermessen wahrscheinlich für eine Re-Identifizierung genutzt werden könnten, liege kein personenbezogenes Datum vor. Damit wurde die Theorie des relativen Personenbezugs ausdrücklich bestätigt. Maßgeblich ist nicht allein das eingesetzte Verfahren, sondern ob der konkrete Empfänger realistische, zumutbare Re-Identifizierungsmöglichkeiten hat. Fehlen diese, gelten die übermittelten Daten für ihn nicht als personenbezogen – auch wenn sie für den ursprünglichen Verantwortlichen noch personenbeziehbar sind.

Für Unternehmen und öffentliche Einrichtungen bedeutet dies, dass bestehende Risikobewertungen, Pseudonymisierungs- und Anonymisierungsverfahren (vor allem bei mehreren beteiligten Parteien) – etwa im Rahmen von Datenschutz-Folgenabschätzungen – überprüft und gegebenenfalls angepasst werden sollten. Von zentraler Bedeutung sind Maßnahmen, die eine Re-Identifizierung (RE-ID) natürlicher Personen wirksam verhindern. Eine Re-Identifizierung liegt vor, wenn pseudonymisierte oder vermeintlich anonymisierte Daten wieder einer Person zugeordnet werden können. In diesem Fall gelten sie für den jeweiligen Empfänger erneut als personenbezogene Daten und unterliegen folglich dem Schutz der Datenschutzgrundverordnung (DSGVO).

KONKRETE ANFORDERUNGEN FÜR GESUNDHEIT, FORSCHUNG UND FINANZBRANCHE

- **Gesundheitseinrichtungen und Forschung:** In Gesundheitseinrichtungen treffen hohe Schutzbedarfe auf komplexe Versorgungs- und Studienprozesse. Relevante Maßnahmen sind klar getrennte Datenströme zwischen Versorgung, Forschung und Dienstleistern, strikte Schlüsselverwaltung und vertragliche Re-Identifizierungsverbote. Die Idee einer relativen Anonymisierung hat durch das Urteil erneut an Bedeutsamkeit gewonnen. Entscheidend ist, dass Empfänger keinen Zugriff auf Re-ID-Hilfsmittel (Schlüssel, Zuordnungstabellen, externe Referenzdaten) haben. Verträge mit IT-Dienstleistern und Laboren sollten dies ausdrücklich festhalten. Da die Daten beim Dienstleister vielfach nicht mehr als personenbezogen gelten, sollten die Verträge angepasst und aktualisiert werden, um sicherzustellen, dass keine gegen die DSGVO verstoßende Verarbeitung erfolgt. So sollte etwa eine Vermischung von Informationen aus unterschiedlichen Quellen (etwa verschiedenen Nutzern oder Geräten) durch strikt getrennte Datenströme verhindert werden. Außerdem ist jeglicher Zugriff auf Zuordnungstabellen zu unterbinden, da solche Tabellen eine Re-Identifizierung ermöglichen würden.
- **MedTech:** Bei MedTech, Software as a Medical Device (SaMD) und KI-Diagnostik entstehen Re-Identifizierungsrisiken vor allem in der Telemetrie, beim Logging und im Support. Sinnvoll sind datenflussbezogene Trennungen zwischen Produktbetrieb, Fehleranalyse und Analytics, eine klare Schlüsselhoheit beim Verantwortlichen sowie Auditklauseln für Dritte. Zusätzlich sollte geprüft werden, ob ein KI-Modell aus seinen Ergebnissen Rückschlüsse auf einzelne Personen zulässt (Model-Inversion-Risiko). Protokolldaten sollten nur zweckgebunden und zeitlich begrenzt vorgehalten werden.
- **Versicherungen und Finanzdienstleistungen:** In Scoring, Underwriting und Betrugsprävention wird häufig mit pseudonymisierten Risikodaten gearbeitet. Der bestätigte relative Personenbezug ermöglicht Analysen beim Dienstleister, sofern Re-Identifizierung praktisch ausgeschlossen und vertraglich untersagt ist. Proxy-Merkmale und Datenanreicherungen aus Drittquellen sind eng zu kontrollieren und regelmäßig zu auditieren.

USA-TRANSFERS: ANGEMESSENHEITSBESCHLUSS VORLÄUFIG BESTÄTIGT

Die nächste Entscheidung betrifft die Frage, wann personenbezogene Daten in ein Drittland außerhalb des Europäischen Wirtschaftsraums (EWR) übermittelt werden dürfen (EuG, Urt. v. 03.09.2025 – Az. T-553/23). Geklagt hatte Philippe Latombe, ein französischer Abgeordneter und Mitglied der französischen Datenschutzaufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL).

Latombe wandte sich mit seiner Klage gegen den Durchführungsbeschluss der EU-Kommission, der die Angemessenheit des Datenschutzniveaus in den USA auf Grundlage des sogenannten EU-U.S. Data Privacy Frameworks festgestellt hatte. Zentrales Argument der Kommission war, dass die Einrichtung des sogenannten

Datentransfers in die USA bleiben vorerst zulässig.

Die Hürden für Schadensersatzansprüche sinken weiter. Unternehmen und öffentliche Stellen müssen nun damit rechnen, dass beinahe jeder DSGVO-Verstoß eine Schadensersatzforderung nach sich ziehen kann.

Data Protection Review Courts (DPRC) angemessene Verfahrensgarantien für europäische Bürgerinnen und Bürger gewährleiste.

Latombe griff den Durchführungsbeschluss vor allem damit an, dass der DPCR kein unparteiisches und unabhängiges Gericht sei. Außerdem sei die massenhafte Datenverarbeitung („Bulk Collection") durch amerikanische Geheimdienste rechtswidrig.

Überraschend ließ das EuG die Klage zu und bestätigte den Angemessenheitsbeschluss. Dabei stärkte es zwar die Rechte der Betroffenen, hielt den Beschluss insgesamt jedoch für wirksam – wenn auch auf teilweise wenig überzeugender Grundlage. Beobachter rechnen deshalb mit einem Rechtsmittel Latombes oder weiteren Klagen von Datenschutzorganisationen (etwa der NGO „None of Your Business"). Für die Praxis gilt: Der Angemessenheitsbeschluss für die USA steht derzeit, bleibt aber politisch und rechtlich umstritten. Mittelfristig dürfte letztlich der EuGH über den Fortbestand des Data Privacy Frameworks entscheiden.

Was bedeutet das operativ? Datentransfers in die USA bleiben vorerst zulässig. Unternehmen sollten eine aktuelle Data-Privacy-Framework-(DPF)-Zertifizierung ihrer US-Dienstleister dokumentieren, auf DPF gestützte Transfers sauber kennzeichnen und Standardvertragsklauseln als Fallback vorhalten. So bleiben Wechseloptionen verfügbar, falls sich die Rechtslage ändert.

DOKUMENTATIONS- UND VORSORGEPFLICHTEN BEI DRITTLANDTRANSFERS

Forschungseinrichtungen, Medizintechnikunternehmen sowie Versicherungs- und Finanzdienstleister werten Daten aus, häufig unter Einbindung externer Dienstleister und – aus Effizienz- oder Spezialisierungsgründen – auch in Drittstaaten wie den USA. Durch die erstinstanzliche Entscheidung des EuG erhalten sie zumindest vorübergehend eine belastbare Orientierung bei diesen Transfers. Gleichwohl sollte den Unternehmen bewusst sein, dass dem Kläger weiterhin ein Rechtsmittel offensteht.

Unternehmen, die personenbezogene Daten in die USA übermitteln, sollten daher den Fortbestand des Angemessenheitsbeschlusses für die USA genau verfolgen, ihre Diensteanbieter regelmäßig auf eine aktuelle DPF-Zertifizierung prüfen und gegebenenfalls vorab Alternativen vertraglich absichern, um im Fall einer etwaigen gegenteiligen EuGH-Entscheidung Datentransfers rechtzeitig zu stoppen und Haftungsrisiken vorzubeugen.

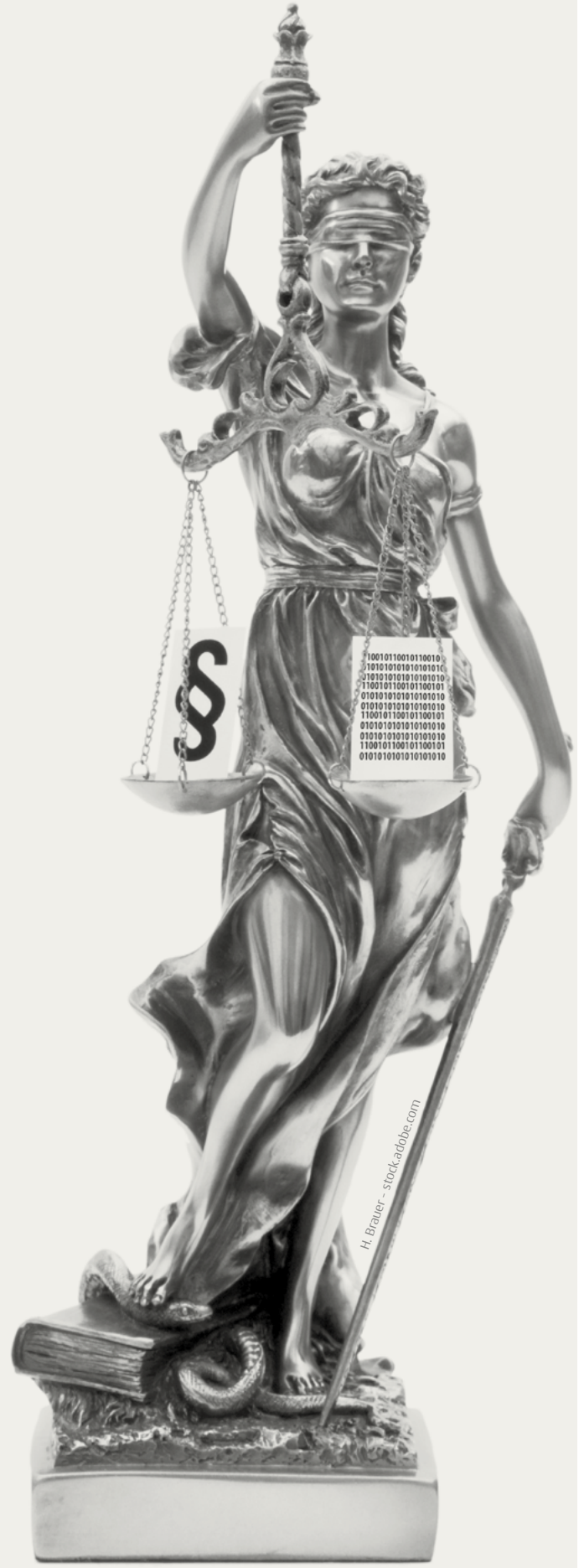
Gleichzeitig ist es essenziell, sämtliche Datenübermittlungen zu dokumentieren – also festzuhalten, welche Daten übermittelt werden, zu welchem Zweck und auf welcher Rechtsgrundlage. Darüber hinaus sollten Unternehmen frühzeitig alternative Maßnahmen vorbereiten, um ein angemessenes Datenschutzniveau sicherzustellen, zum Beispiel zusätzliche vertragliche Garantien sowie klar definierte Fallback-Prozesse für den Wechsel auf Standardvertragsklauseln oder EU-basierte Anbieter.

SCHADENSERSATZ: NEGATIVE GEFÜHLE REICHEN AUS

Die dritte Entscheidung gehört zu einer Reihe von Urteilen deutscher und europäischer Gerichte, die klären, wann Betroffene Anspruch auf Schadensersatz nach Art. 82 DSGVO haben (EuGH, Urt. v. 04.09.2025 – Az. C-655/23). Im vorliegenden Fall ging es um einen Bewerber, der über das berufliche Netzwerk XING Gehaltsverhandlungen mit der Quirin Privatbank geführt hatte. Die Bank verschickte die Absage versehentlich an einen ehemaligen Kollegen des Bewerbers. Dieser klagte auf Schadensersatz wegen der erlittenen Bloßstellung.

Die Gerichte sprachen in den Instanzen teils sowohl Unterlassungs- als auch Schadensersatzansprüche zu, teils nur Unterlassung. Schließlich legte der Bundesgerichtshof (BGH) dem EuGH sechs Fragen zur Auslegung vor. Der EuGH entschied unter anderem, dass auch negative Gefühle wie Unmut, Sorge, Angst oder Scham immaterielle Schäden nach der DSGVO darstellen, die daher zu kompensieren sind.

Die Entscheidung verdeutlicht, dass die Hürden für Schadensersatzansprüche weiter sinken. Unternehmen und öffentliche Stellen müssen nun damit rechnen, dass beinahe jeder DSGVO-Verstoß eine Schadensersatzforderung nach sich ziehen kann. Dies gilt auch für die zuvor diskutierten Konstellationen – etwa wenn sich ein Pseudonymisierungskonzept in der Praxis als



unzureichend erweist oder Daten unrechtmäßig in ein unsicheres Drittland übermittelt werden. Der EuGH stellte zugleich klar, dass bereits negative Gefühle wie Sorge, Ärger oder Scham als immaterieller Schaden im Sinne von Art. 82 DSGVO anerkannt werden können – vorausgesetzt, deren Vorliegen und konkrete nachteilige Folgen sind belegt. Eine Erheblichkeitsschwelle ist nicht erforderlich.

Ferner enthält die DSGVO keinen eigenständigen präventiven Unterlassungsanspruch. Mitgliedstaaten dürfen jedoch nationale Unterlassungsregelungen vorsehen. Ein vorbeugender Unterlassungsanspruch lässt sich nicht unmittelbar aus der DSGVO ableiten; stattdessen können Betroffene über Art. 17 und 18 DSGVO Löschung oder Einschränkung der Verarbeitung verlangen. Für die Bemessung des Schadensersatzes kommt es allein auf die Auswirkungen beim Betroffenen an; weder Verschulden noch nationale Abhilfemaßnahmen dürfen kompensationsmindernd berücksichtigt werden.

Präventive Maßnahmen sind unverzichtbar, um Datenschutzverstöße möglichst zu verhindern oder zumindest das Ausmaß des Schadens zu begrenzen

PRÄVENTIONSMAßNAHMEN UND KOMMUNIKATIONS-STRATEGIEN ERFORDERLICH

Gerade im Gesundheits- und Forschungsbereich können Datenschutzverletzungen erhebliche immaterielle Schäden verursachen. Bereits das Bekanntwerden sensibler Informationen oder der Verlust des Vertrauens in die Datenverarbeitung kann einen kompensationspflichtigen Schaden darstellen. Um dies zu vermeiden, sind präventive Maßnahmen unverzichtbar, um Datenschutzverstöße möglichst zu verhindern oder zumindest das Ausmaß des Schadens zu begrenzen. Besonders anfällig hierfür sind Gesundheitseinrichtungen aufgrund der umfangreichen Verarbeitung von Gesundheitsdaten nach Art. 9 DSGVO. Bei Verstößen mit solchen Daten drohen besonders gravierende Folgen, sodass eine ausgefeilte Prävention unerlässlich ist, um Schadensersatzansprüche zu verhindern.

Die Entscheidungen des EuGH und des EuG schaffen Klarheit in lange umstrittenen Fragen und zeigen zugleich, dass die rechtlichen Anforderungen zwar flexibler, aber auch anspruchsvoller werden.

Falls es dennoch zu einem Datenschutzvorfall kommt, sollten Verantwortliche klare interne Abläufe etablieren – von technischen Sofortmaßnahmen über die rechtliche Bewertung bis hin zur sensiblen, transparenten Kommunikation mit den Betroffenen. Andernfalls drohen erhebliche Reputations- und Haftungsrisiken. Eine offene und sachliche Kommunikation kann die Schadenshöhe wesentlich begrenzen. Für forschende Einrichtungen und MedTech-Unternehmen bedeutet dies insbesondere, Support- und Logging-Zugriffe strikt zu steuern, Protokolldaten nur zweckgebunden und zeitlich begrenzt zu speichern und die Rollen- und Berechtigungskonzepte regelmäßig zu auditieren. Versicherer und Banken sollten zusätzlich Fehladressierungen in der Korrespondenz durch Vier-Augen-Prinzip und Adressvalidierung minimieren sowie Scoring-Erläuterungen transparent dokumentieren.

Zudem sollten Unternehmen berücksichtigen, dass die DSGVO selbst keinen eigenständigen Anspruch auf vorbeugende Unterlassung kennt. Allerdings können Betroffene nach deutschem Recht – etwa über § 1004 Bürgerliches Gesetzbuch (BGB) analog in Verbindung mit Art. 6 ff. DSGVO – auf Unterlassung klagen, sofern eine rechtswidrige Datenverarbeitung droht. Die Gefahr entsprechender präventiver Klagen ist daher real und muss im Risikomanagement berücksichtigt werden. Praktisch empfiehlt sich eine dokumentierte Eskalationskette mit Zuständigkeiten, Fristen und Kommunikationsleitlinien, damit Unterlassungs-, Lösch- oder Einschränkungsverlangen nach Art. 17 und 18 DSGVO zeitnah und nachweisbar bearbeitet werden können.

FAZIT UND HANDLUNGSEMPFEHLUNGEN

Die Entscheidungen des EuGH und des EuG schaffen Klarheit in lange umstrittenen Fragen und zeigen zugleich, dass die rechtlichen Anforderungen zwar flexibler, aber auch anspruchsvoller werden.

Die Bestätigung des relativen Personenbezugs unterstreicht die Bedeutung wirksamer Pseudonymisierungs- und Anonymisierungskonzepte. Verantwortliche sollten fortlaufend prüfen, welche Möglichkeiten zur Re-Identifizierung beim Empfänger bestehen, und sämtliche technischen sowie organisatorischen Schutzmaßnahmen sorgfältig dokumentieren, um Rechtssicherheit zu gewährleisten und Haftungsrisiken zu minimieren.

Die Bestätigung des Data Privacy Frameworks verschafft Unternehmen vorübergehend Stabilität bei internationalen Datenflüssen. Unternehmen sollten jedoch überprüfen und dokumentieren, ob ihre US-Dienstleister DPF-zertifiziert sind. Zudem sind ein kontinuierliches Monitoring der Rechtslage und die Vorbereitung von Alternativlösungen – etwa Standardvertragsklauseln – ratsam, um auf künftige Änderungen flexibel reagieren zu können.

Die Anerkennung der Ersatzfähigkeit immaterieller Schäden bedeutet für Unternehmen, dass sie besonders vorsichtig mit personenbezogenen Daten umgehen müssen, da schon geringfügige Beeinträchtigungen Schadensersatzansprüche auslösen können. Darüber hinaus sollten sie ihr Datenschutzmanagement und ihre Löschprozesse optimieren, um Unterlassungsansprüche nach nationalem Recht sowie zukünftige Schäden zu vermeiden. ■

ILAN LEONARD SELZ
ist seit 2018 Rechtsanwalt bei Schürmann Rosenthal Dreyer und spezialisiert auf Datenschutzrecht, IT- und Telekommunikationsrecht sowie auf regulatorische Anforderungen im technologiegetriebenen und datenintensiven Umfeld. Er ist zertifizierter Datenschutzbeauftragter (CIPP/E).

www.srd-rechtsanwaelte.de

FLORIAN SCHAUTIES
ist Diplom-Jurist und seit 2025 wissenschaftlicher Mitarbeiter bei Schürmann Rosenthal Dreyer. Sein Tätigkeitsschwerpunkt liegt im Datenschutzrecht, IT- und Telekommunikationsrecht.

www.srd-rechtsanwaelte.de

Online-Schulungen IT-Sicherheit

Themen	Referenten
Incident-Response-Maßnahmen – Auf Sicherheitsvorfälle optimal reagieren	Dominik Strauß
KI im Kontext der Cybersecurity	Alexander Jaber
KI unter Kontrolle – ISO/IEC 42001 als Wegweiser für systematisches KI-Management	Hendrik Schlademann
KI-Verordnung – Geltungsbeginn am 2. Februar 2025: KI-Kompetenz und verbotene Praktiken	Alexander Forssman
KI-Verordnung – Neue Vorschriften ab dem 2. August 2025 zu GPAI & Sanktionen	Alexander Forssman
Künstliche Intelligenz im Betrieb – Regulatory Mapping: (Daten-)Arbeitsrecht	Ralf Bruns, Kinga Möller
ISO 27001 Foundation Kurs – PECB zertifiziert	Alexander Jaber

10 % Rabatt für <kes>+ Abonnenten

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

Wie kognitive Verzerrungen Sicherheitsentscheidungen sabotieren

DENKEN IN FALLEN

Trotz steigender Budgets für Cybersicherheit treffen selbst erfahrene IT-Experten systematische Fehlentscheidungen – nicht aus Unwissenheit, sondern wegen kognitiver Verzerrungen. Denn Ankereffekte, Gruppendenken oder die Kontrollillusion beeinflussen die Risikowahrnehmung, die Budgetplanung und strategische Weichenstellungen erheblich. Wer langfristig resilient bleiben will, muss diese „Denkfallen" gezielt adressieren: durch strukturierte Entscheidungsprozesse, heterogene Teams und eine Sicherheitskultur, die Widerspruch zulässt.

Die globalen Ausgaben für Cybersicherheit sollen laut IDC bis 2028 auf fast 400 Milliarden US-Dollar steigen, in Deutschland werden laut Branchenverband BITKOM bereits über zehn Milliarden Euro investiert.[2,7] Dennoch oder gerade deswegen professionalisieren sich Cyberkriminelle immer weiter: Sie agieren arbeitsteilig, hochspezialisiert und nutzen mit Cybercrime-as-a-Service und künstlicher Intelligenz (KI) zunehmend industrielle Strukturen.[5,6] Das FBI schätzt, dass rund 90 Prozent aller cyberbezogenen Delikte nicht gemeldet werden.[9] Dieses Dunkelfeld verzerrt die Risikowahrnehmung erheblich und erschwert eine realistische Einschätzung der Bedrohungslage.

Während sich viele Investitionen auf technologische Aspekte konzentrieren, rückt der menschliche Faktor häufig in den Hintergrund – obwohl er eine zentrale Angriffsfläche darstellt. Die Wirksamkeit von Cybersicherheitsmaßnahmen hängt maßgeblich vom Verhalten der Menschen ab. Doch viele unterschätzen ihre eigene Verwundbarkeit und wiegen sich fälschlicherweise in Sicherheit.[1,10] Selbst sogenannte „Digital Natives" weisen oft hohe Defizite im Bewusstsein für Cyberrisiken auf. Es ist ein weitverbreiteter Irrglaube, dass ihre Technikaffinität auch mit höherer Sicherheitskompetenz einhergeht. Trotz erheblicher Investitionen in Schulungen zeigen viele Beschäftigte ein übersteigertes Vertrauen in die Fähigkeiten ihrer Organisation und ihre eigene Kompetenz zur Erkennung und Abwehr von Cyberangriffen.

Dabei beeinflussen systematische Denk- und Wahrnehmungsfehler die Entscheidungsfindung in hohem Maße. Die Wissenschaft hat inzwischen über 150 solcher Verzerrungen identifiziert, die Wahrnehmung, Informationsverarbeitung und Urteilsbildung erheblich beeinträchtigen können.[4] Selbst erfahrene IT- und Sicherheitsexperten sind anfällig für kognitive Verzerrungen, was zu materiellen Fehlentscheidungen führen kann. Im Folgenden werden einige dieser typischen Denkfallen näher vorgestellt.

WENN AWARENESS-KAMPAGNEN AN IHRE GRENZEN STOßEN

Als Reaktion auf die zunehmende Bedrohungslage setzen viele Organisationen auf Awareness-Kampagnen, um Mitarbeiter für Cyberrisiken zu sensibilisieren. In Schulungen, E-Learnings oder simulierten Phishing-Tests sollen sie lernen, Bedrohungen frühzeitig zu erkennen und entsprechend zu handeln. Ziel ist es, eine „menschliche Firewall" zu etablieren – ein kollektives Risikobewusstsein, das technische Schutzmechanismen ergänzt.

Das ist zunächst auch sinnvoll. In der Praxis bleiben die Erfolge jedoch leider oft hinter den Erwartungen zurück. Trotz regelmäßiger Trainings klicken Mitarbeiter weiterhin auf verdächtige Links, verwenden schwache Passwörter oder umgehen Sicherheitsrichtlinien.[3,13] Häufig wird dies als mangelnde Disziplin oder fehlendes Interesse ausgelegt – eine Sichtweise, die die tieferliegenden Ursachen verkennt.

Menschliches Verhalten folgt nicht ausschließlich rationalen Regeln. Entgegen dem normativen Idealbild der Volkswirtschaftslehre, das den Menschen als homo oeconomicus charakterisiert – also als ein rational handelndes Wesen, das immer darauf abzielt, seinen Nutzen zu maximieren – weiß die Forschung schon lange, dass Menschen keine rationalen Rechenmaschinen sind. Selbst gut informierte Personen handeln in kritischen Situationen häufig nicht so, wie es die Theorie erwarten lässt.

Diese Diskrepanz liegt nicht nur an fehlendem Wissen oder mangelnder Aufmerksamkeit, sondern auch an psychologischen Faktoren: Menschen unterliegen systematischen Denkfehlern, sogenannten kognitiven Verzerrungen. Sie wirken unbewusst, sind stabil und lassen sich nur schwer durch klassische Aufklärung beseitigen. Selbst wenn Menschen sich ihrer eigenen Schwächen bewusst sind, ändern sie deshalb nicht notwendigerweise ihr Verhalten. Oft bleibt man in gewohnten Mustern gefangen, auch wenn man deren Auswirkungen erkennt.

Damit geraten die besten Awareness-Maßnahmen an ihre Grenzen. Sie adressieren zwar das „Was", aber zu selten das „Wie" des Denkens. Auch Fach- und Führungskräfte sind nicht immun. Wer Cybersicherheit nachhaltig verbessern will, muss daher verstehen, wie Menschen tatsächlich Entscheidungen treffen – und warum sie dabei immer wieder in dieselben Fallen tappen.

ZWEI SYSTEME DES DENKENS: SCHNELL VERSUS LANGSAM

In der psychologischen und verhaltensökonomischen Forschung wird zur Erklärung kognitiver Verzerrungen häufig auf die Duale Systemtheorie verwiesen und das von Daniel Kahneman[8]

zusammengefasste Modell von zwei Denkmodi herangezogen (siehe auch Tabelle 1):

- ein schnelles, automatisiertes und erfahrungsbasiertes System („System 1“) sowie
- ein langsames, reflektiertes und analytisches System („System 2“).

Im Alltag verlassen wir uns oft auf System 1 für viele Entscheidungen. Das spart Zeit und Energie, hat jedoch seinen Preis. So wissen wir, ohne ernsthaft darüber nachzudenken, dass 2+2 = 4 ergibt oder dass London die Hauptstadt von Großbritannien ist. Im Umkehrschluss neigen wir dazu, selbst wenn eigentlich eine gründliche Analyse (System 2) notwendig wäre, unbewusst auf erlernte Muster zurückzugreifen.

Wir ziehen voreilige Schlüsse, lassen uns von oberflächlichen Reizen fehlleiten oder übersehen wichtige Details – einfach, weil unser Gehirn aus Effizienzgründen den konditionierten Abkürzungsweg 1 nimmt und sich den Aufwand spart, tiefer zu analysieren über den mühsamen Weg 2. Besonders unter Stress, Unsicherheit oder Zeitdruck gewinnen diese Automatismen an Einfluss.

FÜNF ZENTRALE VERZERRUNGEN

Im Kontext der Cybersicherheit zeigen sich fünf typische Beispiele, die immer wieder zu suboptimalen Entscheidungen führen:

1. **Affektheuristik:** Die Affektheuristik ist eine kognitive Verzerrung, bei der emotionale Reaktionen Entscheidungen stark beeinflussen. Anstatt rational zu entscheiden, verlassen sich Menschen oft unbewusst auf ihr Bauchgefühl, besonders bei komplexen Risiken. Die Frage „Wie fühle ich mich dabei?“ ersetzt die anspruchsvollere „Was halte ich objektiv davon?“.

   In der Cybersicherheit zeigt sich dies bei der Wahl von Cybersicherheitsanbietern, wo persönliche Sympathie oder ein überzeugendes Auftreten zu voreiligen Entscheidungen führen können. Bei der Angebotspräsentation beispielsweise wird dann der Eindruck der präsentierenden Personen überbewertet, obwohl sie üblicherweise weder für die Produktentwicklung noch den späteren Betrieb verantwortlich sind und sich aus der Präsentation keine Ableitungen auf die Produktqualität vornehmen lassen.

   Das geht zum Teil einher mit dem sogenannten Halo-Effekt (Heiligenschein), wonach bekannten Anbietern oft voreilig Vertrauen geschenkt wird, nicht aufgrund objektiver Überlegenheit, sondern aus Unsicherheit und dem Wunsch, Fehler zu vermeiden („Nobody ever got fired for buying IBM“).

2. **Ankereffekt:** Dieser Effekt stellt eine kognitive Verzerrung dar, bei der externe Informationen als fester Bezugspunkt (Anker) für nachfolgende Entscheidungen fungieren. Besonders bekannt ist dieses Phänomen in den Finanzmärkten, wo Personen bei Schätzungen oder Prognosen häufig von einem Anfangswert ausgehen und ihre Einschätzungen nur unzureichend anpassen. Zahlen und Statistiken wirken oft ebenfalls als Anker und treten beispielsweise in Verbindung mit der sogenannten Regressionsverzerrung auf, bei der irrtümlicherweise die Diskussion von einem falschen Basiswert aus startet.

   Im Kontext der Cybersicherheit können fehlerhaft ermittelte Schätzungen der Kosten eines Systemausfalls die Risikowahrnehmung und die darauf basierenden Entscheidungen erheblich verzerren. Werden solche Werte als „Fakten“ präsentiert, haben sie nachhaltige Auswirkungen auf Budgetplanungen und Ressourcenzuweisungen. Studien zeigen, dass etwa ein Drittel der Unternehmen die Eintrittswahrscheinlichkeit und die Auswirkungen von Cyberrisiken nicht angemessen bewerten kann. Dennoch werden diese unsicheren Werte als Anker verwendet, was die Investitionsentscheidungen erheblich verfälscht.

3. **Gruppendenken:** Hierbei handelt es sich um ein soziales Phänomen, bei dem der Wunsch nach Harmonie in einer Gruppe so stark ist, dass abweichende Meinungen unterdrückt werden. Selbst kompetente Personen passen sich oft der Gruppenmeinung an, nicht aus Überzeugung, sondern aus Angst vor sozialer Ablehnung. Diese „falsche“ Einigkeit führt dazu, dass kritische Aspekte übersehen und Risiken falsch eingeschätzt werden.

   Besonders in der Cybersicherheit kann Gruppendenken gravierende Folgen haben. Wenn Sicherheitsrisiken oder Notfallmaßnahmen besprochen werden, bleiben alternative Sichtweisen oft ungehört, besonders wenn Mitglieder sich unsicher fühlen, ihre Meinung zu äußern. Dominante Meinungen können die Diskussion lenken, während stillschweigende Übereinstimmung als kollektives Urteil missverstanden wird. Das führt zu Echokammern, in denen bekannte Narrative verstärkt und neue Ideen unterdrückt werden, wodurch Warnsignale übersehen und fragwürdige Entscheidungen getroffen werden.

4. **Kontrollillusion:** Das Fehlen von Sicherheitsvorfällen wird oft fälschlicherweise als Beweis für Sicherheit angesehen. Ein nicht erfolgter – oder schlimmstenfalls nicht erkannter – Cyberangriff wird als Zeichen für Kontrolle missinterpretiert. Zudem gibt es psychologische Hürden: Cybersicherheit bringt selten direkte finanzielle Erträge, was Investitionsentscheidungen erschwert. Entscheidungsträger sind darauf konditioniert, einen „Business Case“ zu präsentieren, der im präventiven Bereich oft schwer zu erstellen ist. Ähnlich wie bei staatlichen Rüstungsausgaben entsteht auch in der Privatwirtschaft eine Legitimationslücke bei Investitionen in Cybersicherheit: Der Erfolg zeigt sich im besten Fall darin, dass nichts passiert, was die Rechtfertigung ge-

	System 1	System 2
Funktionsweise	automatisch, emotional, intuitiv	logisch, analytisch, berechnend
Aufwand	gering	hoch
Ziel	Bearbeitung von Routinen und einfachen Aufgaben	Lösen komplexer Fragestellungen
Steuerung	unbewusst, nebenher	bewusst, konzentriert

Tabelle 1: Gegenüberstellung der Denkmodi nach Kahnemans Dualer Systemtheorie

genüber Stakeholdern erheblich erschwert. Gerade in wirtschaftlich schwierigen Zeiten kann das dazu führen, dass Einsparungen zu schnell an kritischen Stellen vorgenommen werden.

5. **Status-quo-Verzerrung:** Beim Treffen von Entscheidungen tendieren Menschen dazu, den Status quo zu bevorzugen – also den gegenwärtigen Zustand aufrechtzuerhalten, auch wenn es rational keine eindeutige Rechtfertigung dafür gibt. Es herrscht eine gewisse Resistenz gegenüber Veränderungen, denn Veränderungen bedeuten Risiken und könnten die Betriebsstabilität gefährden.

   IT-Teams halten daher lange an bewährten und lieb gewonnenen Systemen fest, was durch Sprichworte wie „Never change a running system" verdeutlicht wird. Die sogenannten Switching Costs – also die mit einem Systemwechsel verbundenen finanziellen, organisatorischen und psychologischen Aufwände – wie Migration und Einarbeitungszeiten verstärken diese Zurückhaltung. Zudem spielt die Verlustaversion eine große Rolle: Menschen bewerten potenzielle Verluste höher als Gewinne, was dazu führt, dass das Risiko durch Veränderungen überbewertet und die Vorteile unterbewertet werden. So bleibt man oft bei suboptimalen, aber vertrauten Lösungen, getrieben von dem Wunsch nach Stabilität und Risikovermeidung.

WECHSELSEITIGE VERSTÄRKUNG

Die Forschung zu kognitiven Verzerrungen zeigt, dass sie oft in Kombination auftreten und sich gegenseitig verstärken.[11,12] Viele Studien betrachten Verzerrungen isoliert, doch die verhaltensökonomische und psychologische Forschung betont, dass sie in einem komplexen „kognitiven Ökosystem" operieren, wo sie sich wechselseitig beeinflussen und in bestimmten Situationen synergetisch wirken.

In organisatorischen Entscheidungskontexten wird dies besonders deutlich, da mehrere Faktoren gleichzeitig interagieren. In dem Fall ist von kognitiven Interferenzen oder Bias-Clustern die Rede. Beispielsweise kann die Status-quo-Verzerrung durch Verlustaversion verstärkt werden, während Ankereffekte und Affektheuristiken die Wahrnehmung von Risiken und Chancen verzerren.

Gruppendenken kann zudem verhindern, dass diese Verzerrungen erkannt werden, was zu falschen Entscheidungen und ineffektiven Sicherheitsmaßnahmen führt. Daher ist es wichtig, Verzerrungen nicht isoliert zu betrachten, sondern ihr Zusammenspiel zu verstehen, um effektive Strategien zur Risikominimierung und Verhaltensänderung zu entwickeln.

STRUKTURIERTE GEGENMAßNAHMEN FÜR DIE PRAXIS

Kognitive Verzerrungen sind allgegenwärtig. Um deren negativen Auswirkungen in der Cybersicherheit wirksam zu verringern, müssen Organisationen über klassische Awareness-Kampagnen hinausgehen. Die folgenden Maßnahmen können helfen, menschliche Fehlentscheidungen zu minimieren und die Sicherheitskultur nachhaltig zu stärken (siehe auch Tabelle 2):

- **Förderung einer Kultur der kritischen Reflexion und der offenen Kommunikation:** Teams müssen möglichst divers sein und ermutigt werden, Risiken offen und ohne Angst vor Repressalien zu diskutieren. Nur in einem Klima, in dem viele verschiedene Erfahrungshintergründe und auch kritische Meinungen explizit willkommen sind, können Warnsignale frühzeitig geäußert werden.

  Teams können Entscheidungsprozesse aktiv strukturieren – etwa durch „Devil's Advocate"-Rollen, in denen gezielt Gegenpositionen vertreten werden, oder durch „Pre-Mortem"-Analysen, die mögliche Fehlentscheidungen vorwegnehmen und deren Ursachen sichtbar machen. So lassen sich Gruppendenken vorbeugen und blinde Flecken frühzeitig erkennen.

- **Systematische Berücksichtigung von Switching Costs und Verlustaversion:** Führungskräfte sollten Veränderungen transparent kommunizieren und die damit verbundenen Risiken sowie Kosten realistisch abwägen. Schulungen, Pilotphasen und redundante Systeme erleichtern den Übergang und verringern die Angst vor Verlusten.

- **Etablierung von Entscheidungshilfen und Checklisten:** Verantwortliche sollten Entscheidungen – besonders zur Cybersicherheitsstrategie – nicht spontan oder unter Zeitdruck treffen. Notfallpläne für verschiedene Szenarien und standardisierte Bewertungsinstrumente fördern eine objektive Analyse von Risiken und Optionen und reduzieren kognitive Verzerrungen.

Entscheidungsfalle	Beispielhafte Gefahr im Cybersecurity-Kontext	Mögliche Gegenmaßnahmen
Gruppendenken	kritische Stimmen verstummen, dominante Meinungen setzen sich durch	Devil's Advocate, Pre-Mortem-Analyse, heterogene Teams, Moderationstechniken
Status-quo-Verzerrung/ Verlustaversion	Verzicht auf notwendige Veränderungen aus Angst vor Instabilität	Pilotprojekte, „Safe-to-fail"-Experimente, transparente Kommunikation von Switching Costs
Ankereffekt	Entscheidungen basieren auf fehlerhaften Ausgangswerten (zum Beispiel Schätzungen)	standardisierte Bewertungsrahmen (FAIR, NIST), externe Benchmarks, strukturierte Risikoreviews
Kontrollillusion	Abwesenheit von Vorfällen wird als Sicherheit missverstanden	regelmäßige Red-/Blue-Team-Übungen, unabhängige Audits, Incident-Simulationen
Affektheuristik	emotionale Eindrücke überlagern rationale Risikoabwägung	Planspiele, Szenarien, Debriefings realer Vorfälle, Training zu Bias-Erkennung

Tabelle 2: Häufige kognitive Verzerrungen im Sicherheitskontext und passende Gegenstrategien

Checklisten und Entscheidungsbäume minimieren emotionale Einflüsse und stellen rationale Kriterien in den Vordergrund. Kennzahlen und Metriken geben zusätzliche Orientierung.

- **Multiperspektivische Entscheidungsfindung fördern:** Unterschiedliche Experten und Abteilungen sollten frühzeitig eingebunden werden, um ein möglichst umfassendes Bild der Risiken und Lösungen zu erhalten. Zudem sind heterogen besetzte, interdisziplinäre Teams weniger anfällig für Gruppendenken: Vielfalt reduziert kollektive Verzerrungen und erweitert den Blick auf potenzielle Bedrohungen.

- **Kontinuierliche Weiterbildung mit Fokus auf kognitive Verzerrungen:** Fach- und Führungskräfte sollten gezielt für typische Denkfehler sensibilisiert werden. Schulungen sollten nicht nur technische Inhalte wiederholen, sondern Verhaltensreflexion und Perspektivenwechsel fördern – etwa durch Szenarien, Rollenspiele oder Debriefings realer Vorfälle.

- **Einbindung externer Experten und Audits:** Unabhängige Reviews durch Dritte decken blinde Flecken auf, die intern durch Verzerrungen oft unbemerkt bleiben. Externe Bewertungen ermöglichen eine realistischere Einschätzung der Cyberrisiken und stärken zugleich die Governance.

FAZIT

Cyberresilienz umfasst weit mehr als nur die technischen Aspekte. Da kognitive Verzerrungen auch Fach- und Führungskräfte der IT-Sicherheit beeinflussen, drohen Fehlentscheidungen selbst dort, wo Wissen und Erfahrung vorhanden sind. Wer nachhaltige Resilienz aufbauen will, muss daher die menschliche Komponente systematisch adressieren.

Die in diesem Beitrag beschriebenen Stolperfallen – von Gruppendenken über Ankereffekte bis hin zur Kontrollillusion – zeigen, wie leicht strategische Entscheidungen verzerrt werden können. Daraus folgt, dass Organisationen gezielt Gegenmaßnahmen etablieren sollten: strukturierte Entscheidungsprotokolle gegen Anker- und Status-quo-Effekte, Devil's-Advocate-Rollen und Pre-Mortems gegen Gruppendenken, Red-/Blue-Team-Übungen gegen Kontrollillusion sowie Szenarien und Rollenspiele zur Sensibilisierung für affektgetriebene Fehlurteile.

Wesentlich ist, diese Verfahren nicht einmalig einzuführen, sondern regelmäßig zu überprüfen und an die dynamische Bedrohungslandschaft anzupassen. So wird das Auftreten der Denkmuster nicht nur erkannt, sondern minimiert – und aus einer potenziellen Schwäche entsteht organisatorische Stärke.

Angesichts stetig wachsender Cyberbedrohungen ist es unerlässlich, die Auseinandersetzung mit kognitiven Verzerrungen als festen Bestandteil der Cyberresilienz-Strategie zu verankern. Nur wenn die menschliche Dimension ebenso konsequent wie die technische adressiert wird, lassen sich Fehlentscheidungen vermeiden, Schutzmaßnahmen effektiv gestalten und Risiken unter Kontrolle halten. Die Sicherheit von morgen beginnt mit den Entscheidungen von heute – und mit der Fähigkeit, die eigenen Denkfallen zu überwinden. ■

Literatur

[1] *Alnifie, K. M., & Kim, C. (2023). Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis. Journal of Information Security, 14(2), 93–110. https://doi.org/10.4236/JIS.2023.142007*

[2] *BITKOM. (2024, 23. Oktober 2024). Erstmals mehr als 10 Milliarden Euro für Deutschlands Cybersicherheit https://www.bitkom.org/Presse/Presseinformation/Erstmals-mehr-als-10-Milliarden-Euro-fuer-Deutschlands-Cybersicherheit*

[3] *Candrick, W., Addiscott, R., Walls, A., & Michaels, A. (2023). Security Awareness Efforts Fall Short! Now What? (Survey Results Analysis). Gartner.*

[4] *Dimara, E., Franconeri, S., Plaisant, C., Bezerianos, A., & Dragicevic, P. (2018). A task-based taxonomy of cognitive biases for information visualization. IEEE transactions on visualization and computer graphics, 26(2), 1413–1432.*

[5] *Huang, K., & Madnick, M. S. S. (2017). Cybercrime-as-a-Service: Identifying Control Points to Disrupt.*

[6] *Huang, K., Siegel, M., & Madnick, S. (2018). Systematically Understanding the Cyber Attack Business: A Survey. ACM Comput. Surv., 51(4), Article 70. https://doi.org/10.1145/3199674*

[7] *IDC. (2025). Worldwide Security Spending to Increase by 12.2% in 2025 as Global Cyberthreats Rise, Says IDC. Retrieved Jul 16, 2025 from https://my.idc.com/getdoc.jsp?containerId=prEUR253264525*

[8] *Kahneman, D. (2011). Thinking, fast and slow. Farrar, Strau and Giroux.*

[9] *Mehta, I. (2019). The Need for Better Metrics on Cybercrime. http://www.jstor.com/stable/resrep20149*

[10] *Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, 2(3), 573–586. https://doi.org/10.3390/jcp2030029*

[11] *Tversky, A., & Kahneman, D. (1974). Judgment Under Uncertainty: Heuristics and Biases. Science, 185(4157), 1124–1131.*

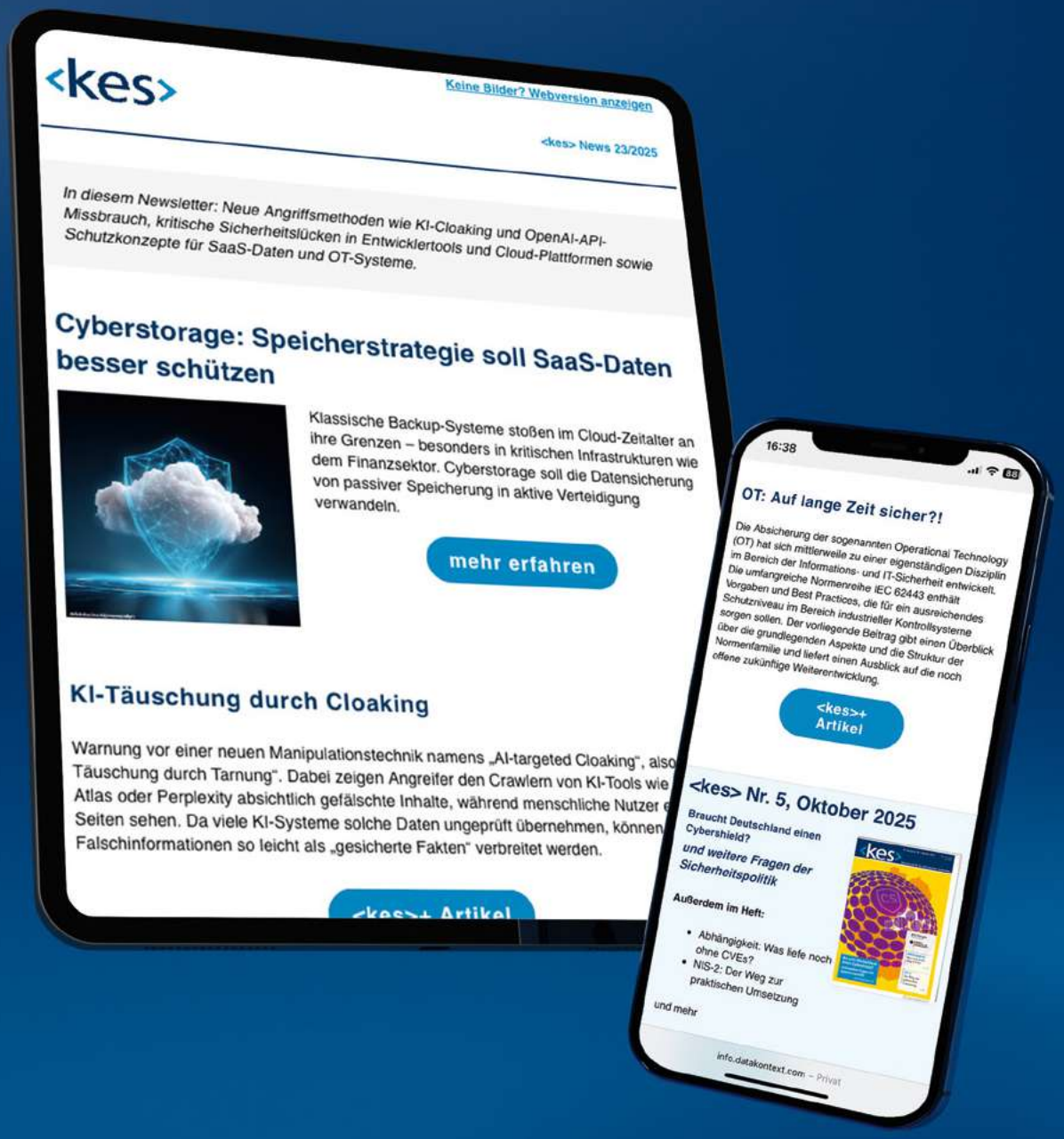
[12] *Tversky, A., & Kahneman, D. (1979). Prospect Theory: An Analysis of Decision under Risk. Econometrica, 47(2), 263–291. https://doi.org/10.2307/1914185*

[13] *Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269*

DR. MARC WILCZEK
ist Technologie-Manager mit über 20 Jahren Erfahrung in Cybersicherheit, Cloud und digitaler Transformation. Zudem engagiert er sich zu diesen Themen in Forschung und Lehre und publiziert regelmäßig – so unter anderem auch in Kooperation mit dem Institut für Internet-Sicherheit – if(is).

RALPH NOLL
ist Cybersicherheitsexperte mit über 28 Jahren Erfahrung bei Professional Services Firmen. In seiner Karriere hat er Teams im Bereich Digitale Forensik geleitet, um digitale Spuren in IT-Systemen forensisch aufzuklären, sowie ein Cyber Incident Response Team bei Deloitte aufgebaut und geleitet, das Unternehmen bei der Abwehr und Analyse von Cyberangriffen unterstützt.

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.



Der Wissensvorsprung für Ihre Arbeit – direkt ins Postfach!

Abonnieren Sie jetzt den kostenfreien <kes> Newsletter:
www.kes-informationssicherheit.de/newsletter

VORSCHAU Ausgabe 1|26 FEBRUAR/ MÄRZ

SCHWERPUNKT: NIS-2 und CRA – Neue Compliance-Anforderungen meistern

Die europäische Cybersicherheitslandschaft steht vor einem Paradigmenwechsel: Mit der NIS-2-Richtlinie und dem Cyber Resilience Act (CRA) treten umfassende neue Regelwerke in Kraft, die Unternehmen vor erhebliche Herausforderungen stellen. Während NIS-2 den Anwendungsbereich kritischer Infrastrukturen deutlich erweitert, etabliert der CRA erstmals verbindliche Cybersicherheitsstandards für Produkte mit digitalen Elementen.

Im kommenden Heft wird die praktische Umsetzung dieser regulatorischen Anforderungen beleuchtet:

- Überblick über Pflichten und kritische Fristen für betroffene Unternehmen
- systematische Gap-Analyse und Risikobewertung nach NIS-2-Anforderungen
- Implementierung technischer Schutzmaßnahmen: von Patchmanagement über kontinuierliches Monitoring bis hin zu modernen Verschlüsselungsverfahren
- Aufbau effektiver Meldeprozesse und Incident-Response-Strukturen für den Ernstfall

Darüber hinaus widmet sich das Special den spezifischen Herausforderungen der CRA-Compliance: von der notwendigen Anpassung bestehender Lieferantenverträge über die Integration neuer Prozesse bis hin zur strategischen Vorbereitung auf behördliche Audits.

(Beitragsangebote für das Special senden Sie bitte an wolfgang.scharf@datakontext.com)

Erscheinungstermin: 27. Februar 2026

IT-SICHERHEIT
Management und Technik

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

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

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

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

Objekt- und Anzeigenleitung:
Wolfgang Scharf (verantwortlich für den Anzeigenteil)
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 31

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

Hersteller:
DATAKONTEXT GmbH
Augustinusstraße 11 A, 50226 Frechen

Kontakt und Informationen zum Thema Produktsicherheitsverordnung:
Dieter Schulz
Tel.: +49 2234 98949-99
E-Mail: dieter.schulz@datakontext.com
www.datakontext.com/produktsicherheitsverordnung

Abonnement:
Jahresabonnement € 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)

31. Jahrgang 2025 · 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