HZ219242 · ISSN 1868-5757 · www.itsicherheit-online.com Februar/März **1/2026**

IT-SICHERHEIT

Management und Technik

Schwerpunkt NIS-2 und CRA

Monitoring und Incident-Management mit Open Source

- **Handlungsfähig bleiben:** Herkunft allein schafft keine Resilienz
- **NIS-2-Meldepflichten:** Kommunikation unter Zeitdruck
- **Synergien nutzen:** NIS-2 und CRA gemeinsam umsetzen

Die Agenten-Lücke
Warum autonome KI-Systeme den AI Act unterlaufen

Assets außer Kontrolle
Ansätze für zukunftsfähiges ITAM in Cloud- und KI-Umgebungen

Risiko in Zahlen
Wie ein Score Cybergefahren für KMU messbar macht

DATAKONTEXT

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

Liebe Leserinnen, liebe Leser,

in dieser Ausgabe widmen wir uns in unserem Heftschwerpunkt NIS-2 und dem Cyber Resilience Act (CRA) sowie der Frage, wie Unternehmen diese Vorgaben tatsächlich umsetzen können. Einer unserer Autoren arbeitet zum Beispiel heraus, wie sich technische Überwachung und Angriffserkennung mithilfe von Open-Source-Lösungen so verzahnen lassen, dass sie die neuen Melde- und Nachweispflichten verlässlich erfüllen (Seite 6).

In einem anderen Text befasst sich der Autor damit, dass Unternehmen NIS-2 und CRA nur dann effizient umsetzen können, wenn sie organisatorische Sicherheit und Produktsicherheit zusammenführen (Seite 14), denn getrennte Prozesse und Rollen erzeugen schnell Lücken – besonders dort, wo beide Regelwerke ineinandergreifen. Wie kritisch das werden kann, zeigt sich bei der Krisenkommunikation: Was passiert in den ersten 24 Stunden, wenn Kanäle ausfallen, Zuständigkeiten unklar bleiben oder Informationen fehlen? Resilienz entsteht in solchen Momenten vor allem durch klare Entscheidungen, eingeübte Abläufe und belastbare Alternativen (Seite 12).

Darüber hinaus beleuchten wir in dieser Ausgabe, wie Unternehmen Risiken überhaupt sinnvoll bewerten können. Ein neu entwickelter Cyber-Risiko-Score macht den Unterschied zwischen technischer Schwachstelle und tatsächlichem Geschäftsrisiko sichtbar (Seite 52). Er berücksichtigt nicht nur technische Befunde, sondern auch deren Bedeutung für Prozesse, Auswirkungen und organisatorische Reife. So entsteht eine Grundlage, auf der Sicherheitsentscheidungen sowohl technisch fundiert als auch betriebswirtschaftlich nachvollziehbar getroffen werden können.

Ein weiterer Blick gilt den Prüfmethoden, die für die Sicherheitspraxis entscheidend sind. Der jährliche Penetrationstest reicht kaum noch aus, um realistische Angriffspfade oder neu entstehende Schwachstellen abzudecken. Stattdessen gewinnen kontinuierliche Tests, automatisierte Analysen und Verfahren an Bedeutung, die technische Befunde zeitnah in strategische Entscheidungen überführen (Seite 40).

Gleichzeitig wächst die Geschwindigkeit, mit der sich Angriffe weiterentwickeln. Unsere Autoren zeigen, wie KI-Werkzeuge Cyberattacken skalierbarer, flexibler und schwerer erkennbar machen – von täuschend echten Social-Engineering-Versuchen bis zu Schadsoftware, die sich aktiv an ihre Umgebung anpasst (Seite 33 und Seite 36). Gleichzeitig entstehen neue Verteidigungsansätze, die Muster automatisiert erkennen, Szenarien simulieren und Sicherheitsanalysen beschleunigen. Das Sicherheitsniveau von morgen hängt damit zunehmend davon ab, wie gut Organisationen künstliche Intelligenz (KI) sowohl als Risiko als auch als Werkzeug verstehen.

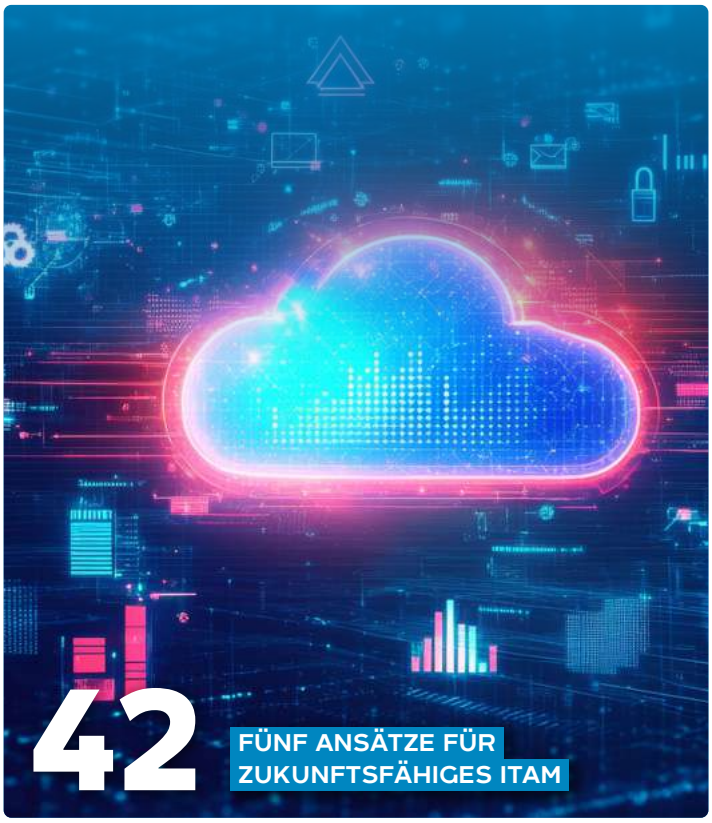
Zum Schluss geht es um eine Ebene, die leicht übersehen wird: die Fähigkeit, Sicherheit dauerhaft zu steuern. Unsere Autoren machen klar, dass neue Vorgaben, KI-getriebene Angriffe und wachsende Abhängigkeiten nur dann beherrschbar bleiben, wenn Governance nicht in immer neuen Einzellösungen endet (Seite 45). Gefordert ist ein integrierter Ansatz, der Risiken, Kontrollen und Verantwortlichkeiten zusammenführt und dadurch die Entscheidungsfähigkeit erhält – gerade dann, wenn Regulierung und Komplexität weiter steigen.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre!
Ihr Sebastian Frank

INHALT

6 **SCHWERPUNKT**
MONITORING UND INCIDENT-MANAGEMENT
ICINGA UND ELASTIC STACK: NIS-2-UMSETZUNG MIT OPEN SOURCE

36 DIE AGENTEN-LÜCKE



42 FÜNF ANSÄTZE FÜR ZUKUNFTSFÄHIGES ITAM

52 DIE VERMESSUNG DER UNSICHERHEIT

Monitoring und Incident-Management

ICINGA UND ELASTIC STACK: NIS-2-UMSETZUNG MIT OPEN SOURCE

Klassisches Infrastrukturmonitoring ist für die Einhaltung der NIS-2-Vorgaben nicht mehr ausreichend. Eine Open-Source-Kombination aus Icinga und Elastic Stack kann diese Anforderungen erfüllen – von der Zustandsüberwachung bis zur forensischen Analyse.

Die NIS-2-Richtlinie verpflichtet Unternehmen zu einer dauerhaft wirksamen technischen Überwachung ihrer IT-Systeme. Die rechtlichen Anforderungen aus NIS-2, dem deutschen Umsetzungsgesetz NIS2UmsuCG und dem überarbeiteten BSI-Gesetz (BSIG) erfordern, dass sicherheitsrelevante Ereignisse kontinuierlich erfasst, analysiert und bewertet werden müssen. Dabei geht es um Angriffserkennung, Incident-Management, Nachvollziehbarkeit und belastbare Dokumentation. Wer nur klassisches Infrastrukturmonitoring betreibt oder Logs isoliert sammelt, erfüllt diese Vorgaben nicht mehr.

Eine technisch saubere Lösung bietet die Kombination aus Icinga und Elastic Stack: Diese Open-Source-Architektur führt Monitoring, Observability und Funktionen aus dem Bereich des Security Information and Event Managements (SIEM) in einer integrierten Struktur zusammen, ohne Abhängigkeit von proprietären Komplettsystemen.

NIS-2 ALS ZWANG ZUR PERMANENTEN SICHTBARKEIT

§ 30 BSIG fordert Maßnahmen zur Risikobehandlung, zur Erkennung sicherheitsrelevanter Ereignisse und zur Bewertung ihrer Auswirkungen. Der Annex der NIS-2-Umsetzungsverordnung wird dabei konkret: Er schreibt Protokollierung, Überwachung, die Minimierung von Fehlalarmen und die Verfügbarkeit der Überwachungssysteme selbst vor.

Betreiber kritischer Anlagen trifft es noch härter: § 31 BSIG verlangt explizit Systeme zur Angriffserkennung, die automatisiert Daten erfassen und auswerten. Technisch lässt sich das nur umsetzen, wenn Zustandsüberwachung, Log-Analyse und Ereigniskorrelation eng zusammenspielen. Genau an dieser Schnittstelle

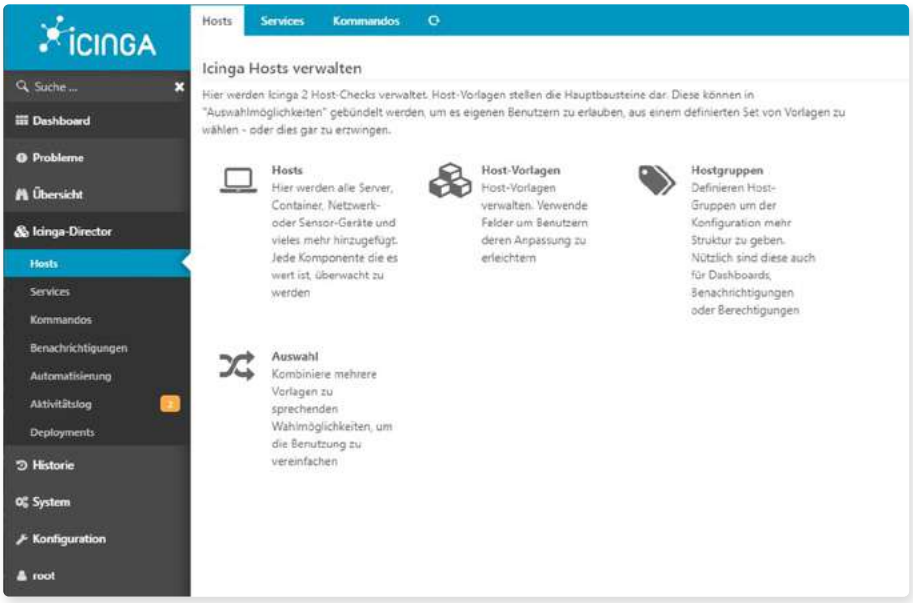


Abbildung 1: Icinga ist ein sinnvolles Überwachungswerkzeug, auch für NIS-2.

entfaltet die Kombination aus Icinga und Elastic Stack ihre Wirkung.

ICINGA ALS OPERATIVE MONITORING-SCHICHT

Icinga übernimmt die kontinuierliche Überwachung von Infrastruktur, Plattformen und Diensten. Das System kann Server, Netzwerkgeräte, Kubernetes-Cluster, Windows-Systeme, Datenbanken, Hyper-V- und VMware-Umgebungen sowie Cloud-Ressourcen einheitlich überwachen. Prüfungen liefern strukturierte Statusinformationen zu Verfügbarkeit, Antwortzeiten, Ressourcennutzung, Zertifikaten, Replikationszuständen und Service-Abhängigkeiten.

Diese Daten erfüllen mehrere NIS-2-relevante Funktionen: Erstens liefern sie eine permanente Zustandskontrolle der Verfügbarkeit, die für die Aufrechterhaltung kritischer Dienste notwendig ist. Zweitens erzeugen Statuswechsel und Schwellwertüberschreitungen sofortige Alarme, die Incident-Response-Prozesse auslösen. Drittens dokumentiert Icinga sämtliche Ereignisse zeitlich konsistent, inklusive Eskalationen, Quittierungen und Wartungsfenstern.

Die Architektur erlaubt verteilte Topologien mit Clustering, Mandantenfähigkeit und Hochverfügbarkeit. Agentenbasierte und agentenlose Prüfungen lassen sich parallel betreiben. Automatisierte Konfiguration über APIs, Git-basierte Workflows und Konfigurationsmanagement-Werkzeuge reduzieren manuelle Fehlerquellen und unterstützen reproduzierbare Betriebsprozesse. Diese Eigenschaften zahlen direkt auf die NIS-2-Forderung nach organisatorisch und technisch kontrollierbaren Sicherheitsmaßnahmen ein.

ELASTIC STACK ALS ANALYSE- UND DETEKTIONS-PLATTFORM

Der Elastic Stack ergänzt das operative Monitoring um eine analytische Ebene. Logs aus Betriebssystemen, Anwendungen, Netzwerkkomponenten, Cloud-Diensten, Identitätsplattformen und Sicherheitswerkzeugen fließen zentral in Elasticsearch. Dort stehen sie für zeitbasierte Suche, Korrelation und Mustererkennung zur Verfügung. Kibana, die Analyse und Visualisierungsoberfläche des Elastic Stack, stellt die Daten übersichtlich dar und ermöglicht das Erkennen von Abweichungen vom Normalverhalten.

Im Kontext von NIS-2 übernimmt der Elastic Stack SIEM-nahe Aufgaben. Ereignisse aus unterschiedlichen Quellen lassen sich zusammenführen, bewerten und in Beziehung setzen. Mehrfache fehlgeschlagene Anmeldungen, ungewöhnliche Prozessketten, atypische Netzwerkverbindungen oder plötzliche Änderungen an sicherheitsrelevanten Konfigurationen treten in aggregierter Form sichtbar hervor. Regelbasierte Detektion und statistische Anomalieerkennung unterstützen die Früherkennung von Angriffen und Missbrauch.

Ein zentraler Aspekt im Rahmen von NIS-2 ist die langfristige Verfügbarkeit von Protokolldaten. Elastic erlaubt flexible Retentionsmodelle, Snapshot-Strategien und die revisionssichere Ablage in externen Speichersystemen. Dadurch bleiben Ereignisse auch für spätere forensische Analysen, Audits oder behördliche Anfragen verfügbar.

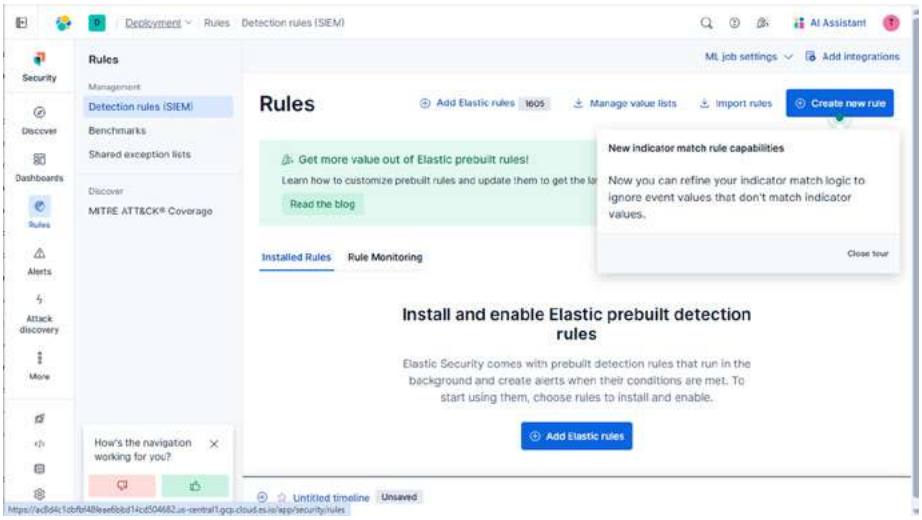


Abbildung 2: Icinga und Elastic Stack lassen sich miteinander kombinieren, um NIS-2 umsetzen zu können.

TECHNISCHE VERZAHNUNG SCHAFFT GEMEINSAMES LAGEBILD

Der entscheidende Mehrwert entsteht aus der engen Kopplung beider Systeme. Icinga liefert strukturierte Zustands- und Performancedaten, die in Elasticsearch übernommen und dort historisiert werden. Gleichzeitig lassen sich sicherheitsrelevante Log-Ereignisse aus dem Elastic Stack in Icinga zurückführen, um sie in bestehende Alarmierungs- und Eskalationsmodelle einzubetten.

Monitoring-Alarme und Security-Incidents erscheinen dadurch in einem gemeinsamen operativen Kontext. Ein plötzlicher Anstieg der CPU-Last, den Icinga meldet, lässt sich unmittelbar mit Log-Ereignissen korrelieren, die auf unautorisierte Prozesse oder externe Zugriffe hindeuten. Umgekehrt führen rein logbasierte Detektionen aus dem Elastic Stack zu operativen Alarmen, die über Icinga an Bereitschaftsdienste, Ticketsysteme oder Incident-Response-Teams weitergeleitet werden. Diese Architektur erfüllt eine zentrale NIS-2-Forderung. Angriffserkennung, Betriebsüberwachung und Reaktion laufen nicht getrennt, sondern integriert. Die Systeme liefern ein konsistentes Lagebild, das technische Störungen und sicherheitsrelevante Ereignisse gemeinsam betrachtet.

Diese Nachvollziehbarkeit erleichtert die Erfüllung gesetzlicher Meldepflichten: Für § 32-BSIG-Meldungen stehen belastbare Daten zur Verfügung, die Zeitpunkt, Umfang und technische Einordnung eines Vorfalls dokumentieren. Die zentrale Log-Ablage verhindert zudem Manipulationen auf Einzelsystemen – ein Vorteil auch für forensische Analysen.

LIZENZMODELLE OHNE VOLUMENBASIERTE KOSTEN

Icinga steht im Kern vollständig als Open-Source-Software zur Verfügung. Die freie Nutzung umfasst unbegrenzte Hosts und Services sowie alle wesentlichen Monitoring-Funktionen. Kommerzielle Subskriptionen ergänzen das Angebot um Support, geprüfte Paketquellen für Enterprise-Distributionen und optionale Zusatzmodule. Die Lizenzierung orientiert sich nicht an überwachten Endpunkten, sondern an Support- und Funktionsbedarf. Diese Struktur ermöglicht kalkulierbare Kosten auch in größeren Umgebungen.

Der Elastic Stack folgt einem gestuften Modell. Grundlegende Funktionen für Log-Management, Suche und Visualisierung stehen kostenfrei zur Verfügung. Erweiterte Sicherheitsfunktionen, maschinelle Anomalieerkennung und erweiterte Zugriffskontrollen erfordern kostenpflichtige Subskriptionen. Alternativ lassen sich vollständig offene Derivate einsetzen, die auf dem gleichen technischen Fundament basieren. In allen Varianten verbleibt die Kontrolle über Datenhaltung und Architektur beim Betreiber.

Im Vergleich zu proprietären SIEM- und Monitoring-Plattformen entfällt die volumenbasierte Lizenzierung pro Endpunkt oder Log-Menge. Investitionen konzentrieren sich auf Infrastruktur, Betrieb und Fachwissen. Für viele mittelständische Unternehmen stellt diese Kostenstruktur den entscheidenden Unterschied dar, um NIS-2-konforme Überwachung überhaupt realisieren zu können.

ROLLE IM NIS-2-GESAMTKONZEPT

Icinga und Elastic Stack ersetzen keine organisatorischen Maßnahmen, Risikoanalysen oder Schulungen. Sie bilden jedoch den technischen Kern für die nachweisbare Umsetzung zentraler NIS-2-Pflichten. Dauerhafte Überwachung, Angriffserkennung, Incident-Analyse und Dokumentation lassen sich mit dieser Kombination konsistent abbilden.

Die Architektur verknüpft Betriebsüberwachung und Sicherheitsanalyse ohne Medienwechsel oder isolierte Werkzeuge. Genau diese Durchgängigkeit fordert NIS-2 implizit. Monitoring und Incident-Management entwickeln sich von unterstützenden Werkzeugen zu tragenden Säulen der Unternehmenssicherheit. Für Organisationen, die regulatorische Anforderungen erfüllen und zugleich operative Kontrolle behalten wollen, liefert der kombinierte Einsatz von Icinga und Elastic Stack eine technisch belastbare, offene und skalierbare Lösung. ■

THOMAS JOOS
ist freier Journalist.

Navigation im Nebel des Cyberspace

Die AURISCON GmbH blickt auf 15 Jahre Navigation ihrer Kunden hin zu effektivem Informationssicherheitsmanagement zurück. Wir begleiten Sie beim operativen Management der IT-Sicherheit und planen mit Ihnen die Bewältigung von Notfällen. Wir verfügen über Fachkompetenz und Erfahrung in der erfolgreichen Vorbereitung einer Zertifizierung gemäß ISO/IEC 27001 und helfen dabei, Compliance im Dschungel der Informationssicherheitsregularien (wie zum Beispiel NIS2) zu gewährleisten.

INFORMATIONSSICHERHEIT ist unser Kerngeschäft. Ihre Kunden möchten, dass Sie die anvertrauten Daten nachweislich sicher verarbeiten? Sie möchten besser verstehen, wie das gehen soll und welche Mehrwerte es bringt?

UNSERE MISSION ist es, Organisationen dabei zu unterstützen, das Informationssicherheitsniveau ihrer Prozesse oder IT-Systeme und deren Resilienz gegen Cyberattacken zu steigern. Mit unserer Fachexpertise begleiten wir Sie auf diesem Weg – von der Analyse bis zur Umsetzung. Wir helfen Organisationen dabei, IT-Sicherheitsbedrohungen rechtzeitig zu erkennen und abzuwehren. Wir haben Methoden, die bei Risikoidentifizierung, -analyse und -behandlung zum Erfolg verhelfen und an Good Practices (ISO-27000-Familie, IT-Grundschutz oder CISIS12) orientiert sind. Wir haben nicht nur Erfahrung mit der Beratung zu Informationssicherheits-Managementsystemen (ISMS), sondern auch mit der Prüfung von ISMS im Rahmen von internen Audits, Lieferantenaudits und Zertifizierungsaudits.

IT-NOTFALLMANAGEMENT Business-Impact-Analysen sind wichtig, um kritische Prozesse identifizieren zu können. Die Ergebnisse haben insbesondere für das Business Continuity Management (BCM, Notfallmanagement) erhebliche Bedeutung. Wir haben Erfahrung bei der Konzeptionierung von IT-Notfallmanagement bis hin zur Erstellung und der Prüfung von Notfallbehandlungsplänen.

BERATUNG ist so gut wie die Berater. Unser Team vereint jahrelange Praxiserfahrung in IT-Infrastrukturen, Managementsystemen und Standardisierung (unter anderem als Mitglied des DIN). Wir verstehen uns als Navigatoren für Ihre IT-Sicherheit: ob als temporäre Lotsen für konkrete Projekte oder als langfristige Begleiter – etwa als externe Informationssicherheitsbeauftragte. Als Navigatoren nehmen wir Ihre Wünsche als „Passagiere" auf und bleiben gleichzeitig auf Kurs in Richtung Ziel (beispielsweise Zertifizierung, Risikoreduzierung).

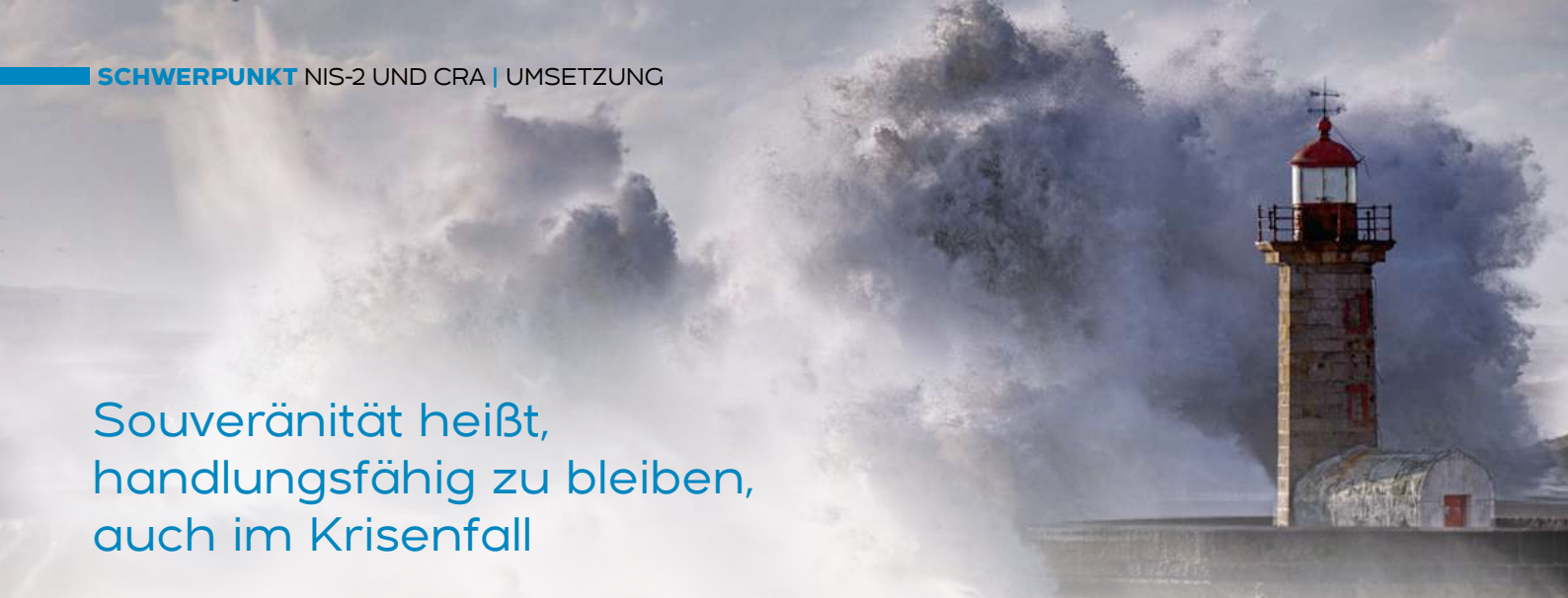
BEISPIEL: NIS2 Das NIS2-Umsetzungsgesetz verpflichtet Unternehmen zu strengen Cybersicherheitsmaßnahmen. Dazu gehören unter anderem ein systematisches Risikomanagement, ein Vorfallsmanagement, technische Schutzvorkehrungen und regelmäßige Audits. Wir haben zahlreiche Planungs- und Umsetzungsprojekte abgeschlossen, bei denen diese Themen im Fokus standen.

UNSERE KUNDEN verteilen sich auf alle Größenklassen. Sie stammen aus diversen Sektoren, denn das Thema Informationssicherheit ist grundsätzlich nicht sektorspezifisch. In den letzten drei Jahren gehörten hauptsächlich Organisationen aus den Sektoren Automobile, Medien, ITK, Messen/Veranstaltungen, Energie, technische Prüfungen, technische Planung sowie Verwaltung (zum Beispiel Ministerien) zu unseren Kunden. ■

Sie können uns wie folgt erreichen:
AURISCON GmbH
Joachimsthaler Straße 17, 14055 Berlin
Tel.: +49 (0)30 235905610
E-Mail: kontakt@auriscon.de
Web: **www.auriscon.info**

Mehr dazu hier

AURISCON



Souveränität heißt, handlungsfähig zu bleiben, auch im Krisenfall

HERKUNFT ALLEIN SCHAFFT KEINE RESILIENZ

Digitale Souveränität lässt sich weder über Herkunftslabels noch über die Postleitzahl eines Rechenzentrums herstellen. Auch europäische Cloud-Anbieter garantieren sie nicht automatisch. Entscheidend ist, ob Organisationen ihre Abhängigkeiten kennen, Risiken realistisch bewerten und im Ernstfall handlungsfähig bleiben. Dazu gehören getestete Alternativen, geübte Exits und belastbare Sicherheitsprozesse – auch dann, wenn zentrale Workloads weiterhin bei internationalen Hyperscalern laufen. Der Beitrag zeigt, was Cyberresilienz praktisch bedeutet und welche Rolle NIS-2 und der Cyber Resilience Act dabei spielen.

Im Kontext digitaler Souveränität bedeutet Resilienz die Fähigkeit, auf unerwartete Herausforderungen zu reagieren und dabei handlungs- und funktionsfähig zu bleiben. Im Kern umfasst sie drei Aspekte: erstens die Anpassungsfähigkeit, um auf rechtliche Veränderungen – etwa den US Cloud Act – schnell reagieren zu können, ohne die eigenen Schutzstandards zu kompromittieren. Dazu gehört, Prozesse und Systeme so auszulegen, dass sich Policy- und Konfigurationsänderungen zügig und sicher umsetzen lassen. Zweitens sind es robuste Sicherheitsstrategien und eine gehärtete Infrastruktur, die man im Ernstfall schnell wiederherstellen kann. Drittens die Sicherstellung von Verfügbarkeit und Integrität der IT-Dienste, auch bei Störungen. Technologische Unabhängigkeit ist damit weniger eine Frage des „Wo“, sondern des „Wie“.

RÜCKENWIND DURCH REGULIERUNG

Die Europäische Union hat mit NIS-2 auf neue Angriffsmethoden, geopolitische Spannungen und wachsende Abhängigkeiten reagiert und einen verbindlichen Rahmen geschaffen, um ein einheitlich hohes Cybersicherheitsniveau in Europa zu etablieren. Die Richtlinie legt klare Mindeststandards fest, verpflichtet Unternehmen zu Meldungen und Wiederherstellungsmaßnahmen und fordert ein konsequent risikobasiertes Vorgehen. Der Cyber Resilience Act (CRA) erweitert diesen Ansatz, indem er für vernetzte Produkte und Software Sicherheitsanforderungen über den gesamten Lebenszyklus vorschreibt. Zusammen erhöhen beide Regelwerke die Resilienz von Organisationen und Lieferketten mit dem Ziel, Sicherheitsvorfälle zu verhindern oder ihre Auswirkungen deutlich zu begrenzen.

Die steigenden Anforderungen an Cyberresilienz sowie die Umsetzung von NIS-2 und dem CRA machen Cybersecurity zur strategischen Führungsaufgabe. Für CISOs entsteht dabei ein konkreter Handlungsdruck:

- Abhängigkeiten und Risiken in Multi-Cloud-Umgebungen, in Softwarelandschaften und entlang der Lieferkette müssen nicht nur sichtbar werden, sondern aktiv sinken.
- Rollen, Prozesse und Meldewege sind neu zu definieren oder konsequent zu ordnen.
- Präventive Kontrollen müssen priorisiert werden und wirksam nachweisbar sein.

Wie sollen die Verantwortlichen in Unternehmen und Organisationen vor dem Hintergrund dieser Anforderungen nun vorgehen?

VON DER RISIKOANALYSE ZUR PRAKTISCHEN UMSETZUNG

Zu Beginn sollte eine vollständige Bestandsaufnahme physischer und digitaler Gefahrenquellen stehen. Von Brand und Diebstahl über den Ausfall kritischer Systeme bis hin zu Zero-Day-Exploits und Phishing gilt es, alle Risiken systematisch zu erfassen. Eine solide Analyse muss den Stand der Technik berücksichtigen und laufend aktualisiert werden, da sich Technologien und Bedrohungen stetig verändern.

Erst auf Basis dieser Risikoeinschätzung lassen sich wirksame und verhältnismäßige Maßnahmen ableiten. Diese sollten sich an der Risikoexposition, der Unternehmensgröße, der Eintrittswahrscheinlichkeit sowie den potenziellen Auswirkungen auf Wirtschaft und Gesellschaft orientieren. Wo möglich, sollten die Verantwortlichen etablierte Normen wie ISO 27001/27002 berücksichtigen.

Bei der Umsetzung der Sicherheitsmaßnahmen bieten cloudbasierte Security-Plattformen einen pragmatischen Weg zu mehrschichtiger Cybersicherheit mit schneller Verfügbarkeit und geringen Anfangsinvestitionen. Bei der Auswahl solcher Lösungen sollten die eigenen Resilienz-Anforderungen ebenso zentral sein wie Zertifizierungen und die Auditierbarkeit der Anbieter.

VIER DIMENSIONEN ALS ENTSCHEIDUNGSKOMPASS

Echte Cyberresilienz bedeutet jedoch mehr, als einzelne Angriffe abzuwehren. Informationen, Daten und Prozesse müssen umfassend geschützt werden. Das erfordert eine ganzheitliche Sicherheitsarchitektur mit entsprechenden Lösungen. Für die strukturierte Entscheidungsfindung helfen die folgenden vier Dimensionen:

- **Souveräne Sicherheit:** technische und organisatorische Resilienz gegenüber externen und internen Bedrohungen.
- **Managebarkeit:** Steuerbarkeit, Skalierbarkeit und Auditierbarkeit der Sicherheitsarchitektur – inklusive klarer Exit-Strategien.
- **Usability:** Nutzungsfreundlichkeit und Akzeptanz im Arbeitsalltag – denn Sicherheit, die umgangen wird, schützt nicht.
- **Kosten und Wertbeitrag:** Total Cost of Ownership sowie der erwartete Nutzen durch Risikominderung.

Dieser Kompass ermöglicht eine systematische Bewertung von Sicherheitsarchitekturen bei der Abwägung zwischen verschiedenen Lösungsansätzen oder Sourcing-Modellen.

HÄRTUNG AUF VIER EBENEN

Jetzt wird es konkret: Härtung passiert dort, wo Sicherheitsprinzipien konsequent in Konfigurationen, Prozesse und Verhalten übersetzt werden. Sie folgt dem Zero-Trust-Prinzip, setzt an Menschen, Endgeräten, Anwendungen und Daten an und reduziert Angriffsflächen damit konsequent.

Der Faktor „Mensch" muss in der Sicherheitsstrategie Asset, nicht Risiko, sein. Das event- und verhaltensbasierte Ausspielen von Sicherheitskampagnen kann für messbare Lernerfolge und eine hohe Sensibilisierung für Cyberrisiken sorgen.

Auf Geräteebene stehen Gerätekontrolle und Verschlüsselungsvorgaben für Wechseldatenträger im Fokus. Schutzmechanismen sollten unmittelbar am Endpoint durchgesetzt werden – unabhängig vom Netzwerkstandort. Bei Applikationen reduziert Allowlisting, also die Beschränkung auf freigegebene Software, die Angriffsfläche erheblich.

Für hochsensible Daten benötigen Unternehmen zudem eine sichere europäische Cloud-Infrastruktur, die geschützten Austausch mit Dritten ermöglicht und volle Zugriffskontrolle gewährleistet. Idealerweise sollten Daten verschlüsselt verarbeitet werden können – auch für KI-Anwendungen –, ohne dass Betreiber oder ausländische Anbieter Zugriff erhalten.

FAZIT

Digitale Souveränität ist kein Ort, sondern die Fähigkeit zur Resilienz. Sie beweist ihren Wert erst im Ernstfall. NIS-2 und CRA setzen dafür einen verbindlichen Mindeststandard. Wirkliche Handlungsfähigkeit entsteht jedoch durch eine präzise Risikoeinschätzung, gezielte Prävention und Härtung, eingeübte Exit-Strategien sowie eine Architektur, die Portabilität und überprüfbare Prozesse konsequent zur Norm macht.

Strategisch klug ist es, Sicherheit nicht als singuläres Tool-Thema, sondern als Betriebsmodell über Menschen, Geräte, Anwendungen und Daten zu verankern. Dazu gehört auch die Option, Workloads je nach Bedarf und Risiko wahlweise in souveränen Cloud-Umgebungen oder beim globalen Hyperscaler zu betreiben. So bleiben Organisationen auch unter Druck steuer- und lieferfähig, reduzieren Lock-in-Risiken und gewinnen den Handlungsspielraum, jederzeit entscheiden zu können, wo und wie kritische digitale Funktionen laufen – ohne Kompromisse bei Sicherheit, Compliance und Geschwindigkeit. ■

FÜNF SCHRITTE FÜR CISOS

- ***Resilienz zur Führungskennzahl machen:*** *Verfügbarkeit kritischer Funktionen und Time-to-Decision als Vorstandsziel verankern.*
- ***Digitale Abhängigkeiten kartieren:*** *Cloud-, Software- und Dienstleisterabhängigkeiten samt priorisierten Exit-Pfaden dokumentieren.*
- ***Prävention priorisieren:*** *Allowlisting, Härtung und Zero Trust vor reiner Detection perfektionieren.*
- ***Schnelle Entscheidungen ermöglichen:*** *Rollen, Eskalationen und Eingriffsrechte vorab verbindlich klären.*
- ***In europäische Resilienz-Netzwerke investieren:*** *Standards, Communities und geübte Zusammenarbeit ausbauen.*

ANDREAS FUCHS
ist Director Product Management bei DriveLock SE.

NIS-2-Meldepflichten: Organisatorische Herausforderungen

KOMMUNIKATION UNTER ZEITDRUCK

Die Schonfrist ist vorbei. Seit dem Inkrafttreten des deutschen NIS-2-Umsetzungsgesetzes im Dezember 2025 gelten für rund 29.500 Unternehmen neue, verbindliche Pflichten in der IT-Sicherheit. Jetzt zeigt sich, ob Meldeprozesse nur auf dem Papier stehen oder einem realen Stresstest standhalten. Im Ernstfall muss binnen 24 Stunden eine Frühwarnung an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gehen. Wer zu Beginn eines Cyberangriffs erst Zuständigkeiten und Abläufe klärt, riskiert seine Handlungsfähigkeit und erhöht das Haftungsrisiko für die Unternehmensleitung.

Der Dezember 2025 markiert eine Zäsur in der deutschen Cybersicherheit. Mit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes (NIS2UmsG) ist die Vorbereitungsphase beendet. Für die betroffenen Unternehmen in Deutschland läuft damit die Schonfrist aus.

Der Gesetzgeber ändert den Fokus von reiner Prävention hin zu nachweisbarer Widerstandskraft. Er erkennt damit an, dass Angriffe nicht vollständig zu verhindern sind. Sanktioniert werden vor allem mangelnde Vorbereitung, unkoordiniertes Handeln und fehlende Kommunikation nach einem Vorfall. Cybersicherheit ist damit kein reines IT- oder Compliance-Thema, sondern Teil der unternehmerischen Sorgfaltspflicht auf Vorstandsebene.

Die Richtlinie erweitert den Kreis der Betroffenen deutlich und unterscheidet nach Systemrelevanz. Sektoren wie Energie, Gesundheit, Verkehr, Bankwesen und digitale Infrastruktur gelten als wesentliche Einrichtungen (Essential Entities). Sie fallen ebenso unter die Richtlinie wie die „Important Entities", zu denen Branchen wie Chemie, Lebensmittel, Abfallbewirtschaftung oder Post- und Kurierdienste zählen.

Doch auch Unternehmen, die nicht direkt unter diese Definitionen fallen, stehen unter Zugzwang. Artikel 21 verpflichtet die Einrichtungen explizit zur „Sicherheit der Lieferkette". Das schafft einen Dominoeffekt: Große Betreiber kritischer Infrastrukturen (KRITIS) auditieren ihre Zulieferer. Wer als kleines und mittleres Unternehmen (KMU) oder als „Hidden Champion" Teil der Wertschöpfungskette bleiben will, muss ein vergleichbares Sicherheitsniveau nachweisen.

DREISTUFIGES VERFAHREN MIT WENIG SPIELRAUM

Kernelement der neuen Pflichten ist das dreistufige Meldeverfahren gemäß Artikel 23. Es lässt wenig Spielraum für Verzögerung. Sobald ein Unternehmen Kenntnis von einem erheblichen Sicherheitsvorfall erlangt, läuft die Zeit.

1. **Frühwarnung (24 Stunden):** Eine erste Meldung an das BSI muss unverzüglich erfolgen. Ziel ist es, grenzüberschreitende Ausbreitungen frühzeitig zu erkennen.

Bild: Symbiot - stock.adobe.com

2. **Vorfallmeldung (72 Stunden):** Diese sollte eine erste Einschätzung des Vorfalls liefern – inklusive Angaben zum Schweregrad, zu den möglichen Auswirkungen sowie Indikatoren für eine mögliche Kompromittierung.

3. **Abschlussbericht (ein Monat):** eine detaillierte Aufarbeitung der Ursachen und getroffenen Maßnahmen.

In der Theorie wirkt dieser Ablauf logisch. In der Praxis eines laufenden Cyberangriffs, etwa einer Ransomware-Attacke, wird dieses Verfahren zur organisatorischen Belastungsprobe. So herrscht in den ersten 24 Stunden in Krisenstäben oft erhebliche Unsicherheit. Welche Systeme sind betroffen? Sind Daten abgeflossen? Was sind die nächsten notwendigen Schritte?

Die eigentliche Herausforderung liegt meist weniger in der Technik als in der Organisation. Wer darf den „Notruf" an das BSI absetzen? Wer validiert die Informationen? Wenn diese Prozesse nicht definiert sind, verstreicht wertvolle Zeit mit internen Abstimmungen. Da die Geschäftsleitung nun persönlich haftet, steigt das Risiko für die Geschäftsführer oder IT-Verantwortlichen erheblich, wenn keine tragfähigen Prozesse existieren.

WENN DER NOTFALL-KANAL SELBST AUSFÄLLT

Ein Aspekt wird in der Vorbereitung häufig unterschätzt: die Verfügbarkeit der eigenen Kommunikationsinfrastruktur. Viele Notfallpläne basieren auf der Annahme, dass E-Mail, VoIP-Telefonie und Kollaborationstools wie Microsoft Teams verfügbar sind. Bei einem gezielten Ransomware-Angriff werden jedoch oft genau diese Systeme als Erstes verschlüsselt oder präventiv vom Netz genommen („Cyber Kill Switch"), um eine Ausbreitung der Schadsoftware zu unterbinden.

Wenn dann der Chief Information Security Officer (CISO) den Angriff erkennt und den Krisenstab einberufen möchte, ist das digitale Adressbuch nicht erreichbar, die Telefonanlage tot und die Dokumente mit den Notfallnummern liegen auf einem verschlüsselten Netzlaufwerk. In diesem Moment bricht die interne Kommunikation zusammen.

Manuelle Workarounds wie private Messenger-Gruppen oder ausgedruckte Telefonlisten sind in der Hektik einer Krise fehleranfällig, datenschutzrechtlich bedenklich und kaum skalierbar.

ANSÄTZE FÜR REDUNDANTE KRISEN-KOMMUNIKATION

Um diese Lücke zwischen technischer Detektion und organisatorischer Handlungsfähigkeit zu schließen, können Organisationen spezialisierte Alarmierungs- und Krisenmanagement-Lösungen in Betracht ziehen. Ein Argument dieser Software-as-a-Service-(SaaS)-Lösungen ist, dass sie autark in gesicherten Rechenzentren laufen, unabhängig von der eigenen IT-Infrastruktur. Auch wenn das eigene Firmennetzwerk stillsteht, bleibt dieser „Out-of-Band"-Kanal handlungsfähig.

Solche Systeme können den Meldeprozess auf drei Ebenen unterstützen: Erstens durch automatisierte Mobilisierung. Statt Listen abzutelefonieren, löst der Sicherheitsverantwortliche per App eine vorbereitete Kommunikationskaskade aus. Das System alarmiert die Mitglieder des Krisenstabs parallel per Anruf, SMS und App-Push und eskaliert automatisch, wenn Personen nicht reagieren. Ziel ist es, den Krisenstab schneller zusammenzubringen.

Zweitens durch strukturierte Prozesse. In solchen Systemen lassen sich für verschiedene Szenarien spezifische Playbooks hinterlegen. Diese digitalen Checklisten führen die Verantwortlichen Schritt für Schritt durch die notwendigen Maßnahmen, inklusive der Erinnerung an die 24-Stunden-Meldepflicht. Vorlagen für Meldungen an Behörden können direkt im System liegen. Das verkürzt Abstimmungen und reduziert Fehlerquellen – vorausgesetzt, Rollen, Vorlagen und Eskalationswege sind zuvor sauber definiert und geübt.

Drittens durch revisionssichere Dokumentation. NIS-2 fordert nicht nur das Handeln, sondern auch dessen Nachweis. Professionelle Systeme protokollieren jeden Schritt: von der Alarmierung über die Aufgabenverteilung bis zur Entscheidung über den Zeitpunkt der Meldung. Dieses Protokoll ist essenziell für den Abschlussbericht nach einem Monat oder bei einer Prüfung durch die Aufsichtsbehörden.

TRAINING ALS SCHLÜSSEL ZUR RESILIENZ

Die Implementierung eines solchen Systems ist kein rein technisches Projekt, sondern verändert Prozesse, Zuständigkeiten und Routinen im Unternehmen. Es führt dazu, dass Unternehmen grundlegende Fragen klären müssen: Sind die Kontaktdaten aktuell? Wer vertritt wen? Welche Rollen und Verantwortlichkeiten gelten konkret im Krisenszenario?

Hier zeigt sich ein zentraler Effekt der Regulierung. Sie bietet einen klaren Rahmen, um digitale Widerstandskraft systematisch aufzubauen. Resilienz ist kein Zustand, den man einmal erreicht. Sie ist eine Fähigkeit, die trainiert werden muss. Ein interner Cyber-Warntag deckt Lücken in den Stammdaten und Prozessen auf. Digitale Lösungen bieten oft integrierte Simulationsmodule, mit denen sich solche Szenarien realistisch durchspielen lassen.

FAZIT

Die NIS-2-Richtlinie macht klar: Cybersicherheit ist Chefsache. Die Bedrohungslage duldet keine Silos zwischen IT-Security und Business-Continuity-Management (BCM). Wer die Meldepflichten nur als Papierarbeit betrachtet, unterschätzt das Risiko. Die Unfähigkeit, schnell und strukturiert zu kommunizieren, kann im Ernstfall den Schaden eines Angriffs deutlich erhöhen, auch was Reputation und Kundenvertrauen betrifft.

Unabhängige Alarmierungssysteme können dazu beitragen, die Widerstandskraft und Handlungsfähigkeit von Unternehmen zu verbessern. Sie können eine Struktur bieten, um auch unter hohem Druck innerhalb der 24-Stunden-Frist die Einhaltung der Vorgaben zu unterstützen. ■

ESKE OFNER
ist Expertin im Bereich Alarmierung und Krisenmanagement und Head of Sales bei F24, einem Software-as-a-Service-Anbieter für Resilienz.

Synergien nutzen

WIE UNTERNEHMEN NIS-2 UND CRA GEMEINSAM UMSETZEN KÖNNEN

Mit dem NIS-2-Umsetzungsgesetz und dem Cyber Resilience Act (CRA) verschärft die EU ihre Anforderungen an die Cybersicherheit deutlich. Erstmals greifen organisatorische Schutzmaßnahmen und die Sicherheit digitaler Produkte ineinander. Für Unternehmen bedeutet das einen Perspektivwechsel: Informationssicherheit beschränkt sich nicht mehr auf technische Maßnahmen wie Firewalls, sondern soll von der Geschäftsführung bis zur Produktentwicklung und Wartung reichen. Wer beide Regelwerke gemeinsam umsetzt, kann Doppelarbeit vermeiden und zugleich die regulatorischen Pflichten erfüllen.

Bild: Fotosphaere - stock.adobe.com

Informationssicherheit kann nur dann wirksam sein, wenn Organisationen sie als ganzheitliche Aufgabe verstehen. Ein Unternehmen, das seine eigenen Systeme sorgfältig schützt, gleichzeitig jedoch digitale Produkte mit offenen Schnittstellen, unsicheren Update-Mechanismen oder unklaren Zuständigkeiten auf den Markt bringt, gleicht einem Gebäude mit moderner Alarmanlage und weit geöffneten Fenstern. Der Schutz endet dann dort, wo er eigentlich weiterwirken müsste.

Längst reicht es deshalb nicht mehr aus, lediglich interne IT-Infrastrukturen zu schützen. Unternehmen, die Produkte mit digitalen Komponenten entwickeln, betreiben oder vertreiben, tragen damit auch Verantwortung für die Sicherheit ihrer Kunden. Sicherheitslücken wirken heute entlang ganzer Wertschöpfungsketten. Diese Realität hat auch die Politik erkannt und nachgesteuert: Mit dem Gesetz zur Umsetzung der NIS-2-Richtlinie und dem Cyber Resilience Act hat der europäische Gesetzgeber zwei Regelwerke geschaffen, die unterschiedliche, aber eng miteinander verknüpfte Aspekte adressieren: den Schutz der eigenen Organisation und die Sicherheit digitaler Produkte über deren gesamten Lebenszyklus hinweg.

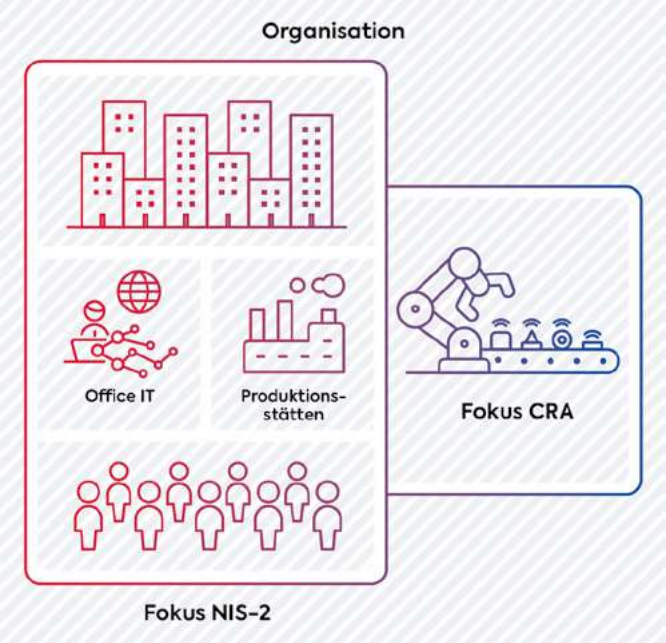


Abbildung 1: NIS-2 und CRA adressieren unterschiedliche Bereiche in Organisationen (Bild: secunet)

ZWEI REGELWERKE MIT UNTERSCHIEDLICHEM FOKUS

Das deutsche **NIS-2-Umsetzungsgesetz** richtet den Blick nach innen. Es verpflichtet betroffene Unternehmen, ein angemessenes Niveau der Informationssicherheit herzustellen und dauerhaft aufrechtzuerhalten. Zentrale Elemente sind ein aktives Risikomanagement, klare Verantwortlichkeiten auf der Leitungsebene, konkrete Anforderungen an das Notfall- und Krisenmanagement sowie explizite Vorgaben zur Sicherheit in der Lieferkette.

Der **Cyber Resilience Act** hingegen fokussiert sich auf die Sicherheit digitaler Produkte. Er stellt konkrete Anforderungen an Cybersicherheit und -resilienz entlang des gesamten Produktlebenszyklus – von der Entwicklung über die Produktion bis zur Nutzung und Wartung der Produkte. Hersteller sind unter anderem verpflichtet, grundlegende Sicherheitsanforderungen zu erfüllen, Sicherheitslücken transparent zu kommunizieren und über einen definierten Zeitraum hinweg Updates bereitzustellen.

Für die Umsetzungsverantwortlichen bedeutet das: Sie müssen Informationssicherheit sowohl auf Organisations- als auch auf Produktebene denken. Wer beide Perspektiven getrennt behandelt, riskiert jedoch Doppelarbeit und inkonsistente Sicherheitsniveaus. Unternehmen benötigen einen ganzheitlichen, integrierten Ansatz, der die gesetzlichen Anforderungen abdeckt, passende Lösungen etabliert und dabei Synergien schafft.

RISIKOMANAGEMENT ALS GEMEINSAMER NENNER

Beide Novellen stellen das Risikomanagement ins Zentrum. Ziel ist nicht die formale Erfüllung von Checklisten, sondern ein realistischer Blick auf unternehmens- beziehungsweise produktspezifische Gefährdungen: Welche Werte sind besonders schützenswert? Welche Bedro-

Abbildung 2: Der strukturierte Risikoanalyse-Prozess umfasst fünf aufeinander aufbauende Phasen: Von der Identifikation der Kernprozesse über die Definition von Rahmenbedingungen und die Schutzbedarfsanalyse bis hin zur Risikobeurteilung und abschließenden Risikobehandlung. (Bild: secunet)

hungen sind wahrscheinlich? Welche Auswirkungen hätte ein erfolgreicher Angriff – auf den Betrieb ebenso wie auf Kunden und Partner?

Zu Beginn steht die Klärung, ob und in welcher Form ein Unternehmen von den Anforderungen betroffen ist. Fällt die Prüfung positiv aus, empfiehlt sich in der Praxis eine kombinierte Gap-Analyse sowohl für NIS-2 als auch für den CRA. Sie zeigt auf, welche Anforderungen bereits erfüllt sind und wo Handlungsbedarf besteht, denn in der Regel sind bereits einige Maßnahmen zur Risikominderung etabliert. Wichtig ist dabei, organisatorische, technische und produktbezogene Aspekte gemeinsam zu betrachten, um die Themenfelder beider Gesetzgebungen – darunter etwa Produktentwicklung, Softwareentwicklung und Dienstleistermanagement – ganzheitlich abzudecken.

Auf die erste Bestandsaufnahme sollte eine individuelle Risikobewertung folgen. Diese orientiert sich an den wesentlichen Assets, Werten und Prozessen des Unternehmens und beurteilt Risiken kontextbezogen. Auf diese Weise lassen sich die Ergebnisse in einen strukturierten Maßnahmenplan überführen, der die nächsten Schritte klar priorisiert, Verantwortlichkeiten schafft und zeitliche Meilensteine festlegt.

Ein solcher Plan schafft Transparenz: Welche Maßnahmen sind kurzfristig umzusetzen? Wo sind strukturelle Anpassungen erforderlich? Und welche Risiken werden bewusst akzeptiert? Diese Entscheidungen gehören auf die Ebene der Geschäftsleitung. NIS-2 macht damit verbindlich, was in der Informationssicherheit lange gefordert wurde: Cybersicherheit ist eine Führungsaufgabe.

SYNERGIEN BEI PARALLELER UMSETZUNG

Gerade bei der parallelen Umsetzung von Sicherheitsmaßnahmen im Sinne von NIS-2 und CRA lassen sich erhebliche Synergien erzielen. Beide Regelwerke fordern, Informationssicherheit über den gesamten Lebenszyklus hinweg zu berücksichtigen – bei IT-Systemen ebenso wie in der Produktentwicklung. Daraus folgt: Es braucht ein Projektmanagement, das Sicherheitsanforderungen konsequent einbindet – von der Planung über die Umsetzung bis in den Betrieb.

Das schafft Möglichkeiten für integrative Prozesse: In vielen Unternehmen sind Produktentwicklungen bereits heute projektbasiert organisiert. Einheitliche Leitlinien in Form eines praxisorientierten Leitfadens, der zentrale Sicherheitsanforderungen aus beiden Regelwerken zusammenführt, können als verbindlicher Rahmen dienen. So lässt sich sicherstellen, dass Informationssicherheit sowohl in IT-Projekten als auch in der Produktentwicklung konsistent einfließt.

STANDARDS ALS ORIENTIERUNGSHILFE

Der Cyber Resilience Act bleibt bewusst technologieoffen, verlangt jedoch nachweisbare Sicherheitsmaßnahmen. Hier bieten etablierte Standards eine wertvolle Orientierung. Besonders die Normenreihe IEC 62443 zur industriellen Cybersicherheit, die aktuell im Harmonisierungsvorschlag zur CRA-Konformität berücksichtigt wird, liefert praxisnahe Vorgaben für sichere Entwicklungsprozesse und technische Schutzmaßnahmen. So lassen sich etwa die Anforderungen der IEC 62443-4-1 für sichere Entwicklungsprozesse direkt auf die vom CRA geforderten Secure-by-Design-Prinzipien abbilden. Ebenso werden die technischen Anforderungen an Komponenten wie Zugriffskontrolle, gesicherte Kommunikation, Integritätsschutz oder Protokollierung von Sicherheitsereignissen, die gemäß IEC 62443-4-2 gelten, durch die im CRA geforderten grundlegenden Cybersecurity-Eigenschaften überprüfbar und konsistent umgesetzt.

Auch im Kontext von NIS-2 spielen derartige, anerkannte Standards eine zentrale Rolle. Sie bieten bewährte Strukturen für den Aufbau eines systematischen Sicherheitsmanagements. Gerade kleine und mittlere Unternehmen profitieren dabei von einem pragmatischen Ansatz: Standards sind Leitplanken, die schrittweise, bedarfsgerecht und ohne das plötzliche Aufkommen hoher Kosten umgesetzt werden können. Eine formale Zertifizierung ist für sie nicht zwingend erforderlich, wichtiger ist hier die Wirksamkeit der Maßnahmen im Alltag.

DIE EIGENTLICHE HERAUSFORDERUNG

Unabhängig vom Regelwerk gilt: Informationssicherheit ist kein kurzfristiges Projekt mit klassischem Enddatum. Bedrohungslagen verändern sich, Geschäftsmodelle entwickeln sich weiter, digitale Abhängigkeiten nehmen zu. Entsprechend müssen Unternehmen Infrastruktur, Risikomanagement, Maßnahmen und Verantwortlichkeiten regelmäßig überprüfen und anpassen.

Langfristig erfolgreich ist, wer Informationssicherheit in ein übergreifendes Konzept integriert, das sowohl organisatorische als auch technische Regeltätigkeiten umfasst. NIS-2 und CRA liefern dafür den regulatorischen Rahmen. Die eigentliche Herausforderung besteht darin, daraus eine Sicherheitskultur zu entwickeln, die über die bloße Pflichterfüllung hinausgeht. ■

MARLITT JULIKA STOLZ
ist Head of Management Systems & Audit bei der secunet Security Networks AG.

DR.-ING. RODRIGO DO CARMO
ist Head of Manufacturing and Information Security bei der secunet Security Networks AG.

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

NIS-2: Pflichtübung oder Rückenwind? Wie Compliance zu Resilienz wird

NIS-2 markiert den Punkt, an dem Cybersicherheit von der guten Absicht zur nachweisbaren Pflicht wird. Trotz der bisherigen NIS-1-Richtlinie und nationaler IT-Sicherheitsgesetze blieb die Cyberbedrohung in Europa hoch – vor allem fehlte eine einheitliche Umsetzung in den Mitgliedstaaten. In Deutschland ist das Umsetzungsgesetz seit dem 6. Dezember 2025 in Kraft. Unternehmen müssen sich registrieren, Vorfälle fristgerecht melden und ein angemessenes Risiko- und Sicherheitsmanagement dokumentieren. Das ist Regulierung – und zugleich die Chance, NIS-2 nicht als eine Übung auf dem Papier zu lesen, sondern als organisatorische Aufgabe zu betrachten.

Das BSI versteht NIS-2 als einen Gamechanger für Sicherheit und Stabilität und unterstützt Unternehmen mit einem NIS-2-Starterpaket, erklärenden Materialien, Kick-off-Webinaren sowie der Möglichkeit zur Vernetzung über die Allianz für Cyber-Sicherheit.

Ziel ist es, Unternehmen nicht allein zu lassen, sondern sie auf dem Weg zur NIS-2-Compliance strukturiert zu begleiten.

Der Mehrwert von NIS-2 liegt in der Struktur, die mit der Umsetzung entsteht: Das Sicherheitsniveau steigt, weil Schwachstellen systematisch sichtbar werden; das Risikomanagement gewinnt an Präzision und Steuerbarkeit; Business Continuity wird belastbar und die Wiederanlaufzeiten nach Vorfällen werden kürzer. Gleichzeitig stärkt NIS-2 den Datenschutz und erhöht das Vertrauen von Kunden und Partnern.

Kurz gesagt: NIS-2 ist weniger eine IT-Pflicht als ein strategischer Hebel für mehr Sicherheit, Resilienz und Vertrauen.

Prävention schlägt Intervention: Warum Endpoint Kontrollen im NIS-2-Kontext zählen

Security Controls sind das operative Rückgrat der NIS-2-Compliance. Die Richtlinie schreibt keine Produktlisten vor, sondern fordert wirksame technische und organisatorische Maßnahmen nach dem Stand der Technik, die sich an etablierten Rahmenwerken wie ISO oder NIST orientieren und auf die NIS-2-Maßnahmenfelder – von Risikoanalyse und Incident-Bewältigung über Kryptografie bis hin zur Zugriffskontrolle – einzahlen.

Ein hilfreiches Denkmodell ist die Kill Chain. Sie beschreibt die typischen Phasen eines Cyberangriffs. Entscheidend ist es, den Angriff zu verlangsamen oder sogar ganz zu verhindern. Je früher ein Angriff unterbrochen wird, desto geringer sind die Auswirkungen und Folgekosten. Deshalb gilt: Prävention ist besser als Intervention – alles, was sich verhindern lässt, muss später nicht entdeckt, analysiert und gemeldet werden.

Security Controls entlang der Kill Chain leisten dabei die kritische Arbeit im Vorfeld: Sie blockieren die nicht autorisierte Ausführung von Applikationen, kontrollieren Wechseldatenträger, härten Systeme und schließen bekannte Schwachstellen. Gleichzeitig erzeugen diese Controls auditfähige Artefakte (wie Policies, Logs, Reports), die die NIS-2-Pflichten im Hinblick auf Dokumentation und Meldewesen vereinfachen.

DriveLock: Von der Richtlinie zur operativen Wirksamkeit

Moderne Endpoint Security funktioniert nicht mit Insellösungen. Am wirksamsten sind die Critical Security Controls dann, wenn sie integriert gedacht, konsistent ausgerollt und zentral nachweisbar betrieben werden.

Genau hier setzt die DriveLock HYPERSECURE Platform an: Sie bündelt zentrale Security Controls in einer Plattform – cloudbasiert oder On-Premises, auf Wunsch als Managed Service. Die Module Device Control und Application Control sind das Herzstück; sie setzen direkt am Endpoint an und gehören zu den wenigen Lösungen am Markt mit Common-Criteria EAL 3+-Zertifizierung – ein Pluspunkt, wenn der „Stand der Technik" geprüft wird.

Darauf aufbauend ermöglicht das DriveLock BitLocker Management die zentrale Verwaltung der Windows-Verschlüsselung – inklusive Recovery Keys und Compliance-Nachweisen. Encryption Solutions sichern sensible Daten durchgängig – lokal, mobil sowie auch in Cloud-Szenarien, und Anti-Malware erkennt und blockiert Bedrohungen in Echtzeit, während Security Awareness gezielt den Faktor Mensch adressiert.

Ergänzt wird das Ganze durch Security Configuration Management für sichere Systemeinstellungen und Vulnerability Management, um Schwachstellen frühzeitig zu identifizieren und gezielt zu schließen.

Kurz gesagt: DriveLock übersetzt NIS-2-Anforderungen in messbare Kontrollen – dort, wo Angriffe ansetzen.

NIS-2 endet aber nicht am Endpoint. Wenn es um das Teilen sensibler und hochsicherer Daten geht, braucht es einen geschützten Kollaborationsraum, der Vertraulichkeit, Integrität und Nachvollziehbarkeit gewährleistet. Hier ergänzt die Lösung des DriveLock Tochterunternehmens idgard das DriveLock-Portfolio mit Sealed-Cloud-basierten Datenräumen, Ende-zu-Ende-Verschlüsselung und einem feingranulierten Rollen- und Rechtemodell.

Die DriveLock HYPERSECURE Platform ist offen aufgebaut, verfügt über eine API-basierte Architektur und lässt sich einfach in bestehende IT-Umgebungen integrieren sowie bei Bedarf gezielt erweitern.

Neben den eigenen Modulen können auch externe Lösungen angebunden werden, zum Beispiel SIEM-Systeme, Human-Risk-Assessments, Auswertungen zu in SharePoint geteilten Dokumenten oder unternehmensspezifische Workflows.

Mit seiner offenen Architektur und der Zusammenarbeit mit starken Plattform-Partnern stärkt DriveLock nicht nur die Sicherheit, sondern auch die digitale Souveränität und Unabhängigkeit von Unternehmen in Europa.

Fazit:

NIS-2 ist kein Selbstzweck – NIS-2 ist der Katalysator, um Security messbar und wirksam zu betreiben. Ihr praktischer Nutzen entsteht dort, wo Organisationen Risiko- und Sicherheitsmanagement systematisch auf- und fortsetzen – mit klaren Zuständigkeiten, aussagekräftigen Metriken, regelmäßigen Reviews und einer Beweisführung, die Auditfragen standhält.

Der Aufwand bleibt, aber er schafft Transparenz über Risiken und Prioritäten – und liefert dem Management belastbare Grundlagen für Entscheidungen. So wird aus Compliance ein laufender Prozess und aus Resilienz ein messbares Ergebnis. ■

Infobox: In sechs Schritten von Compliance zu operativer Resilienz

1. **Betroffenheit klären und registrieren:** Einstufung vornehmen und die Registrierung beim BSI abschließen; das BSI-Portal als One-Stop-Shop für Meldungen und Nachweise etablieren.
2. **Risikoanalyse professionalisieren:** Asset-Inventar, Bedrohungs-/Schwachstellenlage und Business-Impact konsistent erheben und Normbezug (ISO 27001/27002, CIS, NIST) dokumentieren.
3. **Kontrollen entlang der Kill Chain implementieren:** DriveLock-Module an kritischen Angriffsvektoren platzieren und Wirksamkeit messen.
4. **Kollaboration absichern:** Externe Austauschprozesse über idgard-Datenräume mit Audit-Trail und granularen Rechten standardisieren.
5. **Meldekonzept testen:** 24-/72-Stunden-/30-Tage-Prozesse als Playbook definieren, Kommunikationskanäle (inkl. Notfall-Datenraum) einüben.
6. **Nachhaltig verankern:** Awareness-Programm, kontinuierliches Monitoring und Reporting, regelmäßige Management-Reviews aufsetzen; Lessons Learned in Härtung und Policies zurückführen.

Mehr dazu hier

DriveLock

Wenn jede Minute zählt

Wie F24 Unternehmen unterstützt, NIS-2-Vorgaben operativ umzusetzen

F24 ist Europas führender Software-as-a-Service-(SaaS)-Anbieter für Resilienz. Mit FACT24 bietet das Unternehmen alle Funktionen, die Unternehmen brauchen, um die Anforderungen der NIS-2-Richtlinie im Alltag umzusetzen – von der technischen Alarmierung über das Incident- und Krisenmanagement bis zur Qualifizierung der handelnden Personen. Statt nur Konzepte und Dokumente vorzuhalten, etabliert FACT24 einen durchgängigen Prozess, der im Ernstfall unter Zeitdruck funktioniert und die Meldepflichten strukturiert unterstützt.

Die 24-Stunden-Frist ist ein Organisationsproblem

Ein Ransomware-Angriff legt Teile der Infrastruktur lahm, die IT nimmt Systeme präventiv vom Netz und der Krisenstab soll zusammenkommen: Genau in diesem Moment fehlt oft das, was NIS-2 voraussetzt: ein eingespielter, gelebter Melde- und Entscheidungsprozess.

Typische Bruchstellen:

- **Unklare Zuständigkeiten:** Wer löst den „Notruf" an BSI oder CSIRT aus, wer gibt die Freigabe?
- **Unvollständige Informationen:** Welche Systeme sind betroffen, welche Services sind ausgefallen? Sind Daten abgeflossen?
- **Medienbrüche:** Verteilter E-Mail-Verkehr, Excel-Listen, manuelle Notizen – niemand behält den Überblick.

Gleichzeitig steigt der Druck auf die Unternehmensleitung: NIS-2 macht Cybersicherheit zur Führungsaufgabe. Leitungsorgane müssen nachweisen, dass sie angemessene technische und organisatorische Maßnahmen getroffen haben, inklusive wirksamer Melde- und Krisenprozesse.

Aus Vorgaben werden Abläufe: NIS-2 mit FACT24 abbilden

NIS-2 verlangt unter anderem ein wirksames Incident Handling, Business Continuity Management (BCM) und Krisenmanagement, sichere Kommunikationskanäle sowie klar geregelte Meldewege an Behörden. FACT24 bündelt zentrale Anforderungen rund um Incident Handling, Business

Continuity, Krisenkommunikation und Meldeprozesse in einer integrierten SaaS-Plattform.

Im System können dafür Rollen, Zuständigkeiten und Eskalationsstufen hinterlegt werden – von der technischen Detektion bis zur Entscheidung über eine Meldung. Das System führt Schritt für Schritt durch den Vorfall: Wer wird wann eingebunden, welche Informationen müssen vorliegen, welche Entscheidung ist zu treffen? Auf dieser Basis können auch die 24-Stunden-Frühwarnung, die 72-Stunden-Meldung und der Abschlussbericht als wiederkehrende Prozesse abgebildet werden.

Antatt im Einzelfall immer wieder neu improvisieren zu müssen, definieren Unternehmen die wesentlichen Meldepfade einmal sauber. Diese stehen danach jederzeit abrufbereit zur Verfügung – inklusive Vorlagen, Checklisten und einheitlicher Dokumentation.

Handlungsfähig bleiben: Out-of-Band-Alarmierung mit FACT24 ENS+

Ein zentrales Problem im Cybervorfall ist die Erreichbarkeit der Schlüsselpersonen. Genau hier setzt FACT24 ENS+ an. Als cloudbasierte Alarmierungslösung arbeitet sie unabhängig von der eigenen, möglicherweise angegriffenen IT-Infrastruktur.

Über ein sicheres Webinterface oder die App lösen die Verantwortlichen mit wenigen Schritten Alarmierungen aus. Vordefinierte Gruppen wie Krisenstab, IT-Forensik, Datenschutz oder Management werden parallel über Anruf, SMS, E-Mail und App-Push-Nachrichten kontaktiert. FACT24 ENS+ erfasst Rückmeldungen automatisch, überspringt nicht reagierende Personen nach einem festgelegten Intervall und startet bei Bedarf direkt aus der Alarmierung heraus eine Konferenz.

So verwandeln Unternehmen das theoretische „Wir müssen den Krisenstab zusammenbekommen" in einen technisch und organisatorisch abgesicherten Prozess und erfüllen damit eine Kernvoraussetzung, um die knappen NIS-2-Fristen praktisch einhalten zu können.

FACT24 CIM: Incident- und Krisenmanagement als durchgängiger Prozess

Aufbauend auf der Alarmierung erweitert FACT24 CIM den Blick auf das gesamte Incident- und Krisenmanagement. Anstelle verstreuter Informationen in E-Mails und Tabellen bietet die Plattform ein zentrales Cockpit zur Steuerung des Vorfalls.

Hier erfasst das Team Ereignisse strukturiert, bewertet sie, macht Auswirkungen auf kritische Dienstleistungen, Standorte und Kunden sichtbar und steuert Maßnahmen. Aufgaben lassen sich zuweisen, Fristen überwachen, Status und Entscheidungen werden umfassend dokumentiert.

Für NIS-2 besonders relevant: In FACT24 CIM können konkrete Abläufe zur Erfüllung der Meldepflichten hinterlegt werden – von der ersten Lagebewertung über die Entscheidung zur Frühwarnung bis hin zum Erstellen einer strukturierten Vorfallmeldung. Vorlagen für die Kommunikation mit Behörden, Aufsichtsstellen oder Kunden lassen sich im System ablegen und im Vorfall mit aktuellen Informationen befüllen. Die automatisch erzeugte Chronik unterstützt zudem bei der Erstellung des Abschlussberichts und schafft nachvollziehbare Nachweise der getroffenen Maßnahmen.

Vom Papier zur Routine: NIS-2-Prozesse trainieren mit FACT24 EDU

Richtlinien und Systeme allein reichen nicht aus, wenn die Beteiligten im Ernstfall unsicher sind. NIS-2 betont deshalb ausdrücklich Schulung, Awareness und regelmäßige Übungen. FACT24 EDU ergänzt die technische Plattform genau an diesem Punkt.

Das E-Learning-Angebot vermittelt Grundlagen zu Resilienz, Business Continuity, Krisenmanagement und Informationssicherheit. Die Inhalte richten sich an unterschiedliche Zielgruppen im Unternehmen – von Mitarbeitenden über Fach- und Linienverantwortliche bis hin zu Mitgliedern von Krisenstäben und Management. Im Fokus steht dabei nicht nur Theorie, sondern die konkrete Rolle im Notfall: Wie läuft ein Incident ab, welche Schritte sind wann erforderlich, wer trifft welche Entscheidung?

In Verbindung mit der Plattform können Unternehmen realitätsnahe Übungen durchführen – etwa Cyberszenarien, bei denen die Alarmierung, Lageführung, Kommunikation und Dokumentation mit FACT24 durchgespielt werden. So werden NIS2-Prozesse nicht nur definiert, sondern auch regelmäßig geübt und verinnerlicht.

Mehr Sicherheit für IT, BCM und Geschäftsleitung

FACT24 macht die Anforderungen aus NIS-2 für unterschiedliche Verantwortliche greifbar:

- **IT- und Security-Verantwortliche** erhalten einen belastbaren „Out of-Band"-Kanal, der die Lücke zwischen Detektion und qualifizierter Reaktion schließt.
- **BCM- und Krisenmanager** können Planungen, Alarmierungen, Maßnahmensteuerung und Nachbereitung in einem System abbilden – inklusive der für NIS-2 wichtigen Nachweise.
- **Geschäftsleitungen** stärken ihre Sorgfaltspflicht, indem sie auf eine Plattform setzen, die auf die operativen Anforderungen der Richtlinie ausgerichtet ist und im Vorfall zeigt, dass Ihr Unternehmen angemessene technische und organisatorische Maßnahmen etabliert hat.

Mit FACT24 und FACT24 EDU wird NIS-2 für Unternehmen operativ beherrschbar: Sie bleiben auch im Ernstfall meldefähig, handlungsfähig und nachweislich gut aufgestellt. ■

F24

Das Ende der Sorglosigkeit:

Wie NIS-2 und CRA die Spielregeln für Open-Source-Software neu definieren

Autor: Chris Dimitriadis,
Chief Global Strategy Officer, ISACA

Open-Source-Software (OSS) ist das Betriebssystem der digitalen Transformation in Europa. Seine Attraktivität ist unbestritten und der Vormarsch unaufhaltsam: Unternehmen setzen auf OSS, weil es Kosteneffizienz verspricht, Entwicklungszyklen drastisch verkürzt und die gefährliche Abhängigkeit von einzelnen Herstellern (Vendor Lock-in) reduziert. Die offene, kollaborative Natur von OSS führt oft zu außergewöhnlicher Qualität und Sicherheit, da nach dem Prinzip „viele Augen sehen mehr" Fehler schneller entdeckt und behoben werden. Ganze Branchen kooperieren in Open-Source-Projekten, um gemeinsame Herausforderungen zu stemmen und zukunftsfähige Standards zu etablieren: zum Beispiel Unternehmen aus dem Bereich Automotive in der Eclipse SDV Working Group zur Beschleunigung der Entwicklung softwaredefinierter Fahrzeuge (SDVs). Auch die EU ist sich dieses Potenzials bewusst und fördert den Einsatz von OSS gezielt, um die digitale Souveränität Europas zu stärken.

Doch die strategische Unabhängigkeit hat eine Kehrseite: Sie schafft eine neue, tiefgreifende Form der technischen Abhängigkeit von einer globalen, oft unübersichtlichen Software-Lieferkette. Jede moderne Anwendung besteht heute aus einem komplexen Gefüge unzähliger OSS-Komponenten, die wiederum von weiteren Bibliotheken abhängig sind. Die wahre Gefahr liegt im Verborgenen: Viele Unternehmen wissen oft gar nicht, welche Elemente genau in ihren Systemen verbaut sind.

Der Log4j-Vorfall Ende 2021 hat dieses Risiko für alle sichtbar gemacht: Eine kritische Lücke in einer einzigen, weitverbreiteten Protokollierungsbibliothek ermöglichte Angreifern die vollständige Übernahme von Servern weltweit und löste eine beispiellose, globale Abwehraktion aus, bei der Unternehmen verzweifelt versuchten, herauszufinden, ob und wo sie verwundbar waren. Log4j war überall. Nicht nur in sichtbaren Anwendungen, sondern auch als Abhängigkeit in anderen Bibliotheken und kom-

Bild: ISACA

merziellen Produkten. Viele Unternehmen wussten gar nicht, dass und wo sie Log4j einsetzen.

Der regulatorische Rahmen und die zentrale Herausforderung

In diesem Spannungsfeld stellt sich die entscheidende Frage: Wie lässt sich das enorme Innovationspotenzial von Open Source mit den neuen, strengen Sicherheitsanforderungen von NIS-2 und dem Cyber Resilience Act (CRA) in Einklang bringen? Die EU reagiert mit einem klaren Kurs:

- **NIS-2** verpflichtet Betreiber wesentlicher und wichtiger Einrichtungen, im Rahmen ihres Risikomanagements, die Sicherheit ihrer gesamten Lieferkette zu bewerten und abzusichern. Die Verantwortung wird damit über die eigenen Unternehmensgrenzen hinaus auf Software-Zulieferer erweitert.

- Der **CRA** zielt direkt auf die Produktsicherheit ab und führt praktisch ein „CE-Zeichen" für Software ein. Hersteller von Produkten mit digitalen Elementen haften künftig für deren Sicherheit über den gesamten Lebenszyklus. Dies schließt explizit alle integrierten Open-Source-Komponenten mit ein und umfasst konkrete Pflichten wie Security-by-Design, die Erstellung einer Software-Inventarliste (Software Bill of Materials, SBOM) und ein verpflichtendes Schwachstellenmanagement.

Dies ist keine rein europäische Entwicklung. Weltweit steigen die Anforderungen an die Sicherheit der Lieferketten, so auch in den Vereinigten Staaten durch das CMMC-Programm (Cybersecurity Maturity Model Certification) für die industrielle Basis des Verteidigungssektors. Obwohl sich die regulatorischen Mechanismen unterscheiden, ist die Stoßrichtung dieselbe: Von Organisationen wird zunehmend erwartet, dass sie nachweisen, dass Cybersicherheitskontrollen nicht nur auf dem Papier definiert, sondern auch über Drittanbieterbeziehungen und Software-Lieferketten hinweg implementiert und bewertet werden. Für europäische Unternehmen, die international tätig sind oder mit den USA verbundene Verteidigungsökosysteme unterstützen, erhöht dies die Dringlichkeit, wiederholbare und nachweisbasierte Sicherheits- und Prüfpraktiken zu etablieren.

Herausforderung und Chance – eine Neubewertung für die Branche

Katalysator oder Bremse: In den Fluren europäischer Tech-Unternehmen wird diese Frage kontrovers diskutiert. Zweifellos bedeuten diese Pflichten zunächst einen erheblichen Mehraufwand für Dokumentation und Prozesse. Es entstehen neue Haftungsrisiken und die Sorge, dass die Innovationsgeschwindigkeit durch komplexe Compliance-Anforderungen leiden könnte.

Doch diese Betrachtungsweise greift aus Sicht von ISACA, dem globalen Berufsverband für IT-Governance, -Risiko, -Sicherheit, Datenschutz und IT-Audit, zu kurz, denn die Regulierung ist gleichzeitig eine positive Entwicklung, die einen Reifeprozess für den gesamten Markt erzwingt. Sie beendet die „Wild-West-Ära" der OSS-Nutzung, in der Komponenten oft aus reiner Bequemlichkeit und ohne tiefere Sicherheitsprüfung eingesetzt wurden. Unternehmen, die OSS bisher nur als kostenlosen Steinbruch für Code betrachtet haben, müssen daher radikal umdenken. Jetzt ist ein bewusstes, risikobasiertes und professionelles Vorgehen gefordert. Dies steigert nicht nur die Sicherheit, sondern hebt auch die Qualität, da nun gut gewartete und transparente OSS-Projekte klar im Vorteil sind. Die neuen Regeln sind somit weniger eine Bremse als vielmehr ein starker Impuls für mehr Sicherheit und Vertrauen in das gesamte digitale Ökosystem.

Struktur, Kompetenz und Wissen heißen die Zauberworte

Um diesen Wandel erfolgreich zu gestalten, sind drei Säulen entscheidend: eine klare Governance, nachweisbare Kompetenz und aktuelles Wissen. In allen Punkten unterstützt ISACA Unternehmen und Fachkräfte mit seiner globalen und herstellerneutralen Expertise. Als Berufsverband mit über 50 Jahren Erfahrung und mehr als 185.000 Mitgliedern weltweit hilft ISACA dabei, Standards für Exzellenz zu etablieren. Dieser ganzheitliche Ansatz, der IT-Audit, Governance, Risiko und Sicherheit verbindet, macht ISACA zu einem vertrauenswürdigen Ratgeber und wichtigem Informationsanbieter in dieser Situation.

- Für die Governance stellt beispielsweise das ISACA-Framework COBIT® den idealen Rahmen, um die von NIS-2 und CRA geforderten Prozesse für Risiko-, Lieferanten- und Schwachstellenmanagement strukturiert aufzusetzen und nachweisbar zu steuern.

- Um die notwendige Kompetenz nachzuweisen, validieren die global anerkannten Zertifizierungen von ISACA genau jene Fähigkeiten, die jetzt erfolgskritisch sind: CISM®-zertifizierte Manager gestalten die Sicherheitsstrategie, CRISC®-zertifizierte Experten managen die neuen Lieferkettenrisiken und CISA®-zertifizierte Auditoren prüfen die Wirksamkeit der Maßnahmen und sichern die Compliance. Darüber hinaus bildet ISACA im Bereich der KI die nächste Generation von Auditoren in den Bereichen Audit (AAIA), Cybersicherheit (AAISM) und Risiko (AAIR) aus. Ebenso schafft ISACA im Hinblick auf branchenspezifische Anforderungen die Fachkräfte für CMMC durch CCA, CCP und CCI.

- Aktuelles Wissen bietet ISACA durch praxisnahe Leitfäden, globale Studien und eine aktive Experten-Community. Sie vermitteln die notwendige Orientierung, um in der dynamischen Regulierungs- und Bedrohungslandschaft fundierte Entscheidungen zu treffen.

Aus Pflicht wird strategischer Vorteil

Die Zukunft der Innovation in Europa wird auf Open Source gebaut. NIS-2 und der CRA schaffen dabei die verlässliche Vertrauensbasis, auf der diese Innovation sicher wachsen kann. Für Unternehmen lautet die entscheidende Frage daher nicht, ob sie ihre Prozesse anpassen, sondern wie sie diesen Wandel als Chance nutzen können. Wer die neuen Regeln nur als lästige Compliance-Aufgabe begreift, bleibt im Verteidigungsmodus. Wer sie jedoch als Mandat für Exzellenz in Sicherheit und Governance versteht, schafft Vertrauen – und macht es zu seinem entscheidenden Wettbewerbsvorteil. ■

Mehr dazu hier

ISACA®

- ADVERTORIAL -

NIS-2 umsetzen: Von regulatorischer Pflicht zu messbarer Cyberresilienz

Autorin: Karin Paulsen, HiScout GmbH

Mit der EU-NIS-2-Richtlinie wurden die Spielregeln für Cybersicherheit in Europa neu definiert. Seit dem 6. Dezember 2025 ist auch in Deutschland das NIS-2-Umsetzungsgesetz (NIS2UmsuCG) in Kraft. Für viele Organisationen stellt sich damit nicht mehr die Frage, ob sie betroffen sind, sondern *wie sie NIS-2 wirksam umsetzen können.*

Gefordert sind unter anderem ein systematisches Risikomanagement, strukturierte Incident-Meldeprozesse, belastbare Notfall- und Krisenkonzepte, Maßnahmen zur Lieferkettensicherheit sowie eine umfassende, jederzeit prüfbare Dokumentation. Für die Organisationen bedeutet das: Maßnahmen müssen nicht nur geplant, sondern als technische und organisatorische Kontrollen wirksam umgesetzt und jederzeit nachweisbar sein.

Wer NIS-2 richtig umsetzt, erfüllt jedoch nicht nur regulatorische Pflichten. Die Richtlinie bietet die Chance, Cyberresilienz als festen Bestandteil der Unternehmenssteuerung zu etablieren. Risiken werden priorisiert, Verantwortlichkeiten klar geregelt, Maßnahmen konsequent verfolgt und Ergebnisse auditfest belegt.

NIS-2 umsetzen heißt: Sicherheit strategisch steuern

Die NIS-2-Richtlinie betrifft nicht nur klassische KRITIS-Betreiber, sondern erweitert den Kreis der betroffenen Einrichtungen deutlich – auch in Wirtschaft und öffentlicher Verwaltung. Gefordert werden unter anderem ein funktionsfähiges Informationssicherheits-Managementsystem (ISMS), ein etabliertes Business Continuity Management (BCM), aktives Schwachstellen- und Risikomanagement sowie klare Melde- und Nachweispflichten bei Sicherheitsvorfällen.

Diese Anforderungen durchziehen alle Ebenen der Organisation – von der operativen IT bis zur Geschäftsführung. Ein isolierter Blick auf Einzelthemen greift zu kurz. Wer NIS-2 umsetzen will, benötigt ein integriertes Vorgehen, das Transparenz schafft, Verantwortlichkeiten verbindlich regelt und kontinuierliche Verbesserung ermöglicht – im Audit ebenso wie im Ernstfall.

Die Falle punktueller Lösungen

In der Praxis starten viele Unternehmen mit Einzellösungen: Risikoanalysen in separaten Tools, Backups als Insellösungen, Excel-Listen zur Dokumentation. Dieser Patchwork-Ansatz führt jedoch häufig zu Medienbrüchen, lückenhaften Nachweisen und hohem manuellen Aufwand ohne den Sicherheitsgewinn, den NIS-2 eigentlich erreichen will.

Für eine nachhaltige NIS-2-Umsetzung braucht es deshalb Systeme, die Risiken, Maßnahmen, Governance und Reporting zusammenführen. Nur so lassen sich regulatorische Anforderungen effizient erfüllen und gleichzeitig die operative Resilienz stärken.

Integrierte Software als Enabler für NIS-2-Compliance

Die **HiScout GRC Suite** unterstützt Organisationen dabei, NIS-2 strukturiert und nachvollziehbar umzusetzen. Sie setzt genau dort an, wo NIS-2 Wirkung entfalten soll: bei der zentralen Steuerung, Standardisierung und Nachweisbarkeit aller relevanten Sicherheitsprozesse. Die Plattform vereint Informationssicherheit, Risikomanagement, BCM, Incident Handling und Reporting in einer integrierten Lösung und macht damit Anforderungen, Umsetzungsstand und Verantwortlichkeiten jederzeit transparent und auditfest.

Ein wesentlicher Effizienzhebel sind **wiederverwendbare Sicherheitsprofile:** Anstatt Anforderungen und Maßnahmen „jedes Mal neu" aufzusetzen, lassen sich Template-basierte Profile erstellen und über Organisationseinheiten hinweg konsistent ausrollen. Das reduziert manuellen Aufwand, erhöht die Vergleichbarkeit und beschleunigt die Umsetzung – besonders in komplexen Strukturen.

Kreuzreferenzen sorgen zudem für eine klare Nachvollziehbarkeit: Es ist jederzeit ersichtlich, welche Anforderungen auf welche Bedrohungen wirken, wie der Umsetzungsstatus aussieht und welcher Reifegrad erreicht wurde. Eine strukturierte Gap-Analyse zeigt frühzeitig, wo Organisationen im Vergleich zu den konkreten NIS-2-Vorgaben stehen, und bildet die Grundlage für eine priorisierte, realistische Umsetzungs-Roadmap, die nach Risiko und Business Impact priorisiert – mit klaren Aufgaben, Terminen und Fortschrittskontrolle.

Darüber hinaus schafft die Plattform Governance-Strukturen: Rollen und Verantwortlichkeiten werden eindeutig zugeordnet, Freigabeprozesse nachvollziehbar gemacht und Entscheidungen dokumentiert – ein wesentliches Element für wirksame Compliance und eine belastbare Managementsteuerung.

Mehr als Compliance: Operative Resilienz schaffen

Die Umsetzung von NIS-2 bedeutet mehr als nur die Erfüllung regulatorischer Pflichten. Entscheidend ist die Integration in den operativen Alltag:

- Risikomanagement als Steuerungsinstrument – nicht als Pflichtübung.
- Incident-Response-Prozesse, die geübt und belastbar sind.
- Business-Continuity-Pläne, die getestet, geübt und aktuell gehalten werden.
- Lieferketten-Transparenz, die Risiken frühzeitig erkennt und steuert.

HiScout unterstützt all diese Bereiche durch eine zentrale Datenbasis und durchgängige Nachverfolgbarkeit von Maßnahmen. Das Ergebnis ist eine gemeinsame, belastbare Sicherheitslage und eine messbar höhere Widerstandsfähigkeit gegenüber Cyberbedrohungen.

Praxisnahe Nachweisführung

Ein Kernelement von NIS-2 ist die Nachweisfähigkeit. Ob Audit, Prüfung oder Sicherheitsvorfall: Unternehmen müssen jederzeit – insbesondere im Rahmen der Meldeepflicht – belegen können, wie Risiken bewertet, Maßnahmen umgesetzt und Vorfälle behandelt wurden.

Die HiScout GRC Suite unterstützt dabei methodisch sauber und operativ effizient – von der Gap-Analyse über Risikobewertung und Governance bis hin zu Incident-Management und Reporting. Damit wird die NIS-2-Umsetzung auch gegenüber Aufsichtsbehörden und Prüfern belastbar darstellbar – ein klarer Vorteil gegenüber manuellen oder fragmentierten Lösungen.

Fazit: NIS-2 umsetzen als strategische Chance

NIS-2 ist kein lästiges Pflichtprogramm, sondern ein Wendepunkt für Cybersicherheit und Unternehmenssteuerung. Wer die Anforderungen strukturiert umsetzt, schafft nicht nur Compliance, sondern nachhaltige Cyberresilienz.

Mit der HiScout GRC Suite gelingt dies nicht nur methodisch sauber, sondern auch operativ effizient: von der Gap-Analyse und Risikobewertung über standardisierte Sicherheitsprofile bis hin zu Nachweisführung, Governance und Incident-Management.

NIS-2 umsetzen heißt: Heute handeln, um morgen resilient zu sein.

Mehr zur strukturierten Umsetzung der NIS-2-Anforderungen mit Software erfahren Sie auf:

www.hiscout.com/nis-2-umsetzen/

Mehr dazu hier

Webinar: NIS-2 umsetzen mit HiScout

Erfahren Sie, was NIS-2 konkret bedeutet und wie Sie die Anforderungen revisionssicher und effizient umsetzen.

In diesem Webinar lernen Sie unter anderem:

- NIS-2-Pflichten und Betroffenheit
- Gap-Analyse und Reifegrad-Check
- Risiko- und Schwachstellenmanagement
- Lieferketten- und Drittanbieterrisiken
- Incident- und Audit-Ready-Reporting
- Live-Demo der NIS-2-Umsetzung mit HiScout

Jetzt Webinar-Platz sichern!

HiScout GmbH
Schloßstraße 1, 12163 Berlin
Tel +49 (30) 33 00 888-0
info@hiscout.com
www.hiscout.com

HiScout
Be Prepared!

Zwischen CRA-Konformität und NIS-2-Anforderungen:

Die Herausforderungen einer harmonisierten sicheren Produktentwicklung


Autor/in:
Marlitt Julika Stolz, Head of Management Systems and Audit - secunet Security Networks AG
Dr.-Ing. Rodrigo do Carmo, Head of Manufacturing and Information Security - secunet Security Networks AG

Digitale Produkte sind heute integraler Bestandteil nahezu aller Geschäftsmodelle. Software steuert Maschinen, vernetzt Produktionsanlagen und ermöglicht gänzlich neue Services. Gleichzeitig steigt mit jeder zusätzlichen digitalen Schnittstelle die Angriffsfläche für Cyberangriffe. Sicherheitslücken wirken dabei selten isoliert, sondern entlang des gesamten Lebenszyklus seiner Produkte, von der Entwicklung über den Betrieb bis hin zu Kundenumgebungen.

Genau an diesem Punkt setzt der europäische Cyber Resilience Act (CRA) an. Er formuliert erstmals verbindliche und überprüfbare Sicherheitsanforderungen an Produkte mit digitalen Elementen sowie deren Herstellungs- und Entwicklungsprozesse. Ergänzend adressiert das deutsche NIS-2-Umsetzungsgesetz schwerpunktmäßig die organisatorischen Rahmenbedingungen der Informationssicherheit auf Unternehmensebene. Sie eint die Forderung einer Umsetzung geeigneter Maßnahmen zur Gewährleistung der Informationssicherheit bei der Entwicklung von IT-Systemen und Produkten mit digitalen Elementen ein. Aus diesem Grund sind betroffene Unternehmen dazu angehalten, beide Gesetze gemeinsam zu denken und einen integrierten Ansatz zu schaffen. secunet unterstützt Sie dabei, die richtigen Maßnahmen zu definieren und umzusetzen.

Der CRA rückt die Produktentwicklung in den Fokus

Während das deutsche NIS-2-Umsetzungsgesetz bewusst technologieneutral bleibt und auf einem hohen Abstraktionsniveau Anforderungen an Governance, Risikomanagement und Nachweisfähigkeit formuliert, geht der CRA deutlich weiter. Er konkretisiert Anforderungen an die sichere Entwicklung von Produkten mit digitalen Elementen und macht diese überprüfbar. Im Mittelpunkt stehen dabei nicht nur technische Sicherheitsprinzipien. Auch eine nachvollziehbare Cybersecurity-Risikobewertung sowie Anforderungen an Prozesse und Nachweise über den gesamten Produktlebenszyklus werden adressiert. Das rückt auch einzelne Prozessschritte in der Entwicklung, saubere Dokumentation, Schwachstellenmanagement, koordinierte Offenlegung und die Update-Fähigkeit verbindlich in den Fokus. Damit rückt die Produktentwicklung selbst – und nicht allein die Organisation – in den Mittelpunkt der Regulierung.

secunet hilft, Synergiepotenziale zu erkennen und zu nutzen

Beide Regelwerke verlangen ein strukturiertes Risikomanagement, geeignete Sicherheitsmaßnahmen und die Fähigkeit, deren Umsetzung nachzuweisen. Während NIS-2 dabei schwerpunktmäßig die

Bild: secunet

organisatorische Grundlage für Cybersicherheit schafft, führt der CRA diese mit seiner produktbezogenen Konkretisierung fort. Gerade diese Differenz eröffnet Synergien. Ein harmonisierter Ansatz verbindet Governance, Rollen und Entscheidungswege mit einem belastbaren Secure-Development-Lifecycle für Produkte. So entsteht ein integriertes Sicherheitskonzept, das regulatorische Anforderungen erfüllt und zugleich praxistauglich bleibt.

Ausgangspunkt einer solchen kombinierten Umsetzung ist eine einheitliche Risikomanagement-Methodik, die sowohl unternehmensbezogene Risiken als auch produktbezogene Cybersecurity-Risiken erfasst. Gängige Standards wie der ISO/IEC 27001 und der IEC 62443 bieten hierfür einen stabilen Rahmen, ohne die notwendige Flexibilität einzuschränken.

Auf dieser Basis lassen sich dann CRA- und NIS-2-relevante Anforderungen, Best Practices und Lösungen im Bereich sichere Softwareentwicklung systematisch zusammenführen. Dazu gehören unter anderem:

- übergreifende Organisation inkl. Verantwortlichkeiten,
- zielgerichtetes Risikomanagement,
- sichere Entwicklungsprinzipien wie „Security by Design“ und „Security by Default“,
- verbindliche Verantwortlichkeiten, Schulungen und Awareness für Engineering und Betrieb,
- eine eindeutige Gestaltung des Entwicklungsprozesses,
- die Durchführung und Dokumentation von Code-Reviews,
- Sicherheitstests und Release- bzw. Update-Freigaben,
- Vulnerability Handling und eine koordinierte Schwachstellenbehandlung,
- das Management von Komponenten und Abhängigkeiten, etwa durch transparente Stücklisten für Software,
- Dokumentation in Form von Sicherheitskonzepten.

Ein standardisierter Anforderungskatalog basierend auf CRA und NIS-2, wie ihn secunet verwendet, hilft, diese Themengebiete zu strukturieren und in umsetzbare Schritte zu übersetzen. Entscheidend ist dabei, bestehende Prozesse nicht einfach neu zu erfinden, sondern gezielt weiterzuentwickeln.

Gap-Analyse, Risikoanalysen, Quality Gates und Umsetzung

Im nächsten Schritt zeigt eine Gap-Analyse, wo bestehende Prozesse bereits CRA- und NIS-2-konform sind und an welchen Stellen konkreter Handlungsbedarf besteht. Dabei geht es nicht nur um formale Abweichungen, sondern um die Frage, wie wirksam die bestehenden Sicherheitsmaßnahmen tatsächlich sind.

Entsprechend lassen sich individuelle Risikoanalysen ableiten, die gezielt die unterschiedlichen Entwicklungs- und Betriebsphasen betrachten. Bewertet wird, ob sowohl die organisatorischen Strukturen im Sinne von NIS-2 als auch die produktbezogenen Entwicklungs- und Betriebsprozesse im Sinne des CRA ein angemessenes Sicherheitsniveau gewährleisten oder ob zusätzliche, kontextspezifische Risiken wie Lieferketten, Legacy-Komponenten oder die OT-Anbindung adressiert werden müssen. In der Praxis bewährt sich hierfür eine phasenweise Umsetzung, etwa über definierte „Quality Gates“, die die Ergebnisse der Risikobewertung systematisch berücksichtigen, von der Konzeption über Entwicklung und Test bis hin zu Betrieb, Wartung und Update-Management.

Die gewonnenen Erkenntnisse münden schließlich in eine priorisierte Maßnahmenplanung, die kurzfristig realisierbare Verbesserungen und strukturelle Anpassungen zusammenfasst und deren Umsetzung gezielt steuert. All das erfordert regulatorisches Verständnis, technisches Know-how und Erfahrung aus der Praxis. secunet begleitet seit vielen Jahren Organisationen bei der Umsetzung regulatorischer Anforderungen und der sicheren Gestaltung von IT- und Produktentwicklungsprozessen. Dieses Wissen fließt in strukturierte Vorgehensmodelle, praxiserprobte Methoden und umsetzungsnahe Maßnahmenkataloge ein.

Ein integriertes Sicherheitskonzept statt isolierter Compliance

Das Ergebnis dieses Vorgehens ist ein ganzheitliches Sicherheitskonzept für die Herstellung, Entwicklung und den Betrieb digitaler Produkte. Es bündelt die CRA-relevante Anforderungen, dokumentiert relevante Nachweise und Abhängigkeiten und beschreibt, wie die konkrete Umsetzung im Unternehmen im Einklang mit geltenden Prozessbeschreibungen, Richtlinien oder Arbeitsanweisungen gelingen soll. Governance-Strukturen, Risikomanagementanforderungen und produktbezogene Sicherheitsmaßnahmen sowie Nachweispflichten greifen dabei ineinander.

Der Mehrwert liegt auf der Hand: Prozesse und Rollen müssen nur einmal angepasst werden, anstatt dieselben Fragestellungen mehrfach zu bearbeiten. Unternehmen gewinnen Klarheit, Effizienz und vor allem belastbare Resilienz, über reine Compliance hinaus. So wird aus regulatorischem Druck eine Chance: für sichere Produkte, robuste Prozesse und eine Informationssicherheit, die nicht nur auf dem Papier besteht, sondern im Alltag wirkt. ■

Mehr dazu hier

secunet

Industrial Cyber Security:

KI wird zur dominanten Technologie

Aufgrund der geopolitischen Veränderungen steigen die Anforderungen an die Cybersicherheit rasant. Dabei stehen insbesondere Industrieunternehmen unter wachsendem Druck. Der Cyber-Security-Experte Götz Schartner, Gründer und CEO der 8com GmbH & Co. KG, einem der führenden deutschen Anbieter für SOC-as-a-Service und Managed Security Services, wird mit seinem Unternehmen auf der kommenden HANNOVER MESSE sein Security Operations Center realitätsgetreu nachbauen, sodass die Messebesucher*innen Cyber Security live erleben können.

Seiner Meinung nach hat sich Cyberkriminalität zu einer hocheffizienten Industrie entwickelt. Cybercrime-as-a-Service macht Angriffe skalierbar, günstig und für nahezu jeden zugänglich. Komplett fertige Angriffsketten, Erpressungsinfrastruktur und automatisierte Tools sind frei verfügbar. Die Grenzen zwischen kriminellen Gruppen und staatlich gesteuerten Akteuren verschwimmen dabei zunehmend. Dabei hebt künstliche Intelligenz (KI) Angriffe und Verteidigung auf ein neues Niveau: KI wird 2026 zur dominanten Technologie in Angriff und Abwehr. Angreifer nutzen KI, um Phishing, Social Engineering, Schwachstellenanalyse und gesamte Angriffskampagnen zu automatisieren. Auch in der Verteidigung wird KI künftig eine zentrale Rolle einnehmen – ob bei der Erkennung von Anomalien und Angriffsmustern, der Triage von Alarmen oder für die Incident Response. Schartners Fazit: Cybersicherheit ist nicht länger eine Zusatzaufgabe – sie ist Grundvoraussetzung für Stabilität und Zukunft. Unternehmen, die Risiken verstehen, Prozesse beherrschen und ihre Sicherheitsstrategie realistisch ausrichten, werden 2026 besser bestehen als jene, die weiterhin nur reagieren.

Secomea, eine 100%ige Tochterfirma von McNaughton-McKay Electric USA, präsentiert auf der HANNOVER MESSE 2026 eine sichere, Zero-Trust-basierte Remote-Access-Lösung für industrielle Umgebungen. Die speziell für OT konzipierte Lösung ermöglicht es Maschinenbauunternehmen, den Fernzugriff auf Maschinen und Produktionsanlagen sicher zu steuern – bei voller Transparenz und Kontrolle. Secomea

Bilder: Deutsche Messe AG

HANNOVER MESSE

sorgt für die sichere Zusammenarbeit mit externen Dienstleistern, schützt kritische Anlagen und unterstützt Unternehmen dabei, industrielle Cybersecurity- und Compliance-Anforderungen wie IEC 62443 und NIS-2 zu erfüllen – ohne den Betrieb zu beeinträchtigen oder zusätzliche Komplexität zu schaffen.

Für das Thema Cyber Security auf der HANNOVER MESSE ist der Industrial Security Circus in Halle 26 die zentrale Plattform. Sie bringt führende Expert*innen, innovative Lösungsanbieter und Anwender zusammen, um aktuelle Bedrohungen, praxisnahe Schutzkonzepte und die Zukunft der industriellen Cybersicherheit erlebbar zu machen. In direkter Nähe befindet sich die „5G & Industrial Wireless Arena". Sie ist Europas größte Plattform für drahtlose Kommunikation in der Industrie. Im Mittelpunkt stehen Schlüsseltechnologien wie 5G, 6G und NBIoT.

Insgesamt werden rund 3.000 Aussteller zur HANNOVER MESSE erwartet. Die Unternehmen aus dem Maschinenbau, der Elektro- und Digitalindustrie sowie der Energiewirtschaft präsentieren Lösungen für eine wettbewerbsfähige und nachhaltige Industrie. Die Hauptausstellungsbereiche sind Automatisierung & Digitalisierung, Energie & Industrieinfrastruktur sowie Forschung & Technologietransfer. Die nächste Ausgabe der HANNOVER MESSE wird vom **20. bis zum 24. April 2026** in Hannover ausgerichtet. ■

Sichern Sie sich jetzt Ihr Ticket!

Mehr dazu hier

WAAP: Schutzkonzepte für 2026

API SECURITY UNTER DRUCK

Wachsende API-Landschaften und KI-getriebene Angriffe stellen bestehende Sicherheitsansätze zunehmend vor Herausforderungen. Web Application and API Protection (WAAP) kann Signale bündeln, Reaktionen beschleunigen und Systeme messbar robuster machen. Markus Limbach und Marvin Kroschel erläutern, warum integrierte Schutzansätze 2026 zum Standard werden könnten.

Webanwendungen und Application Programming Interfaces (APIs) bilden das Rückgrat digitaler Dienste und damit eine der größten Angriffsflächen moderner IT-Infrastrukturen. Mit Blick auf das Jahr 2026 gewinnt die Absicherung dort an Bedeutung, wo Interaktionen tatsächlich stattfinden: in integrierten Schutzmechanismen, die Web-, API- und Bot-Signale gemeinsam erfassen und auswerten. Angreifer nutzen künstliche Intelligenz (KI), um Social-Engineering-Kampagnen und Malware schneller zu erstellen und präziser zu steuern. Dadurch steigen Geschwindigkeit und Varianz von Angriffen spürbar. Die eigentliche Herausforderung für Verteidiger entsteht jedoch weniger durch einzelne Schwachstellen als durch das Zusammenspiel vieler kleiner Angriffsvektoren, die erst in ihrer Summe kritisch werden.

APIS ALS VERWUNDBARE SCHNITTSTELLEN

APIs verbinden Mobile Apps mit Backends, orchestrieren Microservices und öffnen Ökosysteme für Partnerunternehmen. Genau diese Offenheit vergrößert zugleich die Angriffsfläche erheblich. In vielen Umgebungen wächst der Bestand an wenig dokumentierten oder veralteten Schnittstellen kontinuierlich an. Parallel dazu testen automatisierte Angriffe systematisch Endpunkte, spielen Rate Limits aus und missbrauchen Business-Logik. Häufig wird das mit Bot Traffic getarnt, der legitime Nutzung nachahmt.

Wer APIs nur begleitend prüft, schützt am Ende weder Daten noch Kernprozesse. Hinzu kommt, dass Distributed-Denial-of-Service-(DDoS)-Wellen immer öfter als Ablenkungsmanöver dienen, während im Hintergrund Datendiebstahl oder der Aufbau von Persistenz stattfindet. Sichtbarkeit und Laufzeitbeobachtung von APIs sollten daher zur ersten Verteidigungslinie werden – doch viele Firmen setzen weiterhin auf fragmentierte Schutzkonzepte.

KLASSISCHE EINZELMAßNAHMEN STOßEN AN GRENZEN

Unternehmen, die Web Application Firewall (WAF), DDoS Mitigation und Bot Abwehr getrennt betreiben, sind auf klar abgegrenzte Angriffsmuster ausgelegt. Moderne Kampagnen erzeugen jedoch häufig viele schwache Signale über mehrere Ebenen. Werden diese Signale nicht zusammengeführt, bleibt die Abfolge dahinter unsichtbar.

Ein vermeintlich harmloser Scrape, also ein automatisierter Datenabruf, auf Endpoint A gehört dann zur gleichen Serie wie fehlschlagende Log-ins auf Endpoint B und Fehlerzuwachs in Endpoint C. Einzelwerkzeuge reagieren zwar, aber die Reaktion trifft zu spät oder zu lokal ein. Daraus folgt, dass Erkennung und Bewertung idealerweise dort stattfinden sollten, wo die Muster zusammenlaufen.

WAAP ALS EVOLUTION

WAAP führt vier Disziplinen in einer Schutz- und Beobachtungsebene zusammen: WAF-Funktionen, spezifische API-Sicherheit mit Inventar, Schema-Validierung und Laufzeitüberwachung, DDoS-Abwehr sowie Bot-Management mit Verhaltensfokus. Der entscheidende Punkt ist die gemeinsame Telemetrie. Erst wenn Requests, Identitätskontext, Volumenanomalien und Sequenzen in einem Analytikpfad landen, lassen sich mehrstufige Angriffe zuverlässig erkennen und automatisch eindämmen.

Für Organisationen ergibt sich damit ein praktischer Nutzen: weniger blinde Flecken, schnellere Eindämmung und eine konsistente Sicht auf Ereignisse, die bislang über mehrere Systeme verteilt waren. Gleichzeitig zwingen strengere Melde- und Nachweisanforderungen Unternehmen dazu, dass diese Beobachtbarkeit nicht optional ist, sondern auditfähig aufgebaut werden muss.

ANGRIFFSGESCHWINDIGKEIT UND VERTEIDIGUNG IN MILLISEKUNDEN

Doch das allein genügt nicht – entscheidend ist auch, wie schnell Systeme auf Bedrohungen reagieren können. IoT Botnetze, elastische Cloud Infrastrukturen und KI-gestützte Musteranpassung führen zu Angriffen, die in Sekunden Fahrt aufnehmen und ihr Verhalten im Millisekundentakt wechseln. Ob ein plötzlicher Lastanstieg eine legitime Kampagne oder der Beginn einer Layer-7-Attacke ist, entscheidet kein statisches Schwellenwertsystem, sondern eine Bewertung der Situation im Kontext.

Modelle, die Historie, Abweichungen und Identitäts-Signale zusammendenken, trennen das hektische Normal von der ruhig getarnten Exfiltration. Genau hier liegt der operative Wert moderner WAAP-Ansätze: Dienste bleiben verfügbar, während pfadbezogene API-Prüfungen Missbrauch gleichzeitig ausbremsen.

Darüber hinaus verstärkt künstliche Intelligenz die Asymmetrie. Angreifer skalieren Social Engineering, E-Mail- und Chat-Imitationen sowie die Ausnutzung vorhandener Werkzeuge. Verteidiger setzen KI ein, um Ereignisse zu korrelieren, Fehlalarme zu reduzieren und Reaktionen teilweise zu automatisieren.

Diese technische Entwicklung trifft zudem auf eine regulatorische Achse: Vorgaben wie das NIST AI Risk Management Framework, ISO/IEC 42001:2023, die OWASP API Security Top 10 oder der EU AI Act verlangen nachvollziehbare Prozesse, schnelle Meldungen und Security by Design. APIs und KI-Schnittstellen sind damit nicht nur ein technisches, sondern auch ein Governance-Thema. Die Verbindung beider Dimensionen kann Entscheidungsprozesse beschleunigen und die Prüffähigkeit erhöhen.

WAS WAAP IN DER PRAXIS LEISTEN KANN

Die theoretischen Vorteile integrierter Schutzansätze lassen sich auf konkrete Anwendungsfelder herunterbrechen. In der Praxis adressiert WAAP fünf zentrale Herausforderungen:

- **Sichtbarkeit zuerst:** Viele Organisationen unterschätzen den Umfang ihrer produktiven API-Oberfläche. Automatisches API-Discovery mit Klassifikation, Versionierung und Deprecation-Überblick wird zur Grundfunktion. Ohne Inventar gibt es keine belastbare Compliance und keine tragfähige Abwehr.
- **Missbrauch der Business-Logik erkennen:** Bei Logikangriffen ist der Input formal korrekt – die Sequenz macht den Angriff. WAAP betrachtet Abläufe und Kontexte: Wer führt in welcher Reihenfolge welche Operationen aus, und passt das zu Rolle, Gerät, Region und Historie? Verhaltenserkennung identifiziert die feine Unstimmigkeit zwischen legitimer Nutzung und strategisch platzierten Requests.
- **Bots abwehren, die Menschen nachahmen:** Wenn Interaktionen nachgeahmt werden, verlieren reine Rate Limits an Wirkung. Moderne Bot Abwehr beobachtet Interaktionsmuster und Reply Strukturen in APIs, statt sich auf Fingerprints zu verlassen. Integriert in WAAP lässt sich die Abwehr risikoadaptiv schalten: blockieren, herausfordern oder drosseln.
- **DDoS als Schirmtarnung entlarven:** Layer-7-Angriffe zielen bewusst auf Ressourcen und Incident-Routinen. Eine modellgestützte Mitigation im gleichen Analysepfad wie die API-Signale verhindert, dass Reaktionsteams zwischen Tickets zerfasern, während die eigentliche Exfiltration läuft.
- **Regulatorik erfüllen:** Sicherheitsmaßnahmen sind 2026 nicht nur technisch zu begründen, sondern dokumentierbar zu machen. Gefordert werden schnelle Meldungen, ein belastbarer Lieferkettenbezug und Security by Design mit klaren Nachweisen. Beobachtbarkeit, Verantwortlichkeiten und Entscheidungswege sollten von Anfang an verankert werden. Wer WAAP als durchgängigen Prozess denkt, verbindet Technik und Governance an denselben Signalen.

ARCHITEKTUR-EMPFEHLUNGEN FÜR DIE UMSETZUNG

Wer WAAP einführen will, steht vor der Frage, wie sich der integrierte Ansatz in bestehende Strukturen einfügt. Vier Prinzipien können dabei als Leitplanken dienen.

Erstens sollten Zugriffe künftig identitäts- und kontextbasiert entschieden werden – nicht mehr am Perimeter. Die Konvergenz von Zugriffsdurchsetzung und Identitätssteuerung reduziert blinde Flecken und erleichtert konsistente Regeln über Web-Apps, APIs und SaaS hinweg. Maschinenidentitäten – von Microservices bis IoT – verdienen dabei denselben Stellenwert wie menschliche Konten.

Zweitens benötigt Automatisierung Augenmaß. Angriffe werden schneller, manuelle Playbooks stoßen an Grenzen. Doch Automatisierung ist nur sinnvoll, wenn sie reversibel bleibt, Richtlinien klar definiert sind und ein Mensch im Entscheidungsprozess verbleibt. Integrierte Signale aus WAAP beschleunigen die Einschätzung, wo Automatik trägt und wo manuelle Prüfung notwendig ist.

Drittens sollte die API-Inventur kein einmaliges Projekt sein, sondern ein Dauerprozess. Startpunkt ist ein vollständiges, lebendes Verzeichnis inklusive Sensitivität, Verantwortlichkeiten, Datenflüssen, Authentifizierungs- und Autorisierungsmodellen sowie Service-Level-Objectives. Schatten-APIs sind aktiv aufzuspüren.

Viertens gilt es, Governance-Strukturen zu verbinden. Meldewege, Lieferkettenbezug und Nachweise sollten mit KI-Governance und Prompt-Sicherheit an KI-Schnittstellen zusammengeführt werden. Technik und Organisation hängen an denselben Ereignissen – und sollten entsprechend verzahnt sein.

Der Einstieg muss nicht komplex sein. Unternehmen können mit einer strukturierten API-Bestandsaufnahme beginnen, Identitätsrichtlinien für Menschen und Maschinen harmonisieren und klar definieren, welche Maßnahmen automatisiert erfolgen und welche geprüft werden müssen. Die Integration von Melde- und Lieferkettenprozessen in bestehende Workflows kann Entscheidungswege bereits kurzfristig verkürzen. ■

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.

Angriffsmodelle und Implikationen für die IT-Sicherheit

CYBERANGRIFFE IM KI-ZEITALTER

Bild: FOTAMA - stock.adobe.com

Künstliche Intelligenz macht Hackerangriffe schneller, gezielter und schwerer erkennbar. Doch dieselbe Technologie stärkt auch die Verteidigung – vorausgesetzt, Unternehmen passen ihre Sicherheitsstrategien an. Unsere Autoren analysieren die neuen Angriffsmethoden und zeigen, wie Organisationen KI-gestützte Abwehrmechanismen aufbauen können.

Die fortschreitende Digitalisierung und der Einsatz von künstlicher Intelligenz (KI) bringen enorme Vorteile mit sich: Prozesse werden effizienter, Informationen sind schneller verfügbar, und es entstehen Geschäftsmodelle, die vor wenigen Jahren noch undenkbar waren. Gleichzeitig vergrößert sich durch diese Entwicklung jedoch auch die Angriffsfläche, der Unternehmen ausgesetzt sind. KI wirkt dabei auf beiden Seiten: Einerseits macht sie Angriffe einfacher, skalierbarer und flexibler. Andererseits eröffnet sie der Cyberabwehr auch völlig neue Möglichkeiten, Bedrohungen schneller zu erkennen und automatisiert zu reagieren.

ÖFFENTLICHE INFORMATIONEN ALS WAFFE

Heutzutage nutzen Angreifer konsequent die riesige Menge öffentlich zugänglicher Informationen. Social-Media-Profile, Unternehmenswebseiten, Handelsregister, Pressemitteilungen, Stellenanzeigen, Entwicklerplattformen wie GitHub oder GitLab liefern zusammengenommen ein detailliertes Bild von Organisationen und Einzelpersonen. KI-gestützte Analysewerkzeuge sammeln diese Daten nicht nur, sondern werten sie auch in kurzer Zeit strukturiert aus, korrelieren und kontextualisieren sie. So entstehen Profile mit sehr hohem Informationsgehalt, die beispielsweise gezielte Social-Engineering-Angriffe erleichtern.

Auf dieser Basis entstehen schwer erkennbare Angriffsmethoden. Phishingmails greifen reale Projekte, interne Bezeichnungen oder aktuelle Kampagnen auf. Anrufer nennen echte Kolleginnen und Kollegen, beziehen sich auf konkrete Termine und geben sich als vertrauenswürdige Personen aus. Gefälschte Log-in-Seiten sind dem Original bis ins Detail nachempfunden. Dadurch wirkt die Kommunikation der Angreifer nicht mehr generisch, sondern wie eine individuelle, sorgfältig vorbereitete Kontaktaufnahme.

KI verstärkt diese Wirkung zusätzlich: Die Texte sind grammatikalisch korrekt, stilistisch stimmig und situativ passgenau formuliert. Selbst in verschiedenen Sprachen lassen sich überzeugende Nachrichten erzeugen, was besonders international agierende Unternehmen betrifft. Einige Chatbots können zudem längere Dialoge führen, Rückfragen stellen, Vertrauen aufbauen und erst spät nach sensiblen Informationen oder Freigaben fragen. Klassische Awareness-Schulungen, die sich ausschließlich auf einfache Erkennungsmerkmale stützen, stoßen hier an ihre Grenzen. Unternehmen müssen sie durch realitätsnähere Trainingsformate ergänzen.

Gleichzeitig setzt auch die Verteidigung zunehmend auf KI. Viele Unternehmen nutzen heute realistische, aber sichere Phishing-Simulationen, die sie mit KI kontinuierlich an aktuelle Kommunikationsmuster anpassen. Die Mitarbeiter erleben in einem geschützten Umfeld, wie überzeugend Angriffe wirken können, und lernen anhand konkreter Beispiele, worauf sie künftig achten müssen. Aus diesen Erfahrungen ergeben sich einfache, alltagstaugliche Verhaltensregeln: Dazu gehört, bei ungewöhnlicher Dringlichkeit innezuhalten, bei sensiblen Anfragen einen zweiten Kommunikationskanal zu nutzen, Absenderadressen und URLs bewusst zu prüfen und Freigabeprozesse konsequent einzuhalten. So wird der Mensch zu einem integralen Bestandteil eines mehrschichtigen Sicherheitskonzepts.

Diese Entwicklung schärft auch das Bewusstsein für den eigenen Umgang mit öffentlichen Informationen. Organisationen stellen sich vermehrt die Frage, ob wirklich interne Informationen wie Strukturen, Tools, Ansprechpartner, Projektkürzel oder Architekturdetails auf der Website oder in sozialen Netzwerken genannt werden müssen. Parallel dazu entstehen neue Sicherheitswerkzeuge, die frei verfügbare Daten aus Verteidigungsperspektive systematisch analysieren. Sie zeigen mögliche Angriffspfade auf, die Außenstehende erkennen könnten, und helfen dabei, exponierte, sicherheitsrelevante Informationen zu identifizieren und zu verbergen, bevor Kriminelle diese missbrauchen können.

AUTOMATISIERTE ANGRIFFSKETTEN UND INTELLIGENTE ABWEHR

Mithilfe von KI lassen sich Angriffsprozesse zunehmend automatisieren und in einzelne, spezialisierte Schritte zerlegen. In solchen Szenarien übernehmen automatisierte, teilweise KI-gestützte Module und KI-Agenten unterschiedliche Aufgaben. Ein Agent scannt etwa kontinuierlich nach Schwachstellen in öffentlich erreichbaren Systemen, ein anderer generiert maßgeschneiderte Phishing-Kampagnen und ein dritter testet systematisch Zugangsdaten oder wertet bekannte Leaks aus. Die Stärke liegt dabei weniger im „perfekten" Einzelangriff als in der schieren Anzahl, Geschwindigkeit und Anpassungsfähigkeit vieler kleiner, kontinuierlicher Versuche.

Für Verteidiger bedeutet dies, dass Sicherheit nicht mehr als punktuelle Aufgabe, sondern als dauerhafter, dynamischer Prozess verstanden werden muss. Gleichzeitig wird auch die Abwehr zunehmend automatisierbar. KI-basierte Systeme überwachen Log-ins, Datenflüsse, Konfigurationen und Netzwerkverkehr nahezu in Echtzeit, erkennen auffällige Muster, priorisieren Alarme und leiten basierend auf dem Schweregrad automatisiert Gegenmaßnahmen ein. Auf diese Weise entsteht ein „digitales Immunsystem", also eine adaptive Kombination aus Überwachung, Analyse und Reaktion.

Auch Angriffe auf Authentifizierungsmechanismen werden durch KI effizienter. Anstelle einfacher Wörterbuchangriffe beziehen Angreifer persönliche Informationen wie Interessen, Hobbys, Lieblingsvereine oder Geburtsdaten mit ein, die sie zuvor aus sozialen Netzwerken oder Datenlecks extrahiert haben. Außerdem können einfach implementierte biometrische Verfahren unter bestimmten Umständen umgangen werden. Mit Deepfake-Technologien lassen sich Stimmen, Gesichter oder Bewegungsmuster in einer Qualität nachbilden, die viele einfache Authentifizierungsmechanismen überlistet. Moderne Systeme kombinieren daher Biometrie mit weiteren Faktoren und Kontextprüfungen, beispielsweise durch starke Passwörter, Hardware-Token, biometrische Verfahren und kontextbasierte Prüfungen.

SCHADSOFTWARE, DIE SICH SELBST ANPASST

Frühere Schadsoftware folgte in der Regel statischen, vorhersehbaren Abläufen. Einmal programmiert, verhielten sich Viren oder Trojaner weitgehend gleich – unabhängig davon, in welcher Umgebung sie ausgeführt wurden. Viele dieser Mechanismen basieren auf bekannten polymorphen und heuristischen Verfahren, die jetzt zunehmend durch KI ergänzt werden. KI-gestützte Schadprogramme arbeiten adaptiv, analysieren ihre Umgebung – beispielsweise das Betriebssystem, aktive Sicherheitslösungen, die Netzwerkarchitektur, Benutzerrechte und laufende Dienste – und entscheiden selbstständig, welche Angriffsstrategie unter den gegebenen Bedingungen am erfolgversprechendsten ist.

Technisch bedeutet dies, dass die Schadsoftware Teile ihres Codes zur Laufzeit neu generiert, kombiniert oder anpasst. Erkennt eine Sicherheitslösung eine Funktion, passen Angreifer den Code in nachfolgenden Varianten gezielt an. So entstehen fortlaufend und mit hoher Geschwindigkeit neue Varianten, die herkömmlichen, rein signaturbasierten Erkennungsverfahren entgehen. Diese Fähigkeit zur Selbstanpassung verschafft Angreifern wertvolle Zeit, bevor ihre Werkzeuge entdeckt, analysiert und blockiert werden können.

Die zugrunde liegenden Prinzipien sind jedoch nicht nur Angreifern vorbehalten, sondern bilden auch die Basis für moderne Verteidigungssysteme. KI-basierte Sicherheitslösungen erkennen nicht nur bekannte Muster, sondern lernen auch kontinuierlich dazu, um das für ein bestimmtes Netzwerk oder eine bestimmte Anwendung typische Verhalten zu erkennen. Weicht ein System plötzlich von diesem Profil ab – beispielsweise durch ungewöhnliche Datenflüsse, verdächtige Prozesse, untypische Zugriffe außerhalb üblicher Zeiten oder aus atypischen Regionen –, kann es einen Alarm auslösen oder automatisch eine Schutzmaßnahme einleiten. So lassen sich auch vollkommen neue oder bisher unbekannte Angriffsmuster frühzeitig identifizieren und unterbrechen, bevor sie größeren Schaden anrichten.

Auch Ransomware-Kampagnen nutzen KI, um die Auswahl, das Timing und die Tarnung von Angriffen zu optimieren. In einigen beobachteten Fällen werden mithilfe von KI gezielt wertvolle Daten und Systeme ausgewählt und Angriffe zu taktisch besonders günstigen Zeitpunkten, etwa kurz vor Quartalsabschlüssen oder Produktvorstellungen, durchgeführt. Dadurch kann das potenzielle Schadensausmaß erheblich steigen. Gleichzeitig entwickeln Verteidiger KI-gestützte Gegenmaßnahmen. Systeme erkennen typische Frühindikatoren wie massenhafte Dateiänderungen, plötzliche Verschlüsselungsversuche, Anomalien bei Servicekonten oder sprunghaft ansteigende Fehlzugriffe. In Verbindung mit klar definierten, teilweise automatisierten Notfallplänen können betroffene Systeme isoliert, Zugänge gesperrt und Datenströme eingefroren werden – im Idealfall, bevor ein Angreifer seine Ziele vollständig erreicht hat.

DEEPFAKES UND DESINFORMATION

Deepfakes, also künstlich erzeugte oder manipulierte Stimmen, Bilder und Videos, ermöglichen gezielte Täuschungen in einem Ausmaß, das klassische Betrugsmethoden bei Weitem übertrifft. Ein vermeintlicher Videoanruf vom „Chef", ein angeblicher Bankmitarbeiter oder ein fingiertes Interview mit einer Führungskraft kann heute so realistisch wirken, dass selbst erfahrene Mitarbeiter ins Zweifeln geraten. Gerade in Kombination mit bereits bekannten Daten über interne Strukturen oder laufende Projekte entstehen äußerst glaubwürdige Szenarien für Social Engineering.

Doch auch hier wächst das Gegengewicht. KI-basierte Erkennungssysteme analysieren Audio- und Videodaten auf kleinste Anomalien wie fehlerhafte Bildartefakte, untypische Lippensynchronität, unnatürliche Tonfrequenzen oder widersprüchliche Metadaten. Erkennungssysteme können so wertvolle Hinweise liefern, auch wenn sie zum jetzigen Zeitpunkt noch kein verlässlicher Alleinmechanismus sind.

Parallel dazu arbeiten Medien, Plattformbetreiber und Sicherheitsanbieter an Mechanismen zur Kennzeichnung authentischer Inhalte, etwa durch digitale Signaturen oder Wasserzeichen. In vielen Fällen bleibt der informierte Mensch die entscheidende Kontroll- und Sicherheitsinstanz: Wer das Phänomen kennt, typische Einsatzszenarien versteht und sich an einfache Prüfmechanismen hält, lässt sich deutlich schwerer täuschen.

KI ALS SICHERHEITSWERKZEUG

So bedrohlich viele dieser Entwicklungen auf den ersten Blick wirken, dieselbe Technologie stärkt zugleich die Cyberabwehr. KI kann enorme Datenmengen aus unterschiedlichen Quellen analysieren, beispielsweise Logdaten, Netzwerkverkehr, Endpoint-Telemetrie, Cloud-Konfigurationen oder Identitäts- und Zugriffsprotokolle, und dabei Muster erkennen, die menschlichen Analysten aufgrund der Menge und Geschwindigkeit allein entgehen würden. So kann KI dabei helfen, Alarme besser zu priorisieren. Bei geeigneter Konfiguration kann dies die Anzahl irrelevanter Meldungen reduzieren und die Effizienz sowie den Fokus menschlicher Sicherheitsanalysten steigern.

Darüber hinaus vereinfacht KI die Kommunikation über Risiken innerhalb von Organisationen. Komplexe Angriffsszenarien, Abhängigkeiten und Auswirkungen lassen sich verständlich visualisieren und in einem für das Management oder die Fachabteilungen passenden Detaillierungsgrad zusammenfassen. Bei Bedarf können sie interaktiv erläutert werden. Mitarbeiter erhalten kontextsensitive Hinweise und verständliche Empfehlungen, etwa direkt in den von ihnen genutzten Anwendungen. KI kann zwar keine grundlegenden Sicherheitsstrukturen ersetzen, jedoch fehlende Kapazitäten teilweise kompensieren. Besonders kleinere und mittlere Organisationen, in denen spezialisierte Sicherheitsteams oft fehlen, können davon profitieren.

EIN REALISTISCHER, ABER ZUVERSICHTLICHER BLICK NACH VORN

KI-gestützte Angriffe sind längst Realität. Sie sind gezielter, schneller, skalierbarer und oft schwerer zu erkennen als traditionelle Angriffe. Der Grund: Sie ahmen menschliches Verhalten überzeugend nach und können Sicherheitsmechanismen adaptiv umgehen. Gleichzeitig wird jedoch auch die Cyberabwehr intelligenter, vernetzter und automatisierter.

Für Unternehmen und Organisationen bedeutet dies, ihre Sicherheitsstrategien ganzheitlich weiterzuentwickeln. Es gilt, in moderne Sicherheitsarchitekturen zu investieren und eine Kultur zu schaffen, die Aufmerksamkeit, Nachfragen und das Melden von Sicherheitsvorfällen ausdrücklich fördert. Regulatorische und organisatorische Rahmenbedingungen spielen eine zentrale Rolle, damit dieser Wandel schnell genug abläuft.

Unternehmen und Organisationen, die heute in moderne Multi-Faktor-Authentifizierung, aktuelle und gehärtete Systeme, KI-basierte Sicherheitslösungen sowie kontinuierliche Aufklärung und Schulungen investieren, verschaffen sich in der neuen Bedrohungslage eine gute Ausgangsposition. Richtig eingesetzt werden diese Maßnahmen und KI-gestützte Sicherheitslösungen zu einem zentralen Baustein für widerstandsfähige digitale Infrastrukturen. ■

KEVIN EULER
ist Associated Partner bei MHP.

BENEDIKT BAUER
ist Consultant bei MHP.

Neue Protokolle unterlaufen den AI Act

DIE AGENTEN-LÜCKE

Der EU AI Act reguliert KI-Modelle anhand ihrer Trainingsrechenleistung – doch autonome KI-Agenten hebeln diesen Ansatz aus. Über Protokolle wie Anthropics MCP oder Googles A2A vernetzen sich kleine Modelle zu mächtigen Systemen, die einzeln unter den Schwellenwerten bleiben, gemeinsam aber sensible Daten verarbeiten und eigenständig handeln. Welche Sicherheitsrisiken daraus entstehen und wie Unternehmen ihre Agenten-Architekturen trotzdem absichern können, zeigt eine Analyse der aktuellen Frameworks von ENISA und NIST.

Der EU AI Act setzt bei der Definition von systemischen Risiken primär auf hohe Schwellenwerte beim Modelltraining. Der Trend zu Agentic-AI untergräbt diesen Ansatz jedoch grundlegend: Durch die Nutzung von Protokollen wie dem Model Context Protocol (MCP) und Agent-to-Agent (A2A) können vergleichsweise kleine Modelle Prozessketten bilden, bei denen jedes einzelne Element unter den kritischen Grenzwerten bleibt, während das verkettete Gesamtsystem diese um ein Vielfaches überschreitet. Das primäre Ziel des AI Acts, Anbieter großer generativer KI-Modelle zu mehr Sicherheit zu drängen, lässt sich so unterlaufen.

Dabei operieren Agentic-AI-Systeme in der Praxis oftmals mit schutzwürdigen Daten, beispielsweise wenn ein KI-Agent im Auftrag eines Anwenders nach einem Produkt sucht, dieses in einem Onlineshop bestellt und dann mit einer Kreditkarte bezahlt. Für eine solche Anwendung greifen die beteiligten Agenten auf sensible Informationen zu, die sie untereinander austauschen und weiterverarbeiten.

Durch autonome Handlungsfähigkeit wie das eigenständige Ausführen von Code kann ein solches System aus verketteten KI-Agenten einen weit größeren Schaden anrichten als ein isoliertes, riesiges Modell. Es stellt sich daher die Frage, ob die Agenten-Architektur selbst als GPAI mit systemischem Risiko eingestuft werden muss, und zwar auch dann, wenn nur die einzelnen KI-Modell-Komponenten des Systems die vom EU AI Act gesetzten Schwellenwerte unterschreiten.

Die EU definiert im AI Act KI-Modelle mit allgemeinem Verwendungszweck (General Purpose AI, GPAI) über die Rechenleistung des Modelltrainings. Darunter fällt jedes Modell, das mit mehr als 10^{23} FLOPS trainiert wurde. FLOP steht für Gleitkommaoperationen; im Kontext des AI Acts bezeichnet der Wert die kumulative Rechenleistung während des Trainings.

Das Modell muss in der Lage sein, Sprach-, Text-zu-Bild- oder Text-zu-Video-Ausgaben zu erzeugen. Für Anbieter solcher GPAI-Modelle gelten umfangreiche Pflichten über den gesamten Lebenszyklus hinweg – von der Modellentwicklung und Schulung über die Veröffentlichung bis hin zu späteren Updates. Die Umsetzung dieser Vorgaben muss per Dokumentation nachgewiesen werden. Dazu gehören eine Zusammenfassung der verwendeten Trainingsdaten und die Einhaltung der Regeln zum Urheberrecht im Modell.

Bei besonders rechenintensiven Modellen, die mit mehr als 10^{25} FLOPS trainiert wurden, gilt das Modell als GPAI mit systemischem Risiko. Das bedeutet zusätzliche Verpflichtungen für den Anbieter. Er muss sein Modell immer und überall daraufhin prüfen, ob es Risiken gibt. Dabei geht es um Technik, aber auch um Ethik und Soziales. Cybersicherheitsmaßnahmen müssen über den gesamten Lebenszyklus ergriffen und umgesetzt werden. Zum Beispiel ist vorgeschrieben, Vorfälle im Internet zu bewerten und Schwachstellen zu schließen. Schwere Cybersicherheitsvorfälle sind an die zuständigen nationalen Behörden zu melden, in deren Land die betroffenen Systeme angeboten werden.

ENISA-FRAMEWORK STÖßT BEI AGENTEN AN GRENZEN

Für die praktische Umsetzung der AI-Act-Anforderungen hat die europäische Behörde für Cybersicherheit (ENISA) das Multilayer Framework for Good Cybersecurity Practice (FAICP) entwickelt. Der Leitfaden liefert konkrete Anleitungen zur Absicherung von GPAI-Systemen, -Vorgängen und -Prozessen und unterscheidet dabei drei Ebenen: allgemeine Cybersicherheit, KI-spezifische Sicherheit und branchenspezifische Anforderungen (siehe Kasten).

Doch auch wer mit kleineren KI-Agenten-Systemen unterhalb der GPAI-Schwellenwerte arbeitet, sollte aus Gründen der System- und Anwendungssicherheit die FAICP-Prinzipien anwenden. Die Integration von Agentic-AI-Protokollen wie MCP und A2A in die Infrastruktur eines Unternehmens betrifft alle Ebenen des ENISA-FAICP-Frameworks.

Auf der Grundlagenebene etwa fungieren MCP-Server als neue Netzwerkendpunkte, was eine strikte Umsetzung des Zero-Trust-Prinzips erfordert. Da Agenten über diese Protokolle oft direkten Zugriff auf Dateisysteme erhalten, müssen Zugriffsrechte deutlich granularer definiert werden, als es in klassischen IT-Umgebungen der Fall ist.

Im Bereich der KI-Sicherheit auf der zweiten Ebene entstehen durch MCP und A2A neue Angriffsvektoren wie die Indirect Prompt Injection. Dabei platziert ein Angreifer eine manipulierte

DIE DREI EBENEN DER KI-SICHERHEIT NACH ENISA

Ebene I – Grundlagen der Cybersicherheit: *Hier wird das technische Fundament zur Absicherung geschaffen. Dazu zählen zum Beispiel: Register über Sicherheits-Assets der Informations- und Telekommunikationstechnik (ITK), Konzepte über Identitäten und Zugriffsrechte nach dem Zero-Trust-Prinzip, ein Schwachstellen-Management, bei dem das Risiko gewichtet wird, Prozesse für Updates und Patching sowie Prozesse für die Beantwortung von Incidents.*

Ebene II – Sicherheit für KI: *Hier geht es um Bedrohungen, die erst durch KI in ITK-Systemen entstehen. Dazu gehören zum Beispiel kryptografisch abgesicherte Datenlieferketten, Detektoren gegen Datenvergiftung, Tests zum Erkennen von Angriffen und Mechanismen für vertrauliche Inferenz. Es wird auch empfohlen, Ausgabe- und Prompt-Filter zu benutzen. Diese kennzeichnen riskante Ergebnisse.*

Ebene III – Sicherheit in bestimmten Bereichen: *Hier werden Sicherheitsprinzipien auf Bereiche übertragen, in denen es unmittelbare Risiken für Menschen, Gesundheit oder Infrastruktur gibt. Im Gesundheitswesen empfiehlt das FAICP etwa Protokolle, die man überprüfen kann, und Pläne für Notfälle. Der Finanzsektor soll sichere Nachhandels-Logs führen und Entscheidungen nachvollziehbar machen. In Operational-Technology-(OT)-Umgebungen sind Notfallstrategien, physische Abschaltungen und Regeln für die Anlagen aufgeführt.*

Abbildung 1: Schichtenmodell im FAICP (Quelle: ENISA, „Multilayer Framework for Good Cybersecurity Practices for AI", S. 6)

Datei in einem Repository, die der Agent über das Protokoll ausliest. Versteckte Befehle in der Datei können den Agenten dazu verleiten, vertrauliche Daten an externe Systeme weiterzugeben. Zur Abwehr sind Netzwerkfilter nötig, die die Agentenkommunikation überwachen und verdächtige Muster blockieren.

Auf der dritten Ebene, den sektorspezifischen Anforderungen, wird es besonders heikel. In kritischen Infrastrukturen wie dem Finanzwesen oder der Energieversorgung könnten KI-Agenten eigenständig Transaktionen auslösen. Die FAICP fordert hier nachvollziehbare Entscheidungen, was bei autonomen Agentenketten eine technische Herkulesaufgabe ist.

Hinzu kommt ein rechtliches Problem: Wer haftet, wenn etwas schiefgeht? Durch verkettete KI-Agenten verschwimmen die Verantwortlichkeiten zwischen Modell-Anbieter und System-Integrator. Koppelt ein Unternehmen einen Agenten an interne Datenbanken und dieser verstößt aufgrund einer Fehlfunktion gegen den AI Act oder Datenschutzregeln, ist unklar, wer verantwortlich ist. Der Integrator kontrolliert schließlich die Agenten-Logik und die Datenanbindung – nicht der Modell-Anbieter.

Dieses neue Zusammenspiel durch KI-Agenten macht deutlich, dass eine rein hardwarebasierte Regulierung durch den EU AI Act zu kurz greift. Für Unternehmen bedeutet dies, dass die Cybersicherheit von einer reaktiven Überprüfung zu einer aktiven Sicherheit bereits während der Designphase des KI-Agenten-Systems übergehen muss. Wer Agenten einsetzt, muss nicht nur das verwendete Modell absichern, sondern den gesamten Aktionsraum, den die MCP und A2A-Protokolle dem Agenten eröffnen. Die FAICP-Leitlinien der ENISA bieten hierfür zwar eine Struktur, müssen aber dringend um spezifische Standards für autonome Agenten-Schnittstellen ergänzt werden, um den Anforderungen der Cybersicherheit in der Praxis zu genügen.

NIST-FRAMEWORK ALS LEITPLANKE FÜR AGENTEN-SICHERHEIT

Sichere Agentensysteme entstehen nicht im Alleingang: KI-Entwickler beherrschen die Modelle, kennen aber oft nicht die klassische IT-Sicherheit. Auch ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001, das viele Unternehmen bereits nutzen, deckt KI-spezifische Risiken nicht ab. Hier hilft das Cyber-Security-Framework des National Institute of Standards and Technology (NIST) als Ergänzung (siehe Abbildung 2).

Im Gegensatz zu klassischen Softwareanwendungen zeichnen sich KI-Agenten durch ein hohes Maß an Autonomie und die Fähigkeit aus, eigenständig Entscheidungen in dynamischen Umgebungen zu treffen, was die Angriffsfläche und die Komplexität der Risiken erhöht. Ein fundierter Ansatz beginnt daher bereits in der Vorbereitungsphase mit der Definition des Kontextes, wobei die spezifischen Ziele des Agenten sowie die potenziellen Auswirkungen auf die Organisation und externe Stakeholder präzise umrissen werden müssen.

Im Zentrum der Methodik nach NIST steht die Identifikation von Risiken, die bei KI-Agenten über herkömmliche Cybersicherheitsbedrohungen hinausgehen. Hier treten besagte Phänomene wie Prompt Injection, Data Poisoning oder das Problem der Modell-Halluzinationen in den Vordergrund, die das Verhalten des Agenten unvorhersehbar machen können.

Ein Agent, der Zugriff auf interne Datenbanken oder E-Mail-Systeme hat, könnte durch

Abbildung 2: Management von IT-Risiken nach NIST gilt auch für KI-Agenten-Systeme. (Quelle: NIST)

geschickte Manipulation Dritter dazu verleitet werden, vertrauliche Informationen preiszugeben oder schadhafte Aktionen auszuführen. Das NIST-Modell verlangt hier eine kontinuierliche Überwachung, da sich das Risikoprofil eines Agenten durch permanentes Lernen oder sich ändernde Datenströme im laufenden Betrieb verschieben kann. Die Bewertung dieser Risiken muss daher dynamisch erfolgen und darf sich keinesfalls auf eine einmalige Prüfung vor dem Rollout beschränken.

Die Umsetzung von Schutzmaßnahmen erfordert darüber hinaus eine enge Verzahnung von technischen Kontrollen und organisatorischen Leitplanken. Hierzu zählen die Implementierung strikter Zugriffskontrollen und die Überprüfung der Output-Integrität durch sekundäre Validierungsschichten bei den KI-Agenten-Protokollen.

Ein wesentlicher Aspekt nach NIST ist die Förderung der Vertrauenswürdigkeit, was im Kontext von KI-Agenten vor allem Erklärbarkeit und Transparenz bedeutet. Entwickler müssen sicherstellen, dass die Entscheidungspfade des Agenten nachvollziehbar bleiben, um im Fall einer Fehlentscheidung eine schnelle Ursachenanalyse und Korrektur zu ermöglichen. Dies korrespondiert mit der NIST-Säule der Verantwortlichkeit, die klare Strukturen für die menschliche Aufsicht (Human-in-the-Loop) fordert, um die Autonomie des Systems dort zu begrenzen, wo kritische Geschäftsentscheidungen getroffen oder ethische Grenzbereiche berührt werden.

GUARDRAILING UND MONITORING IM BETRIEB

Um die Integrität und Sicherheit von KI-Agenten zu gewährleisten, müssen die Kontrollmechanismen für die Überprüfung von Protokollen weit über einfache Filterfunktionen hinausgehen. Im Rahmen des NIST-Ansatzes kann dazu eine mehrstufige Validierungsarchitektur implementiert werden, die als Korrektiv zwischen dem autonomen Agenten und der Außenwelt fungiert.

Ein primärer technischer Kontrollmechanismus ist das sogenannte Guardrailing. Dabei untersuchen spezialisierte Sprachmodelle oder regelbasierte Systeme die Protokollinhalte in Echtzeit auf Richtlinienverstöße, Halluzinationen oder die Preisgabe von sensiblen Daten. Diese Instanz fungiert als Sicherheitsschleuse, die potenziell schädliche Aktionen von KI-Agenten blockiert, bevor sie eine Wirkung entfalten können.

Ergänzend dazu spielt die semantische Konsistenzprüfung eine entscheidende Rolle. Hierbei wird das Verhalten von KI-Agenten gegen eine verifizierte Wissensbasis geprüft, um sicherzustellen, dass die vorgeschlagene Handlung logisch und faktisch fundiert ist. In hochkritischen Umgebungen sieht das NIST-Framework zudem die Einbindung von deterministischen Validierern vor. Diese prüfen beispielsweise bei Agenten, die Anweisungen und Prompts erzeugen oder Datenbankabfragen generieren, ob die Syntax korrekt ist und ob deren Ausführung innerhalb definierter Berechtigungsgrenzen bleibt, etwa durch den Einsatz von Sandbox-Umgebungen.

Ein weiterer wesentlicher Aspekt ist das Monitoring des Verhaltens von KI-Agenten im Betrieb. Dabei wird kontinuierlich abgeglichen, ob die vom Agenten gewählten Zwischenschritte noch mit der ursprünglichen Zielvorgabe des Nutzers übereinstimmen. Da Agenten oft über mehrere Stufen hinweg planen, besteht das Risiko des sogenannten Driftens, bei dem sich das System durch eine Kette von Fehlinterpretationen von den gewünschten Eigenschaften entfernt.

Durch die Implementierung von Checkpoints, die eine explizite Bestätigung durch einen menschlichen Operator (Human-in-the-Loop) bei Überschreiten bestimmter Risikoschwellen erfordern, kann eine notwendige Absicherung zur Intervention sichergestellt werden. Dieser hybride Ansatz aus automatisierter Echtzeit-Prüfung und strategischer menschlicher Aufsicht ermöglicht es, die Effizienzvorteile autonomer Agenten zu nutzen, ohne die Kontrolle über die Systemsicherheit einzubüßen.

FAZIT

Der Übergang von klassischen IT-Prozessen zu dynamischen KI-Prozessen mit autonomen KI-Agenten erfordert eine ganzheitliche Betrachtung von KI-Sicherheit und IT-Sicherheit. Ein isolierter Fokus auf die KI-Modellentwicklung und GPAI-Modelle wie Large Language Models (LLMs) reicht nicht aus. Ein resilientes KI-Agenten-System zeichnet sich dadurch aus, dass es Sicherheitsgrenzen nicht nur erkennt, sondern innerhalb gesetzter Leitplanken proaktiv agiert und nicht ausbricht.

Die Frameworks von ENISA (FAICP) und NIST bieten dafür eine Struktur – auch wenn das Verhalten autonomer Systeme nie vollständig vorhersehbar sein wird. Letztlich ist der sichere Einsatz von KI-Agenten kein rein technisches Problem, sondern eine Frage der organisatorischen Reife. Organisationen, die Transparenz, Verantwortlichkeit und kontinuierliches Monitoring tief in ihrer Unternehmenskultur verankern, können das volle Potenzial autonomer Systeme ausschöpfen, ohne untragbare Risiken einzugehen. ■

MIRKO ROSS
ist CEO der asvin GmbH.

Warum der jährliche Pentest nicht mehr ausreicht

ECHTZEIT STATT MOMENTAUFNAHME

Penetrationstests galten lange Zeit als jährliche Routine und wurden in der Praxis häufig als rein formale Compliance-Übung verstanden. Doch in Zeiten von DORA, NIS-2 und KI-gestützten Angriffen reicht die bloße Momentaufnahme nicht mehr aus. Ein Plädoyer für den Wechsel von statischer Prüfung zu kontinuierlicher Resilienz.

Der klassische Penetrationstest hat ein grundlegendes Problem: Zum Zeitpunkt der Berichtsfertigstellung bildet er oft nur noch eine begrenzte Momentaufnahme ab. Angreifer finden heute teils binnen Stunden neue Wege in Systeme, sobald sie eine Sicherheitslücke erkannt haben. Ein jährlicher Check stößt unter diesen Bedingungen an seine Grenzen. Getrieben durch neue regulatorische Anforderungen ist daher ein Umdenken erforderlich: weg von der punktuellen Momentaufnahme, hin zu einer kontinuierlichen Überprüfungsmethodik.

Viele Unternehmen verlassen sich dennoch weiterhin auf den jährlichen Penetrationstest als zentralen Sicherheitsnachweis. Traditionell lag der Fokus dabei stark auf der Technik: Server, Netzwerke und Firewalls wurden geprüft. Doch die Angriffsziele haben sich verschoben. Die moderne IT-Landschaft verändert sich ständig: Durch Cloud-Nutzung und schnelle Software-Updates (CI/CD) kann die Infrastruktur bereits nach kurzer Zeit deutlich anders aussehen als zum Testzeitpunkt. Ein Test, der nur einmal im Jahr stattfindet, lässt den Angreifern unter Umständen längere Zeiträume, um unentdeckte Schwachstellen auszunutzen.

Ein Beispiel dafür ist ein Vorfall aus dem Jahr 2023. Dabei nutzten Angreifer eine Schwachstelle in einer weitverbreiteten Dateiaustausch-Software aus. Zwar hätte auch ein kontinuierlicher

Bild: Visi Hue - stock.adobe.com

Test diesen Zero-Day-Exploit in der Fremdsoftware nicht per se verhindert, doch er ändert die Reaktionsfähigkeit drastisch: Anstatt erst beim nächsten Audit zu prüfen, zeigt eine kontinuierliche Überwachung sofort, wo sich die verwundbare Komponente im eigenen Netz befindet. Diese Transparenz kann die Reaktionszeiten verkürzen und potenzielle Schäden begrenzen.

DORA UND NIS-2 ERHÖHEN DEN DRUCK AUF UNTERNEHMEN

Mit dem Digital Operational Resilience Act (DORA) für die Finanzbranche und der NIS-2-Richtlinie für wesentliche und wichtige Einrichtungen, deren Ausfall erhebliche Auswirkungen auf Wirtschaft oder Gesellschaft haben kann, hat der Gesetzgeber die Anforderungen deutlich verschärft. Es reicht nicht mehr, ein Sicherheitskonzept nur auf dem Papier zu haben – die Widerstandsfähigkeit muss im operativen Alltag bewiesen werden.

DORA fordert von Banken und Versicherungen ein Testprogramm, das sich am tatsächlichen Risiko orientiert. Das schafft Budget-Effizienz durch Differenzierung: Für weniger bedrohte Assets wie eine statische Marketing-Webseite, die nicht von der Bank selbst betrieben wird und isoliert von anderen Assets agiert, genügen einfache, automatisierte Scans. Aber für das Herzstück der Bank – etwa den Zahlungsverkehr – sieht der Gesetzgeber fortgeschrittene Methoden wie Threat-Led Penetration Tests (TLPT) vor.

Viele Institute haben sich deshalb vom pauschalen Ansatz verabschiedet und priorisieren ihre Maßnahmen risikobasiert: Hochriskante Bereiche wie Kunden-Apps werden quasi permanent überwacht. Automatisierte Systeme suchen laufend nach Standardlücken, während sich die menschlichen Experten auf die komplexen, logischen Schwachstellen konzentrieren.

KI ALS HELFER UND RISIKO ZUGLEICH

Künstliche Intelligenz (KI) spielt in diesem neuen Ansatz eine Doppelrolle. Einerseits kann sie die Verteidigung unterstützen, indem sie beispielsweise die Identifikation potenzieller Einfallstore automatisiert oder Angriffsszenarien simuliert, die früher einen deutlich höheren manuellen Aufwand erforderten.

Gleichzeitig bleibt der Mensch unverzichtbar – besonders vor dem Hintergrund noch nicht vollständig umgesetzter Regulierung wie des EU AI Act. Fachliche Expertise ist erforderlich, um Ergebnisse einzuordnen und zu bewerten, welche Schwachstellen tatsächlich geschäftskritisch sind. Zudem schafft KI neue Risiken: Wenn Unternehmen ihre KI-Anwendungen unzureichend absichern, können Angreifer diese etwa durch Prompt Injection manipulieren. Hier greifen klassische Scanner zu kurz. Es braucht neue „Adversarial Testing"-Ansätze, bei denen spezialisierte KI-Modelle gezielt gegen die eigenen Systeme antreten, um diese logischen Lücken aufzudecken.

CTEM ALS UMFASSENDER SICHERHEITSANSATZ

Vor diesem Hintergrund gewinnt das Continuous Threat Exposure Management (CTEM) an Bedeutung. CTEM ist dabei kein Ersatz für den Penetrationstest, sondern eine konzeptionelle Weiterentwicklung. Es fungiert als strategische Klammer, die verschiedene Maßnahmen wie Pentests, Schwachstellen-Scans und Threat Intelligence bündelt und priorisiert. Während der Pentest die technische Validierung liefert, sorgt CTEM für den kontinuierlichen Prozess dahinter. Vereinfacht gesagt: Der Weg führt vom isolierten, statischen Bericht zu einem integrierten Echtzeit-Dashboard für Entscheidungsträger.

Auch aus Compliance-Sicht bedeutet der Abschied vom jährlichen Report keinen Verlust an Nachweisfähigkeit. Moderne Dashboards können relevante Informationen für Audits fortlaufend und strukturiert bereitstellen. Werden neue Angriffsmethoden bekannt, kann geprüft werden, ob eigene Systeme betroffen sind. Sicherheit entwickelt sich damit zunehmend von einer reinen Pflichtaufgabe zu einem Faktor für Vertrauen und Stabilität in der Zusammenarbeit mit Kunden und Partnern.

VOM REAGIEREN ZUM AGIEREN

Der Wandel zur kontinuierlichen Prüfung ist heute ein wesentlicher Bestandteil eines zeitgemäßen Risikomanagements. Entscheidend ist dabei der strategische Dreiklang aus Transparenz, Automatisierung und Business-Bezug. Nur wer seine kritischen Assets kennt, kann sie effektiv schützen. Gleichzeitig sollte die Routine automatisiert werden, damit Expertenkapazitäten für komplexe Bedrohungsszenarien frei werden.

Zentral ist zudem, technische Erkenntnisse zeitnah in geschäftliche Risikobewertungen zu übersetzen. Unternehmen, die sich ausschließlich auf periodische Sicherheitsberichte verlassen, laufen Gefahr, zu spät auf neue Bedrohungen zu reagieren. Dynamische, risikobasierte Testzyklen leisten daher einen wichtigen Beitrag zur nachhaltigen Stärkung der digitalen Resilienz. ■

CHRISTIAN NERN
ist Partner und Head of Security bei KPMG im Bereich Financial Services in München. Vor seiner Tätigkeit bei KPMG hat der Diplom-Kaufmann 25 Jahre lang in exponierten Leadership-Positionen verschiedener Bereiche in der IT-Industrie gearbeitet.

JULIAN KRAUTWALD
ist Practice Lead Detection & Response bei KPMG im Bereich Financial Services. Er ist Experte auf dem Gebiet digitale Transformation des Financial-Services-Sektors mit dem Fokus auf die operative Cyber-Sicherheit.

IT-Asset-Management für Cloud- und KI-Umgebungen

FÜNF ANSÄTZE FÜR ZUKUNFTSFÄHIGES ITAM

Cloud, künstliche Intelligenz (KI) und neue Regulierungen verändern die Spielregeln für IT-Asset-Management (ITAM). Die aktuelle Deloitte-Studie zeigt: ITAM muss vom reaktiven Kostenkontrolleur zum strategischen Steuerungsinstrument werden. Fünf zentrale Handlungsfelder helfen, Transparenz zu schaffen, Risiken zu senken und Innovation verantwortungsvoll zu ermöglichen.

Cloud-Dienste, Software-as-a-Service (SaaS) und KI-Anwendungen wachsen rasant, während regulatorische Anforderungen wie der Digital Operational Resilience Act (DORA), die NIS-2-Richtlinie und der EU AI Act die Komplexität für Unternehmen erhöhen. ITAM ist längst kein Backoffice-Thema mehr: Es beeinflusst Kosten, Compliance, Cyberresilienz und Nachhaltigkeit. Die Ergebnisse des Deloitte Global ITAM Survey 2025 verdeutlichen diese Entwicklung.

Wer ITAM weiterhin als rein operative Funktion betrachtet, riskiert erhebliche Folgen: Kostenexplosionen durch unzureichend kontrollierte Cloud- und SaaS-Nutzung, Compliance-Verstöße mit hohen Strafzahlungen und Reputationsschäden, Cybersecurity-Lücken, die Angriffsflächen vergrößern, sowie verpasste Nachhaltigkeitsziele, die zunehmend regulatorisch und reputationsrelevant sind. Führungsteams sollten ITAM daher als strategisches „Betriebssystem" ihrer Technologieentscheidungen betrachten.

1. GRUNDLAGEN FÜR CLOUD- UND KI-FÄHIGES ITAM SCHAFFEN

In hybriden und Multi-Cloud-Umgebungen entstehen Assets als flüchtige Ressourcen, die sich dynamisch skalieren und wieder auflösen. Traditionelle ITAM-Modelle, die auf statische Inventarlisten und einmalige Erfassungen setzen, sind dafür nicht gemacht. Die Studie zeigt, dass mangelnde Transparenz über Cloud-Ressourcen und elastische Nutzungsmuster zu den größten Herausforderungen zählen.

Einige Unternehmen reagieren darauf mit einem stärker integrierten ITAM-Ansatz: Sie konsolidieren Asset-Daten aus Cloud, On-Premises und Development-and-Operations-(DevOps)-Pipelines, definieren die Verantwortung (Ownership) klar und verbinden ITAM mit Finanzsteuerung (Financial Operations (FinOps) in der Cloud), um Kosten und Governance zusammenzuführen.

Operativ bedeutet das: Echtzeit-Telemetrie für Computer-, Speicher- und Netzwerkressourcen, Lifecycle-Modelle für kurzlebige Dienste und präzise Klassifizierungen für KI-Workloads. Die Integration cloudnativer Werkzeuge, beispielsweise mittels Infrastructure-as-Code, Daten aus Observability-Plattformen und Mapping in Service-Katalogen, ermöglicht eine kontinuierliche Aktualität und Einordnung der Daten.

Diese operative Umsetzung bringt jedoch mehrere strukturelle Probleme mit sich:

- In vielen Unternehmen fehlen einheitliche Datenmodelle, die transiente Cloud-Objekte neben klassischen Hardware- und Software-Assets gleichwertig abbilden.
- Die Verantwortlichkeiten sind oft verteilt: Projektteams, Fachbereiche und zentrale IT besitzen jeweils Teilansichten, häufig ohne verbindliche Governance.
- Die finanzielle Steuerung ist komplex: Verbrauchsorientierte Preismodelle, Bündelangebote und KI-spezifische Lizenzmetriken erschweren die Prognose und Abrechnung.

Um diesen Herausforderungen zu begegnen, bauen viele Unternehmen zentrale Datenplattformen auf – beispielsweise Data Warehouses –, die kontinuierlich technische Daten über Software und Hardware im Betrieb und in Nutzung, kommerzielle Daten zu Softwareverträgen, Nutzungsrechten und Lizenzmengen sowie Schwachstellen-, End-of-Life- und Support-Daten zusammenführen.

Auf Basis dieses konsolidierten Datenpools lassen sich vielfältige Fragestellungen aus den Bereichen Compliance, FinOps, Procurement, Enterprise Architecture und Cyber Security beantworten – KI-gestützte Analysen unterstützen gleichzeitig proaktives Handeln.

Die Kopplung mit DevOps erhöht die Datenaktualität erheblich: Jede Bereitstellung wird automatisch in Konfigurations- und Asset-Datensätzen erfasst, jede Stilllegung bereinigt den Bestand. Entscheidend ist, dass IT-Asset-Management dabei nicht als Kontrollhürde, sondern als Unterstützung einer schnellen und zugleich verantwortungsvollen Bereitstellung wirkt.

2. SAAS-GOVERNANCE MODERNISIEREN

Eine dezentrale Beschaffung von SaaS führt zu Schatten-IT, fragmentierten Vertragslandschaften und einer unübersichtlichen Nutzung im Unternehmen. Fehlende Transparenz erschwert die Kostenoptimierung und erhöht Compliance-Risiken, beispielsweise durch unzulässige Datenübertragungen oder Nichtbeachtung lizenzrechtlicher Einschränkungen.

Ein reifer Ansatz setzt dagegen stärker auf nachvollziehbare Prozesse und eine klare Rollenverteilung. Unternehmen nutzen zunehmend zentral gesteuerte SaaS-Management-Plattformen, definieren einheitliche Genehmigungsverfahren und verzahnen ITAM enger mit Identitäts- und Zugriffsmanagement. Praktisch bedeutet das die systematische Erkennung aller eingesetzten Anwendungen, eine konsolidierte Lizenzverwaltung, klare Rollenkonzepte für Bereitstellung und Entzug von Zugängen sowie regelmäßige Nutzungsanalysen, um Redundanzen zu reduzieren.

Ohne einheitliche Steuerung entstehen redundante Tools, die ähnliche Aufgaben erfüllen, während Volumenrabatte ungenutzt bleiben. Eine fehlende Integration mit dem Identitätsmanagement kann zu übermäßigen Berechtigungen und Schattenzugriffen führen. Vertragslaufzeiten werden verstreut verwaltet, Kündigungsfenster versäumt und automatische Verlängerungen erhöhen die Kosten.

Ein zentraler Portfolio- und Beschaffungsprozess, ergänzt um vorab genehmigte Anbieterlisten und standardisierte Vertragsklauseln, reduziert die Komplexität. Dashboards mit Nutzungs- und Kostenkennzahlen geben Fachbereichen und ITAM eine gemeinsame Sicht. Die Erweiterung der Zusammenarbeit zwischen ITAM und FinOps auf SaaS schafft transparente Kostenstellen, erlaubt Benchmarking und priorisiert Konsolidierung dort, wo der größte Effekt entsteht.

3. ITAM ALS PFEILER DER CYBERRESILIENZ ETABLIEREN

ITAM ist für Cybersecurity elementar: Ohne vollständige, aktuelle Asset- und Configuration-Item-(CI)-Informationen bleiben Lücken im Patch-Management, bei Schwachstellenscans und bei der Incident Response. Regulatorische Vorgaben wie DORA und NIS-2 verlangen belastbare Nachweise zur Resilienz und zu kontrollierten Abhängigkeiten. Besonders relevant ist die Behandlung von Open-Source-Komponenten: Ohne formale Steuerung von Lizenzen und Sicherheitsmeldungen entstehen schnell konkrete Risiken. Unternehmen nutzen dafür Software-Stücklisten (Software

Bill of Materials), um Komponenten aufzulösen, Lizenzen zu prüfen und Schwachstellen zeitnah zu adressieren.

Sicherheits- und ITAM-Teams benötigen eine gemeinsame Arbeitsgrundlage: geteilte Datenquellen, abgestimmtes Monitoring, gemeinsame Kennzahlen. ITAM liefert Inventar und Versionen, Cybersecurity priorisiert nach Kritikalität. Beide Teams planen zusammen und verfolgen Maßnahmen. Im Störfall beschleunigt ITAM die Identifikation betroffener Systeme und verkürzt Wiederherstellungszeiten.

4. INTELLIGENTE AUTOMATISIERUNG NUTZEN

Skalierbare ITAM-Prozesse erfordern Automatisierung: von der Datenerfassung bis zur Ableitung und Umsetzung von Maßnahmen. Künstliche Intelligenz kann Muster in Nutzungs- und Kostendaten erkennen, Prognosen für Bedarf und Budget liefern und Optimierungsvorschläge bei Lizenzen unterbreiten. Gleichzeitig bleiben Hürden bei der Datenqualität, bei eindeutigen Nutzennachweisen, Tool-Lock-ins und der Kapazität von Fachexpertise. Wer erfolgreich automatisiert, beginnt mit klaren Zielen, robusten Datenpipelines und eng verzahnten Teams aus ITAM, FinOps und Einkauf.

In der Praxis setzen Unternehmen Automatisierung vor allem bei der Lizenzoptimierung über alle Umgebungen hinweg ein, bei automatisierten Vertragsanalysen und der Vorbereitung von Renewals sowie bei der Echtzeit-Überwachung von Cloud-Ausgaben mit FinOps-Kopplung. Hinzu kommt eine integrierte Sicht über IT-Service-Management, Asset-Management und Konfiguration, um Ursache-Wirkungs-Zusammenhänge schneller zu erkennen. Wo Hardware eine Rolle spielt, lässt sich der Lebenszyklus mit Telemetrie und prädiktiver Wartung effizienter steuern.

5. ITAM MIT NACHHALTIGKEITSZIELEN VERKNÜPFEN

ITAM unterstützt Unternehmen direkt bei der Umsetzung ihrer Nachhaltigkeitsziele (Environmental, Social, Governance, ESG): Längere Nutzungszyklen von Geräten reduzieren nicht nur Emissionen und Kosten, sondern auch den Bedarf an Ressourcen. Vollständige Asset-Daten erleichtern die Erstellung von ESG-Berichten erheblich. Einige Unternehmen integrieren ITAM-Daten bereits systematisch in ihre Nachhaltigkeitssteuerung und nutzen die gewonnene Transparenz, um Beschaffungsentscheidungen gezielter auf Energieeffizienz und Kreislaufwirtschaft auszurichten.

Unternehmen können mit einer transparenten Sicht auf Alter, Zustand und Nutzung von Geräten Refresh-Zyklen fundiert verlängern, ohne die Produktivität zu gefährden. In ESG-Berichten ermöglicht ITAM die Nachverfolgung von der Beschaffung bis zur Verwertung und macht Nachhaltigkeitsaussagen nachprüfbarer.

AUSBLICK

ITAM entwickelt sich zunehmend von einer operativen zu einer strategischen Funktion: Es verbindet Innovation und Verantwortung. Unternehmen, die die beschriebenen fünf Handlungsfelder systematisch angehen, stärken ihre Widerstandsfähigkeit, erhöhen die Transparenz und treffen bessere Technologieentscheidungen – heute und in einer zunehmend durch KI geprägten IT-Landschaft. ■

ANDRÉ KUNTZE
ist Partner bei Deloitte und leitet den Bereich Extended Enterprise im Offering Portfolio Cyber mit über 20 Jahren Erfahrung.

CHRISTOPH GOMANN
ist Leiter im Bereich IT Asset Management (ITAM) bei Deloitte mit Schwerpunkt im Aufbau und der Professionalisierung von ITAM-Organisationen und Kostenmanagement.

STRATEGISCHE ROADMAP FÜR ITAM-LIZENZMANAGER UND IT-SECURITY-VERANTWORTLICHE

Kurzfristig (0–6 Monate)

- *Sichtbarkeit herstellen, zentrale Governance definieren, SaaS-Inventar konsolidieren, erste Automatisierungs-Use-Cases starten und Software-Bill-of-Materials-(SBOM)-Prozesse für kritische Anwendungen aufsetzen*
- *Pilotieren von zentralen Dashboards, Abstimmen von Kennzahlen zwischen ITAM, FinOps und Cybersecurity und Schaffen einer „Single Source of Truth" für Assets und CIs*

Mittelfristig (6–18 Monate)

- *Datenqualität an der Quelle verbessern, ITAM, FinOps und Cybersecurity enger verzahnen, Cloud- und SaaS-Kosten kontinuierlich optimieren, Portfolio konsolidieren und resilienzbezogene Berichte etablieren*
- *Aufbau von integrierten Workflows, die Beschaffung, Bereitstellung, Nutzung und Stilllegung nahtlos verbinden*
- *Entwicklung von verbindlichen Rollen- und Freigabeprozessen*
- *Verankern von Service-Level-Agreements-(SLA)- und Key-Performance-Indicators-(KPI) zur Steuerung*

Langfristig (18+ Monate)

- *Operating Model für intelligentes, nachhaltiges ITAM institutionalisieren, KI-gestützte Entscheidungsfindung integrieren, Lebenszyklus- und Kreislaufwirtschaftspraktiken standardisieren und Governance kontinuierlich weiterentwickeln*
- *Skalieren mittels Automatisierung über zusätzliche Use-Cases und Etablieren eines kontinuierlichen Verbesserungsprogramms mit regelmäßigen Reifegrad-Assessments*

Von der Norm zur Wirkung (4):
Wie Unternehmen regulatorische Anforderungen wirksam steuern können

INTEGRIERTE GOVERNANCE STATT REGELFLUT

Bild: Eigene Darstellung, generiert mit ChatGPT (SORA)

Mit NIS-2, DORA und ESG wächst die Regulierungsdichte für Unternehmen stetig. Unsere Autoren zeigen im vierten Teil der Artikel-Serie, warum additive Compliance-Ansätze scheitern und wie ein integriertes Steuerungsmodell aus ISO 27001 und Internem Kontrollsystem (IKS) die Lösung sein kann.

Regulatorische Anforderungen stellen längst kein temporäres Phänomen mehr dar. Mit der Network and Information Security Directive 2 (NIS-2), dem Digital Operational Resilience Act (DORA), Environmental, Social and Governance (ESG) Vorgaben und branchenspezifischen Anforderungen hat sich ein dauerhafter Ordnungsrahmen für Unternehmen entwickelt.[1, 2] Organisationen sehen sich kontinuierlich mit neuen Erwartungen an Prozesse, Kontrollen und Nachweise konfrontiert.

Dabei ist nicht die einzelne Vorschrift die eigentliche Herausforderung. Entscheidend ist vielmehr ihre kumulative Wirkung: Anforderungen überlagern sich, greifen ineinander und verstärken sich gegenseitig.[3, 4] Jede neue Regel schafft zusätzliche Erwartungen an Prozesse, Kontrollen, Nachweise und Verantwortlichkeiten – häufig ergänzend zu bereits bestehenden Governance-Strukturen.

Damit verändert sich die zentrale Frage unternehmerischer Steuerung: Verfügen wir über ein Governance-Modell, das auch zukünftige Anforderungen integrieren kann – ohne an Wirksamkeit, Stabilität oder Übersicht zu verlieren?[5]

In den bisherigen Beiträgen dieser Artikelreihe haben die Autoren schrittweise aufgezeigt, wie ein solches Modell entstehen kann: von prozessorientierter Steuerung als Fundament (Teil 1),[6] über strukturierte Informationssicherheit als Vertrauensbasis (Teil 2),[7] bis hin zu methodischem Risikomanagement als Entscheidungsgrundlage (Teil 3).[8]

Dieser vierte Beitrag vollzieht nun den Übergang von methodischer Exzellenz zu integrierter Steuerungsfähigkeit. Er führt die Perspektiven zusammen und richtet den Fokus auf integrierte Governance – besonders auf das Zusammenspiel von Internem Kontrollsystem, Managementsystemen und aktuellen regulatorischen Anforderungen wie ESG und DORA.

Im Zentrum steht dabei eine wesentliche Einsicht: Zukunftsfähige Governance muss stabil, erweiterbar und dauerhaft wirksam sein. Sie darf nicht bei jeder neuen Regulierung neu

WAS BEDEUTET „IKS“ IN DIESEM BEITRAG?

Ein Internes Kontrollsystem (IKS) umfasst alle Grundsätze, Verfahren und Maßnahmen, die darauf ausgerichtet sind,

- ***Risiken zu begrenzen,***
- ***Prozesse verlässlich zu steuern und***
- ***die Zielerreichung einer Organisation sicherzustellen.***

Im klassischen Verständnis wird das IKS häufig aus einer prüfungsorientierten Perspektive betrachtet. Der Fokus liegt dabei auf der Angemessenheit und Ausgestaltung von Kontrollen – also darauf, ob Kontrollen formal vorhanden, dokumentiert und plausibel konzipiert sind.

In diesem Beitrag wird das IKS bewusst weiter gefasst: als aktiver Steuerungsmechanismus, der überprüft, ob Kontrollen im operativen Betrieb tatsächlich wirksam sind – kontinuierlich, nachvollziehbar und entscheidungsrelevant.

Diese Unterscheidung ist wesentlich: Während eine reine Design-Betrachtung Aussagen über die formale Eignung von Kontrollen zulässt (vergleichbar mit einer Angemessenheitsprüfung), liefert erst die Betrachtung der Wirksamkeit über einen Zeitraum belastbare Erkenntnisse zur tatsächlichen Steuerungsfähigkeit einer Organisation.

Dieses Verständnis orientiert sich an internationalen Referenzrahmen wie dem COSO Internal Control – Integrated Framework sowie an Prüfungsstandards wie IDW PS 980, geht jedoch bewusst über eine rein prüfungs- oder zertifizierungsorientierte Sicht hinaus.[9, 10]

In der Prüfungspraxis entspricht diese Differenzierung der Unterscheidung zwischen einer reinen Angemessenheitsbetrachtung (zum Beispiel „Type 1“) und einer Wirksamkeitsbetrachtung über einen definierten Zeitraum („Type 2“).

In diesem Verständnis fungiert das IKS nicht als nachgelagerte Prüfmechanik, sondern als Betriebssystem integrierter Governance: Es verbindet Regeln, Prozesse und Verantwortlichkeiten, macht Abweichungen frühzeitig sichtbar und wirkt als Sensor der Organisation, der belastbare Grundlagen für fundierte Führungs- und Steuerungsentscheidungen liefert.

aufgebaut werden müssen, sondern muss zusätzliche Anforderungen als weitere Perspektiven in ein bestehendes Steuerungsmodell integrieren.

WENN GOVERNANCE WÄCHST, WÄCHST DIE KOMPLEXITÄT

In vielen Organisationen zeigt sich ein wiederkehrendes Muster: Neue regulatorische Anforderungen beantworten Verantwortliche mit neuen Maßnahmen. Sie ergänzen bestehende Systeme um zusätzliche Richtlinien, weitere Kontrollkataloge, neue Berichtsformate und separate Prüfzyklen. Jede Regulierung wird als eigenes Vorhaben behandelt – mit eigener Logik, eigenen Zuständigkeiten und eigenen Nachweisen.

Was zunächst strukturiert erscheint, entwickelt in der Praxis eine problematische Nebenwirkung: Governance wächst additiv, nicht integrativ. An diesem Punkt trennt sich klassische von zukunftsfähiger Governance.

Denn additive Governance stößt hier strukturell an ihre Grenzen. Kontrollen adressieren vergleichbare Risiken, sind jedoch in unterschiedlichen Systemen verankert. Unternehmen erzeugen Evidenzen mehrfach, Fachbereiche erleben Governance als Zusatzarbeit und das Management erhält umfangreiche Berichte – jedoch nur begrenzt entscheidungsrelevante Informationen. Mehr Governance bedeutet also nicht automatisch mehr Steuerung.[5]

Im Kern beruht diese Entwicklung auf einem verbreiteten Denkfehler: der Annahme, Organisationen könnten Steuerung durch das schrittweise Ergänzen weiterer Regelwerke, Kontrollen und Dokumentationen beherrschen.

Dieses additive Verständnis erzeugt zwar formale Vollständigkeit, steigert jedoch selten die tatsächliche Wirksamkeit. Isolierte Governance-Systeme konkurrieren um Aufmerksamkeit, Ressourcen und Prioritäten. Governance entwickelt sich reaktiv und aufwandsgetrieben, statt vorausschauend zu wirken und aktiv zu steuern.

Die zentrale Frage moderner Governance lautet daher nicht mehr, ob alle Anforderungen umgesetzt sind, sondern ob ein Steuerungsmodell vorhanden ist, das Wirkung erzeugt und diese Wirkung als Entscheidungs- und Handlungsfähigkeit des Managements auch unter wachsender Regulierung aufrechterhält und damit die Leistungsfähigkeit des Kontrollumfelds dauerhaft sicherstellt. Integration ist dabei keine optionale Optimierung, sondern eine strukturelle Notwendigkeit.

DER ORDNUNGSRAHMEN INTEGRIERTER GOVERNANCE

Was fehlt, ist kein weiteres Regelwerk, sondern ein zentraler Ordnungsrahmen, der bestehende Anforderungen zusammenführt und dauerhaft tragfähig macht. Ein solcher Ordnungsrahmen ist in vielen Organisationen bereits vorhanden: die ISO 27001.[11]

In der Praxis reduzieren viele Verantwortliche diesen Standard häufig auf Informationssicherheit oder Zertifizierung. Tatsächlich ist er als Managementsystem konzipiert und folgt einer klaren Governance-Logik.[12] Er bietet eine strukturierende Klammer, die weit über technische Sicherheitsmaßnahmen hinausgeht.

Die ISO 27001 bringt zentrale Elemente mit: Sie schafft Kontext- und Zielorientierung, leitet Maßnahmen risikobasiert ab, definiert klare Rollen und Verantwortlichkeiten und verankert regelmäßige Reviews sowie Managementbewertungen.

Der entscheidende Perspektivwechsel besteht darin, die ISO 27001 nicht als Ziel, sondern als Fundament für integrierte Governance zu verstehen. Die in Teil 3 dargestellte risikobasierte Entscheidungslogik findet hier ihren strukturellen Anker. Neue regulatorische Anforderungen werden damit nicht zu neuen Systemen, sondern zu Erweiterungen eines bestehenden Kerns.[5]

Abbildung 1: Governance im Prozess. (Bild: eigene Darstellung, generiert mit ChatGPT (SORA))

IKS ALS WIRKSAMKEITSMOTOR

Genau hier entscheidet sich, ob Governance wirkt oder nur beschrieben ist: das Interne Kontrollsystem. Während die ISO 27001 den Ordnungsrahmen definiert, sorgt das IKS dafür, dass dieser Kern im operativen Betrieb tatsächlich wirkt. In einem integrierten Governance-Verständnis übernimmt es drei zentrale Funktionen:

- Überprüfung der Wirksamkeit von Kontrollen,
- Sichtbarmachung von Abweichungen,
- Auslösung von Steuerungsimpulsen.

Auf diese Weise wirkt das IKS systemübergreifend und macht Governance steuerbar. Es fungiert nicht als reine Prüfmechanik, sondern als kontinuierlicher Feedback- und Steuerungsmechanismus.

Governance entfaltet ihre Wirkung nicht in Richtlinien oder Kontrollkatalogen, sondern dort, wo Arbeit stattfindet: in den Prozessen.[13] Prozesse sind der Ort, an dem Risiken wirksam werden, an dem Kontrollen greifen oder versagen und an dem Entscheidungen vorbereitet werden.

Integrierte Governance verankert Kontrollen direkt im Ablauf. Dieses Prinzip lässt sich als Compliance by Design beschreiben: Organisationen überprüfen Anforderungen nicht nachträglich, sondern integrieren sie von Beginn an in Prozesse, Rollen und Systeme. So entwickelt sich Governance von einer nachgelagerten Prüfaktivität zu einer laufenden Steuerungsfunktion.

AUTOMATISIERUNG ALS VORAUSSETZUNG

Mit wachsender Regulierungsdichte stellt sich eine pragmatische Frage: Wie bleibt integrierte Governance handhabbar? Die Antwort liegt in der gezielten Nutzung von Automatisierung. Sie sorgt dafür, dass Kontrollen, Aufgaben und Evidenzen im Arbeitsfluss entstehen – nicht als manuelle Nacharbeit. Entscheidend ist dabei die Reihenfolge: Nicht Technologie definiert Governance, sondern Governance definiert sinnvolle Automatisierung.

Ohne Automatisierung kippt integrierte Governance unweigerlich wieder in additive Zusatzarbeit.[9] Künstliche Intelligenz kann dabei unterstützen – etwa durch Mustererkennung oder

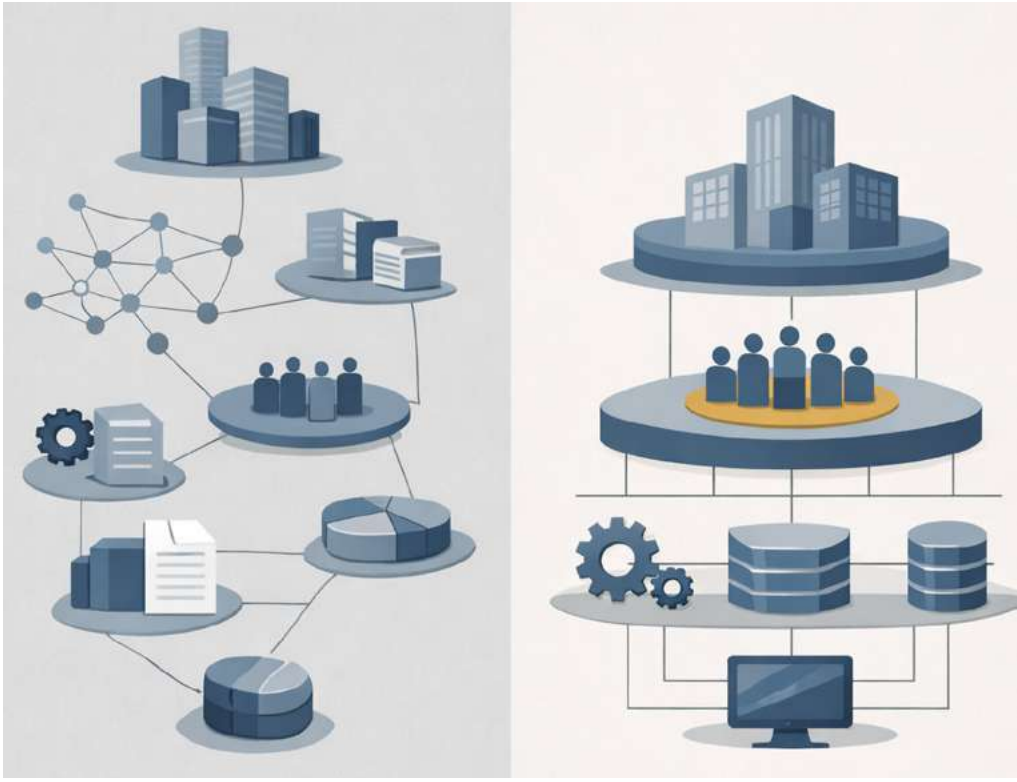


Abbildung 2: Zentraler Governance-Kern. (Bild: eigene Darstellung, generiert mit ChatGPT (SORA))

Priorisierung. Die Verantwortung für Entscheidungen über Risiken und Maßnahmen verbleibt jedoch bewusst beim Menschen.

UNTERSCHIEDLICHE PERSPEKTIVEN AUF EINEN GEMEINSAMEN KERN

IKS, ESG und DORA stehen exemplarisch für unterschiedliche regulatorische Zielsetzungen. Sie beruhen jedoch auf demselben grundlegenden Steuerungsmechanismus: Organisationen identifizieren Risiken, leiten daraus Kontrollen ab, überprüfen deren Wirksamkeit und steuern Abweichungen gezielt.[5, 9]

Der Unterschied liegt dabei nicht im Mechanismus, sondern im jeweiligen Blickwinkel. In einem integrierten Governance-Modell werden diese Anforderungen zu unterschiedlichen Perspektiven auf einen gemeinsamen Steuerungskern. Das IKS übernimmt in diesem Kontext eine verbindende Rolle und ermöglicht konsistente Aussagen über Steuerungsfähigkeit –unabhängig davon, welcher regulatorische Auslöser im Vordergrund steht.

FAZIT

In einer Welt permanenter Regulierung ist Governance keine Compliance-Frage mehr, sondern eine Führungsentscheidung.[3] Organisationen, die Governance additiv aufbauen, erzeugen Komplexität. Organisationen, die Governance integrieren, schaffen Übersicht, Wirksamkeit und Entscheidungsfähigkeit.

Ein integriertes Governance-Modell nutzt einen zentralen Ordnungsrahmen, verankert regulatorische Anforderungen direkt in den Prozessen, macht Wirksamkeit kontinuierlich sichtbar und skaliert durch Automatisierung statt durch zusätzlichen Aufwand. So entwickelt sich Governance vom Pflichtprogramm zum aktiven Führungsinstrument.

Richtig verstanden wird Governance damit zum Enabler für Skalierung: Nur Organisationen, deren Steuerungsmodelle stabil, integriert und wirksam sind, können wachsen, ohne dass Komplexität und Regulatorik ihre Handlungsfähigkeit überlagern.

AUSBLICK

Mit diesem integrierten Verständnis endet Governance nicht an den Grenzen der eigenen Organisation. Anforderungen wie DORA, NIS-2 oder ESG verlagern Risiken zunehmend in die Lieferkette. Damit wird integrierte Governance zur Voraussetzung für eine belastbare Steuerung von Lieferketten.

Der abschließende Beitrag dieser Artikelreihe in der nächsten Ausgabe der IT-SICHERHEIT richtet den Blick konsequent nach außen – auf Abhängigkeiten, Partner und die Frage, wie Governance auch über Organisationsgrenzen hinweg wirksam gestaltet werden kann. Denn: Sicherheit, Resilienz und Verantwortung enden nicht am Werkstor. ■

Literatur

[1] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[2] European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[3] OECD. (2021). OECD Regulatory Policy Outlook 2021. OECD Publishing. https://doi.org/10.1787/38b0fdb1-en

[4] European Commission. (2023). Better Regulation Toolbox. Publications Office of the European Union. https://commission.europa.eu/better-regulation-toolbox

[5] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise risk management: Integrating with strategy and performance. COSO. www.coso.org/enterprise-risk-management

[6, 7, 8] IT SICHERHEIT. (2025). Von der Norm zur Wirkung (Teil 1–3). Ausgabe 4/2025, S. 42–48; Ausgabe 5/2025, S. 42–47; Ausgabe 6/2025, S. 44–50

[9] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal control – Integrated framework. COSO. www.coso.org/guidance-on-ic

[10] Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW). (2022). IDW Prüfungsstandard 980: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (Neufassung September 2022). IDW Verlag.

[11] International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

[12] International Organization for Standardization. (2015). ISO 9001:2015 — Quality management systems — Requirements. ISO.

[13] Deming, W. E. (1986). Out of the crisis. MIT Press.

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.

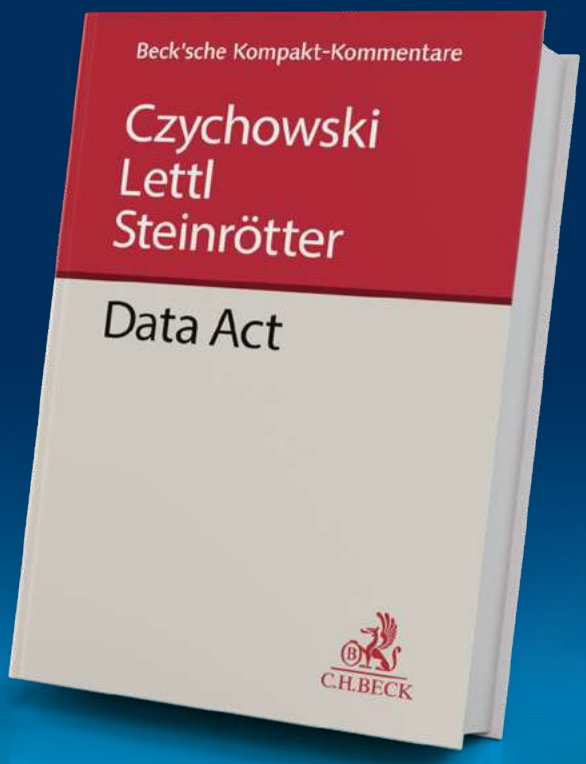
Jeder Beitrag entwickelt praxisnahe Lösungsansätze und zeigt, wie diese in Rollen, Abläufen und Kennzahlen verankert werden können.

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.

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

Data Act



Czychowski / Lettl / Steinrötter

Data Act – Kommentare

2025, 854 Seiten, 139,00 €
C.H.BECK.
ISBN 978-3-406-82090-8

Fast zeitgleich mit dem Geltungsbeginn der Datenverordnung (EU) 2023/2854, auch als Data Act bekannt, erschien im Oktober 2025 das vorliegende Buch. Die Herausgeber, allesamt Direktoren der Potsdamer Forschungsstelle „Geistiges Eigentum – Digitalisierung – Wettbewerb", und ihr vornehmlich aus Rechtsanwältinnen und Rechtsanwälten bestehendes 16-köpfiges Autorenteam wollen betroffenen Anwendern, die den Data Act verstehen und umsetzen müssen, eine fundierte Orientierungshilfe an die Hand geben. Der Verlag verspricht eine „handliche Erstausgabe", die „kompakte Informationen" und „eine klare Struktur für schnelle Orientierung" bietet. Dass „handlich" und „kompakt" dabei nicht „knapp" bedeutet, zeigt der Umfang von 854 Seiten für die Kommentierung der 50 Artikel des Data Acts. Dies deutet zugleich die Komplexität dieses wichtigen Pfeilers des EU-Datenwirtschaftsrechts an.

Der Data Act bezieht sich auf personenbezogene und nicht-personenbezogene Daten, die von vernetzten Produkten oder damit verbundenen Diensten erzeugt werden. Er regelt unter anderem eine Pflicht zur Bereitstellung von Daten, ein Recht auf Datenweitergabe und macht Vorgaben zur fairen Ausgestaltung von Vertragsklauseln. Dieses Regelungskonglomerat lässt die Ausstrahlung der Materie auf andere Rechtsgebiete erahnen. Die richtigen Abgrenzungen insbesondere zum Datenschutzrecht zu finden, wird eine der großen Herausforderungen bei der Anwendung des Data Act sein. Neben der ausführlichen Erläuterung der einzelnen Normen, die zum besseren Verständnis auch Hinweise zu Zielen und Entstehungsgeschichte umfasst, wird gerade diese Abgrenzung beziehungsweise Verflechtung mit anderen Rechtsgebieten von den Autoren immer wieder thematisiert.

Bis zur zweiten Auflage werden durch die Überführung des Data Act in die Praxis und die damit einhergehenden Erfahrungen sowie die folgende Rechtsprechung sicherlich einige derzeit kontrovers diskutierte Aspekte klarer werden. Dennoch sind die Erläuterungen des Kommentars schon jetzt eine wichtige Einstiegshilfe in die neue Materie. ■

THOMAS MÜTHLEIN, KÖLN

Datenrecht

Moritz Hennemann

Datenrecht

2025, 342 Seiten, 49,80 €
C.H.BECK.
ISBN 978-3-406-80381-9

Was mit dem zarten Pflänzchen Datenschutz Anfang der 1970er-Jahre begann, hat sich mittlerweile unter der „Digitalen Dekade der Europäischen Union" zu einem wahren Regulierungsdschungel der „Datenverarbeitung" im umfassendsten Sinne auf europäischer und nationaler Ebene entwickelt. In dieses weite Feld, in dem die Datenschutz-Grundverordnung, die KI-Verordnung oder der Data Act derzeit wohl die prominentesten Vertreter sind, versucht der Autor unter dem Sammelbegriff „Datenrecht" Durchblick und Systematik zu bringen. Wie herausfordernd das ist, lässt sich schon an der Aufzählung von 38 europäischen und nationalen deutschen Gesetzen erahnen, die dem Leser „im Laufe dieses Lehrbuchs immer wieder begegnen werden". Dabei ist die Aufzählung nicht vollständig und schließt eine Behandlung des Datenschutzrechts über Grundlagen und die Schnittstellenthematik hinaus explizit aus. Das hätte – so der Autor – den Rahmen des Werkes von ohnehin schon 342 Seiten vollends gesprengt!

So nimmt sich der Autor der herausfordernden Aufgabe an, das verbleibende Datenrecht für ein „Juristisches Kurz-Lehrbuch" aufzuarbeiten. Dabei stehen besonders der Data Act und der Data Governance Act im Fokus der Betrachtungen, neben:

- den Grundlagen des Datenrechts,
- dem allgemeinen und dem sektorspezifischen Datenrecht,
- der privaten und der behördlichen Rechtsdurchsetzung im Datenrecht,
- der Datenrechtsvergleichung und den globalen Dimensionen des Datenrechts.

Die systematische Aufarbeitung wird von Beispielsfällen begleitet – jeweils am Anfang eines Abschnitts, mit Lösungen an dessen Ende. Darüber hinaus versucht der Autor anhand zahlreicher Skizzen das häufig komplexe Beziehungsgeflecht darzustellen.

Insofern eignet sich das Werk weit über die vom Verlag genannte Zielgruppe hinaus: Neben Studierenden der Rechtswissenschaft, Forschenden im Datenrecht sowie Juristinnen und Juristen in Justiz, Anwaltschaft, Behörden und Verbänden profitieren auch interessierte Politologinnen und Ökonomen davon. Ebenso bietet es Nicht-Juristinnen und Nicht-Juristen sowie Praktikerinnen und Praktikern an den Schnittstellen zum Datenschutz – etwa Datenschutzmanagerinnen, Datenschutzmanagern oder Datenschutzbeauftragten – einen hilfreichen Einstieg in die Welt des Datenrechts jenseits des klassischen Datenschutzes. ■

THOMAS MÜTHLEIN, KÖLN

Der neue Cyber-Risiko-Score

DIE VERMESSUNG DER UNSICHERHEIT

Wissenschaftler der Westfälischen Hochschule Gelsenkirchen entwickeln ein transparentes Bewertungsmodell, das technische Schwachstellen mit dem Geschäftskontext von Unternehmen verknüpft. Der Score soll besonders kleinen und mittleren Unternehmen helfen, ihre Cyberrisiken zu quantifizieren und Investitionen zu priorisieren.

Die Ausgaben für IT-Sicherheit in Deutschland steigen kontinuierlich. Laut Bitkom beliefen sie sich 2024 auf 10,1 Milliarden Euro, für 2025 werden 11,1 Milliarden und für 2026 bereits 12,2 Milliarden Euro prognostiziert.[1] Doch ob diese Investitionen tatsächlich zu mehr Sicherheit führen, bleibt für viele Unternehmen unklar.

Zwar sind sich viele Firmen ihrer internen Risiken grundsätzlich bewusst, doch mangelt es häufig an einer präzisen Einschätzung und einem daraus resultierenden adäquaten Umgang. Gerade im Zeitalter des Homeoffice ist Konnektivität essenziell, birgt jedoch gleichzeitig neue Gefahrenpotenziale: Von außen erreichbare Dienste bieten Angriffsfläche für Angreifer, und oft haben kleine und mittlere Unternehmen (KMU) die eigenen Assets nicht im Blick.

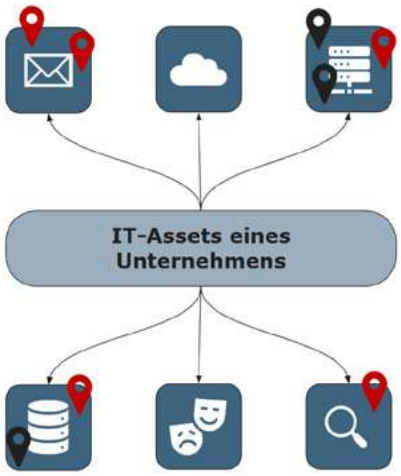


Abbildung 1: Mögliche Assets eines Unternehmens und ihre Schwachstellen, kategorisiert in CVEs und CWEs. (Bild: if(is))

Bild: whyframeshot - stock.adobe.com

Automatisierte Pentests und Schwachstellenscanner liefern zwar wertvolle Erkenntnisse über Sicherheitslücken und Fehlkonfigurationen. Doch lassen die Ergebnisse in puncto Vergleichbarkeit und konkreter Handlungsempfehlungen oft zu wünschen übrig. Zudem ist eine Diskrepanz innerhalb der Unternehmen festzustellen: Während das Management Kennzahlen für finanzielle Risikoabschätzungen und Investitionsentscheidungen benötigt, liefert die IT-Abteilung meist rein technische Berichte. Diese unterschiedlichen Perspektiven führen zu erheblichen Kommunikationsproblemen, obwohl beide Seiten dasselbe Ziel verfolgen: die Absicherung des Unternehmens.

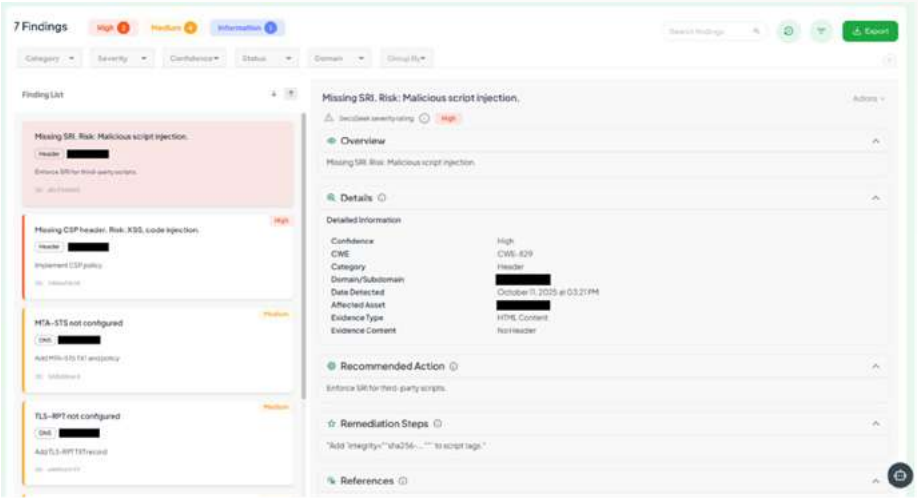


Abbildung 2: Beispiel eines Schwachstellen-Scans mit der Plattform SecuSeek (Bild: if(is)).

Um diese Lücke zu schließen, müssen technische Befunde in quantifizierbare Werte übersetzt werden. Die Bewertung der IT-Sicherheitslage ist kein neues Konzept, doch bestehenden Modellen mangelt es häufig an Transparenz und Verhältnismäßigkeit. Viele Bewertungssysteme agieren als proprietäre „Blackboxen" oder ignorieren den Geschäftskontext und damit kritische Ankerpunkte des Unternehmens. Aspekte wie ein funktionierendes Notfallmanagement oder klare Hierarchien werden häufig nicht ausreichend berücksichtigt. Zudem wirken langwierige Audits und Zertifizierungen durch ihren hohen Aufwand oft eher abschreckend als motivierend.

An dieser Stelle setzt der Cyber-Risiko-Score (CRS) an. Ziel ist ein kontextsensitiver, objektiver Bewertungsmaßstab, der nicht nur transparent und verständlich ist, sondern auch eine faire Vergleichbarkeit innerhalb von Branchen ermöglicht. Doch warum reichen die bisherigen Ansätze nicht aus?

SCHWÄCHEN UND BLINDE FLECKEN

Eine zentrale Schwäche vieler aktueller Risikomanagement-Tools ist ihre Unvollständigkeit. Wesentliche Aspekte einer ganzheitlichen Bewertung bleiben oft außen vor – etwa die wirtschaftliche Bewertung von Assets oder eine systematische Risikoevaluierung. Auch die Konsistenz der Ergebnisse lässt zu wünschen übrig: Zwischen qualitativen und quantitativen Ansätzen klafft eine deutliche Lücke.[2]

Hinzu kommt: Quantitative Methoden, die das gesamte Ausmaß eines Risikos abbilden könnten, fehlen häufig. Die exakte Verortung von Schwachstellen oder Fehlkonfigurationen ist jedoch entscheidend. Ein weiteres Problemfeld ist die Diskrepanz zwischen den Perspektiven von Softwareentwicklung und Unternehmensmanagement. Die Abhängigkeiten beider Bereiche sind bislang kaum erforscht.[3] IT-Sicherheitsaspekte werden im Managementalltag oft zugunsten anderer Entscheidungen vernachlässigt – ein wiederkehrendes Phänomen, das bereits in früheren Studien diskutiert wurde.[4]

Kritik gibt es auch an sogenannten Punktlösungen: Isolierte IT-Sicherheitsmaßnahmen ignorieren den Gesamtaufwand und die Anpassungsfähigkeit der Angreifer. Für eine fundierte Bewertung müssen jedoch auch Implementierungskosten und operative Kompromisse einbezogen werden. Unternehmensziele und Umsatz sind die eigentlichen Treiber – ein Risk-Assessment muss diese Faktoren berücksichtigen.[5]

Ein weiteres Thema ist die Detektion von Angriffen und Schäden, die auf fehlende oder fehlerhafte IT-Sicherheitsmechanismen zurückgehen. Neben technischen Faktoren spielt hier der „Human Factor" eine zentrale Rolle. Ein Bewertungsmodell sollte daher auch die Art und Weise der Detektion widerspiegeln.[6]

Die Fachliteratur betont immer wieder: Der menschliche Faktor und die Interaktion der Nutzer mit dem Netzwerk sind entscheidend. Gängige Bewertungsmethoden vernachlässigen diesen Aspekt häufig, obwohl Nutzerverhalten Risiken sowohl verursachen als auch mindern kann.[7]

Die Quantifizierung von Risiken bleibt eine Herausforderung. Bei der Übertragung qualitativer Aussagen gehen oft wichtige Informationen verloren. Hinzu kommen ökonomische Hürden: Investitionen in Cybersicherheit bringen selten einen unmittelbaren Return on Investment (ROI). Gerade kleine und mittlere Unternehmen mit begrenztem Budget benötigen daher Scores mit konkreten Handlungsempfehlungen, um fundierte Entscheidungen treffen zu können.[8]

CYBER-RISIKO-CHECK DES BSI

Ein praktisches Beispiel für standardisierte Risikobewertung ist der Cyber-Risiko-Check des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dieser IT-Sicherheitscheck für KMU basiert auf der DIN SPEC 27076, die das BSI gemeinsam mit 20 Partnern entwickelt hat. Mithilfe eines kurzen Interviews mit 27 Anforderungen wird die IT-Sicherheit eines Unternehmens geprüft. Die Teilnehmer erhalten anschließend Handlungsempfehlungen für nicht erfüllte Anforderungen. Damit schafft der Check eine strukturierte IT-Sicherheitsbewertung und bietet zugleich konkrete, leicht umsetzbare Verbesserungsimpulse, die auf die Bedürfnisse von KMU abgestimmt sind.[9]

Die Ergebnisse sind ernüchternd: Laut BSI-Lagebericht 2025 sind die meisten KMU nicht ausreichend gegen Cyberbedrohungen geschützt. Lediglich rund 56 Prozent der überprüften Unternehmen erfüllen die Anforderungen des Cyber-Risiko-Checks.[10]

Die anonymisierten Ergebnisse dieser Checks dienen als Datenquelle für die Validierung und Weiterentwicklung des hier vorgestellten Cyber-Risiko-Scores.

DER CYBER-RISIKO-SCORE

Das Kernkonzept des CRS ist eine hybride Heuristik, die auf den fundamentalen Prinzipien der Risikobewertung basiert.[11] Anstatt sich auf die bloße Identifizierung technischer Schwachstellen zu beschränken, integriert der CRS diese in den übergeordneten Geschäftskontext des Unternehmens. Das Ziel besteht darin, komplexe Datenpunkte zu einer einzigen, intuitiven Kennzahl zusammenzufassen, die auf einer Skala von 0 (minimales Risiko) bis 10 (kritisches Risiko) dargestellt wird. Diese Zahl dient nicht der Panikmache, sondern ist eine objektive Grundlage für die Priorisierung von Ressourcen.

Der CRS wird aus zwei Hauptkomponenten berechnet: der Eintrittswahrscheinlichkeit (Likelihood) und dem Schadensausmaß (Impact), moduliert durch die organisatorische Reife des Unternehmens.

Die Likelihood-Bewertung im CRS stellt eine Abkehr vom Dogma dar, dass ein hoher CVSS-Score automatisch ein hohes Risiko bedeutet. Ein CVSS-Score von 9.8 beschreibt lediglich den technischen Schweregrad einer Lücke, ignoriert aber zwei entscheidende Fragen: Wird diese Lücke tatsächlich angegriffen? Und wie wichtig ist das betroffene IT-System für das Unternehmen?

Die Likelihood-Heuristik beantwortet diese Fragen durch eine zweistufige Kontextualisierung:

1. **Interne Kontextualisierung (Asset-Kritikalität)**
   Nicht jedes IT-System hat die gleiche Priorität. Eine Schwachstelle auf einem isolierten Testsystem stellt ein vernachlässigbares Risiko dar, während dieselbe Schwachstelle auf dem zentralen Enterprise-Resource-Planning-(ERP)-Server oder dem Domain-Controller existenzbedrohend sein kann. Der CRS führt daher den Faktor der „Kontext-Schwere" ein. Bei der Berechnung wird der technische Roh-Score eines Befunds mit einem festgelegten Kritikalitätsfaktor multipliziert. Dies gewährleistet, dass das Modell „business-aware" agiert und Risiken dort priorisiert, wo die Wertschöpfung des Unternehmens stattfindet.

2. **Externe Bedrohungsanalyse (Threat Intelligence)**
   Die bloße Existenz einer Lücke stellt noch keinen Angriff dar. Um die Wahrscheinlichkeit eines Angriffs zu bewerten, integriert der CRS moderne Threat-Intelligence-Metriken:

   - **EPSS (Exploit Prediction Scoring System):** Dieser Wert gibt die statistische Wahrscheinlichkeit an, mit der eine Schwachstelle innerhalb der nächsten 30 Tage aktiv ausgenutzt wird.[12] Eine Lücke mit einem EPSS-Wert von 95 Prozent wird im Modell deutlich höher gewichtet als eine theoretische Lücke mit 0,1 Prozent, auch wenn beide denselben CVSS-Wert aufweisen.

   - **CISA KEV (Known Exploited Vulnerabilities):** Das Modell ist mit einem „Not-Aus-Schalter" ausgestattet. Wird eine

Common Vulnerabilities and Exposures (CVE) im Katalog der Cybersecurity and Infrastructure Security Agency (CISA) für aktiv ausgenutzte Schwachstellen gefunden, wird der Likelihood-Score – unabhängig von anderen Faktoren – auf das Maximum gesetzt. Dies reflektiert die Realität, dass bei einer aktiv ausgenutzten Lücke die Zeit für probabilistische Abwägungen vorbei ist; hier herrscht akuter Handlungsbedarf.

Die finale Berechnung der Likelihood erfolgt über eine gewichtete Formel, die entweder der internen Relevanz (Kontext-Schwere) den Vorrang gibt, oder die externe Bedrohungslage (EPSS) höher bewertet (siehe Abbildung 3).

$$LIKELIHOOD = \max\left(\frac{Crit_x \cdot CVSS_x}{Crit_{max} \cdot 10} \cdot v + EPSS_x \cdot (1 - v)\right)$$

Abbildung 3: Berechnung des Likelihood-Scores mittels CVSS, EPSS und dem Kritikalitätsfaktor (Bild: if(is))

RELATIVER IMPACT STATT ABSOLUTER EURO-BETRÄGE

Die zweite Säule des CRS ist der Impact-Score. Die Bewertung des Schadensausmaßes für KMUs stellt eine Herausforderung dar, da die Relation von entscheidender Bedeutung ist. Ein Schadensfall in Höhe von 500.000 Euro wird von einem Konzern als „Cost of doing business" verbucht, während er für ein kleines mittelständisches Unternehmen die Insolvenz bedeuten kann. Absolute Euro-Beträge sind daher als Risikometrik ungeeignet, um Dringlichkeit vergleichbar zu machen.

Der CRS löst dies durch das Konzept des „relativen Impacts" auf. Die Heuristik folgt dabei einem dreistufigen Prozess:

1. **Basis-Schaden:** Zunächst wird auf Basis von Branchen-Reports (zum Beispiel für das Gesundheitswesen, die Fertigungsindustrie oder den Finanzsektor) oder Daten von Versicherern ein durchschnittlicher monetärer Schaden durch Cybervorfälle ermittelt. Dies dient als statistischer Anker.

2. **Modulation:** Dieser Wert wird durch die individuelle Resilienz des Unternehmens angepasst.

3. **Relativierung:** Die Verhältnissetzung zum Jahresumsatz des Unternehmens ist von entscheidender Bedeutung. Das Modell quantifiziert, welchen Prozentsatz des Jahresumsatzes potenzielle Vorfälle gefährden.

Im Anschluss wird diese prozentuale Belastung über eine Normierungsfunktion auf einer Skala von 0 bis 10 abgebildet. Das Modell definiert Schwellenwerte für die „Schmerzgrenze". Ein Schaden, der mehr als 20 Prozent oder in aggressiveren Modellen 50 Prozent des Jahresumsatzes entspricht, wird als existenziell (Impact-Score 10) eingestuft. Das gewährleistet, dass der CRS für ein 5-Millionen-Euro-Unternehmen genauso präzise funktioniert wie für ein 500-Millionen-Euro-Unternehmen. Das Risiko wird für die Geschäftsführung durch die direkte Kopplung an die finanzielle Leistungsfähigkeit spürbar.

$$IMPACT = f\left(\frac{Schaden_{Branche}}{Jahresumsatz}\right)$$

Abbildung 4: Berechnung des Impact-Scores, indem der durchschnittliche Branchenschaden nach einem Cyberangriff durch den jeweiligen Jahresumsatz dividiert wird (Bild: if(is))

Ein rein technischer Scan kann die organisatorische Verteidigungsfähigkeit eines Unternehmens nicht adäquat abbilden. Der Nutzer ist sich der Existenz des offenen Ports bewusst, hat jedoch keine Kenntnis darüber, dass dieser von einem Administrator überwacht wird. Er erkennt die veraltete Software, nicht jedoch den Notfallplan, der im Fall eines Ausfalls greift. Um diese Blindheit zu überwinden, integriert der CRS die Ergebnisse des BSI CyberRisikoChecks.

Im CRS dienen diese Ergebnisse als mathematische „Modulatoren", die die technischen Scores verstärken oder abschwächen:

- **Impact-Modulation (Fokus: reaktive Maßnahmen):** Fragencluster zu den Themen Notfallmanagement und Datensicherung (Backups) beeinflussen den Impact-Score. Ein Unternehmen mit einem hohen Reifegrad (etwa etablierte und getestete Notfallpläne) erhält einen Bonus-Faktor, der den angenommenen monetären Schaden reduziert. Die zugrunde liegende Logik ist, dass eine vorbereitete Partei eine schnellere Wiederherstellung der Online-Verfügbarkeit, einen geringeren Umsatzverlust und eine Minimierung von Reputationsschäden und Bußgeldern erfährt. Im Gegenzug wird ein Unternehmen ohne Notfallkonzept mit einem Malus-Faktor belegt. Im Ernstfall kann Chaos zu erheblichen Kosten führen.

- **Likelihood-Modulation (Fokus: präventive Maßnahmen):** Fragencluster zu den Themen Patchmanagement, Mitarbeitersensibilisierung und Zugriffssteuerung wirken sich auf den Likelihood-Score aus. Selbst wenn technische Schwachstellen existieren, reduziert ein gut durchdachter Prozess die Wahrscheinlichkeit einer erfolgreichen Ausnutzung erheblich. Ein funktionierendes Patchmanagement ist essenziell, um das Zeitfenster für Angreifer zu schließen. Geschulte Mitarbeiterinnen und Mitarbeiter erkennen Phishingmails, bevor Malware ausgeführt wird. Auch hier wird proaktives Verhalten direkt in der Score-Berechnung belohnt.

Durch diese Integration wird der CRS zu einem ganzheitlichen Instrument. Er bestraft nicht nur technisches Versagen, sondern belohnt Investitionen in organisatorische Sicherheit. Unternehmen können ihren Score also nicht nur durch teure Hardware, sondern auch durch optimierte Prozesse („Hausaufgaben machen") aktiv verbessern.

HYBRIDE FORMEL VERHINDERT RISIKO-VERWÄSSERUNG

Die letzte Meile der Heuristik besteht in der Synthese von Impact und Likelihood zum finalen Cyber-Risiko-Score. Das Modell vermeidet den Fehler einfacher Durchschnittsberechnungen, die extreme Risiken oft verwässern („hoher Impact + niedrige Likelihood = mittleres Risiko"; eine oft trügerische Sicherheit).

Stattdessen nutzt der CRS eine hybride Formel, die zwei mathematische Prinzipien vereint (siehe Abbildung 5):

1. **Das geometrische Mittel:** Dies veranschaulicht die multiplikative Natur von Risiken. Es wird betont, dass ein signifikantes Risiko nur entsteht, wenn beide Faktoren

vorhanden sind. Wenn einer der Faktoren den Wert Null erreicht, bricht das Risiko zusammen, was der logischen Definition von Risiko entspricht.

2. **Die Maximum-Funktion:** Dieser sogenannte „Dominanz-Term" stellt sicher, dass ein Extremwert in einer Dimension nicht ignoriert werden kann. Ein existenzbedrohender Impact (Score 10) führt auch bei geringer Wahrscheinlichkeit zu einem erhöhten Alarmzustand, ebenso wie eine akute Angriffswelle (Likelihood 10), die auch bei moderatem Schaden ernst genommen werden muss.

$$CRS = f_{max}\left(\sqrt{IMPACT \cdot LIKELIHOOD}\right)$$

Abbildung 5: Finale Berechnung des Cyber-Risiko-Scores mittels geometrisches Mittel und einer Maximum-Funktion (Bild: if(is))

Die Auswertung umfasst jedoch nicht nur die Zahl. Der CRS nutzt die im Prozess gesammelten Daten – besonders die Kontextschwere der einzelnen Assets –, um einen priorisierten Handlungsplan zu generieren. Das Bewertungssystem identifiziert nicht nur das Problem, sondern simuliert auch die Lösung: „Wenn Sie Maßnahme A auf Server B umsetzen, sinkt Ihr Score voraussichtlich um 1,2 Punkte."

Dadurch wird die IT-Sicherheit von einer unübersichtlichen technischen Herausforderung in eine steuerbare Managementaufgabe transformiert. Der CRS liefert Transparenz durch Methodik, Relevanz durch Kontext und Handlungsfähigkeit durch Priorisierung. In einer Zeit, in der die Frage nicht mehr „ob", sondern „wann" ein Angriff erfolgt, ist diese Klarheit der wertvollste Schutzschild, den ein Unternehmen haben kann.

DATENBESCHAFFUNG ALS ZENTRALE HERAUSFORDERUNG

Die Entwicklung eines öffentlichen Scoring-Modells ist mit zahlreichen Herausforderungen verbunden. Derzeit basiert der Cyberrisiko-Score auf öffentlich verfügbaren Daten, wie der Anzahl und den Kosten von Cybersicherheitsvorfällen je Unternehmensbranche. Diese Grundlage ist jedoch begrenzt und eignet sich vorerst nur für interne Evaluationen der Heuristik. Für den produktiven Einsatz sind hochwertige Unternehmensdaten in großer Menge erforderlich.

Die Beschaffung der Daten stellt sowohl organisatorisch als auch methodisch eine Herausforderung dar. Sicherheitsrelevante Unternehmensdaten sind häufig vertraulich, nicht standardisiert oder regulatorisch eingeschränkt zugänglich, was eine systematische Sammlung erschwert. Gleichzeitig besteht die Herausforderung, ausreichend große Datenmengen pro Branche zu erhalten, um robuste und generalisierbare Scoring- und Lernmodelle zu ermöglichen.

Neben der Qualität spielt auch die Herkunft dieser Daten eine zentrale Rolle. Um einen Bias zu vermeiden, ist es ratsam, die erhobenen Daten diversifiziert in einer hohen Anzahl pro Branche und aus geografisch verteilten Regionen zu beziehen. Dies ist besonders dann relevant, wenn die Daten aus öffentlichen Quellen stammen, da diese häufig nur von US-Unternehmen bereitgestellt werden. Einseitige Datenquellen können das Modell verzerren und zu einer Über- oder Unterbewertung bestimmter Branchen oder Regionen führen, obwohl die Risiken global unterschiedlich ausgeprägt sind. Ebenso ist darauf zu achten, dass die verschiedenen Unternehmensgrößen, Digitalisierungsgrade und regionale Bedrohungsprofile ausreichend repräsentiert sind, um systematische Verzerrungen zu vermeiden.

Ein Bias entsteht unter anderem durch die selektive Datengrundlage, wenn etwa Unternehmen mit bestimmten IT-Sicherheitsniveaus über- oder unterrepräsentiert sind. Dies könnte etwa der Fall sein, wenn nur besonders gut abgesicherte oder ausschließlich stark betroffene Organisationen Daten bereitstellen würden. Ohne geeignete Maßnahmen zur Diversifizierung besteht das Risiko, dass das Modell branchenspezifische Risiken nicht objektiv lernt.

Um die Heuristik zu evaluieren und stetig zu verbessern, ist der Cyber-Risiko-Score darauf angewiesen, dass sich zahlreiche Unternehmen aktiv testen lassen, um eine ausreichende Datengrundlage aufzubauen.

Die zuvor beschriebene Heuristik bildet ein unmittelbar einsetzbares Fundament für den Cyber-Risiko-Score. Die wahre Stärke und der langfristige strategische Wert des CRS liegen jedoch in seiner Weiterentwicklung zu einem prädiktiven, selbstlernenden Analysemodell. Regelbasierte Scoring-Logiken ermöglichen heute bereits eine transparente und deterministische Bewertung von IT-Sicherheitsmängeln. Der Nutzen dieses Modells steigt jedoch exponentiell an, sobald es zusätzlich prädiktive Muster, Risikodynamiken und latente Zusammenhänge erkennen kann, die heuristisch nicht explizit modelliert wurden. Die größte Herausforderung für ein prädiktives Sicherheitsmodell ist die Verfügbarkeit von Trainingsdaten. Besonders im Kontext der Cybersicherheit sind geeignete Datensätze oft fragmentiert, sensibel oder gar nicht in ausreichender Tiefe öffentlich verfügbar, obwohl sie für die Modellgüte entscheidend wären.

Das langfristige Ziel besteht darin, das regelbasierte Modul mithilfe von ausreichend gesammelten Trainingsdaten durch ein trainiertes

Bild: Deemerwha studio - stock.adobe.com

Machine-Learning-(ML)-Modell zu ersetzen. Um dieses Ziel datenschutzkonform und skalierbar zu erreichen, bietet sich der Einsatz von Federated Learning an. Das zukünftige Machine-Learning-Modell wird dezentral innerhalb der IT-Umgebungen teilnehmender Organisationen trainiert, ohne dass sicherheitskritische Rohdaten zentral gesammelt oder übertragen werden müssen. Federated Learning schafft damit eine strategische Grundlage, um den Cyber-Risiko-Score langfristig zu einem selbstlernenden, prädiktiven und anonym datenoptimierten Sicherheitsmodell weiterzuentwickeln.

FAZIT

Cyberrisiko-Scoring-Modelle sind keine neue Entwicklung. Große Unternehmen nutzen bereits eigene Modelle, um ihre IT-Sicherheit messbar zu machen. Für die meisten anderen Organisationen bleibt diese Möglichkeit jedoch verschlossen: Die existierenden Modelle sind unternehmensspezifisch zugeschnitten und nicht öffentlich zugänglich.

Der Cyber-Risiko-Score soll hier Abhilfe schaffen: Auch kleinen und mittelständischen Unternehmen soll es möglich sein, ihre IT-Sicherheit einfach zu messen. Der Fokus liegt deshalb bewusst auf einer nicht-invasiven, leicht umsetzbaren Bewertung, die bestehende IT-Prozesse nicht stört.

Der entwickelte Score dient als Metrik zur Vergleichbarkeit der IT-Sicherheit unterschiedlicher Unternehmen. Voraussetzung ist die Standardisierung des Scoring-Modells. Nur durch einheitliche Bewertungslogiken, Mängelkategorien und Gewichtungen entsteht eine faire, nachvollziehbare und sektorübergreifende Vergleichbarkeit.

Eine Standardisierung des Cyber-Risiko-Score wäre zudem ein Schritt zur Stärkung der deutschen IT-Sicherheits-Souveränität – viele Frameworks und darauf aufbauende Modelle stammen aus den USA. Ein offener, standardisierter deutscher Score kann langfristig ein interoperables Ökosystem ermöglichen, in dem Sicherheitsbenchmarks, Branchenanalysen und ML-basierte Risiko-Prognosen auf einer gemeinsamen Methodik aufbauen – statt auf proprietären Insellösungen.

Zudem stärkt Standardisierung die digitale Resilienz des Mittelstands, erleichtert Audit-Prozesse, verbessert die Messbarkeit von Security-Investitionen und schafft die Grundlage für vertrauenswürdige und anonymisierte Lernarchitekturen. ■

Literatur

[1] *Statista, „Ausgaben für IT-Sicherheit in Deutschland bis 2026", Statista, 28. November 2025. https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/*

[2] *I. D. Sánchez-García, J. Mejía und T. S. F. Gilabert, „Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation", Applied Sciences, Bd. 13, Nr. 1, S. 395, Dez. 2022, doi: 10.3390/app13010395. https://doi.org/10.3390/app13010395*

[3] *M. Ekstedt, Z. Afzal, P. Mukherjee, S. Hacks und R. Lagerström, „Yet another cybersecurity risk assessment framework", International Journal Of Information Security, Bd. 22, Nr. 6, S. 1713–1729, Juli 2023, doi: 10.1007/s10207-023-00713-y. https://doi.org/10.1007/s10207-023-00713-y*

[4] *P. Katsumata, J. Hemenway and W. Gavins, „Cybersecurity risk management," 2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, San Jose, CA, USA, 2010, pp. 890-895, doi: 10.1109/MILCOM.2010.5680181. https://ieeexplore.ieee.org/document/5680181*

[5] *J. Hughes und G. Cybenko, „Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity", Technology Innovation Management Review, Bd. 3, S. 15–24, Aug. 2013, doi: 10.22215/timreview/712. https://www.researchgate.net/publication/326311568_Quantitative_Metrics_and_Risk_Assessment_The_Three_Tenets_Model_of_Cybersecurity*

[6] *Ö. Söner, G. Kayisoglu, P. Bolat und K. Tam, „Cybersecurity risk assessment of VDR", Journal Of Navigation, Bd. 76, Nr. 1, S. 20–37, Jan. 2023, doi: 10.1017/S0373463322000595. https://www.cambridge.org/core/journals/journal-of-navigation/article/abs/cybersecurity-risk-assessment-of-vdr/8C1F2DEA2F6FA516526B8804C5B07DBC*

[7] *Z. M. King, D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman und C. Sample, „Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment", Frontiers in Psychology, Bd. 9, S. 39, Feb. 2018, doi: 10.3389/fpsyg.2018.00039. https://doi.org/10.3389/fpsyg.2018.00039*

[8] *A. Fielder, S. König, E. Panaousis, S. Schauer und S. Rass, „Risk assessment uncertainties in cybersecurity investments", Games, Bd. 9, Nr. 2, S. 34, Juni 2018, doi: 10.3390/g9020034. https://doi.org/10.3390/g9020034*

[9] *„CyberRisikoCheck", Bundesamt für Sicherheit in der Informationstechnik (Zugriff am: 18.01.2026). https://www.bsi.bund.de/dok/crc*

[10] *„IT-Sicherheit auch für KMU", BSI Lagebericht 2025 (Zugriff am: 18.01.2026). https://medien.bsi.bund.de/lagebericht/de/it-sicherheit-fuer-kmus/*

[11] *„4.3 Risiken bewerten", Bundesamt für Sicherheit in der Informationstechnik (Zugriff am: 18.01.2026). https://www.bsi.bund.de/dok/6611132*

[12] *„What is EPSS (Exploit Prediction Scoring System)?", Bitsight, 30. September 2025 (Zugriff am: 18.01.2026). https://www.bitsight.com/glossary/epss-exploit-prediction-scoring-system#:~:text=Exploit%20Prediction%20Scoring%20System%20(EPSS)%20is%20a,pose%20the%20greatest%20threat%20to%20their%20organizations*

[13] *„Known Exploited Vulnerabilities Catalog", Cybersecurity and Infrastructure Security Agency (Zugriff am: 18.01.2026). https://www.cisa.gov/known-exploited-vulnerabilities-catalog*

MERT AYAS
studiert den Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Ganzheitliche und einheitliche Risikobewertung der Unternehmens-IT – Cyber-Risiko-Score".

FERHAN KESICI
studiert den Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Ganzheitliche und einheitliche Risikobewertung der Unternehmens-IT – Cyber-Risiko-Score".

DENNIS STROZ
studiert den Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Ganzheitliche und einheitliche Risikobewertung der Unternehmens-IT – Cyber-Risiko-Score".

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.

VORSCHAU Ausgabe 2|26 APRIL/ MAI

SCHWERPUNKT: OT-Security – Cyberresilienz für Industrie und Versorgung

Operational Technology ist das Herz moderner Industrie – und zugleich eine der verwundbarsten Zonen digitaler Wertschöpfung. Legacy-Systeme, lange Lebenszyklen, proprietäre Protokolle und ein hoher Vernetzungsdruck machen OT-Umgebungen zum bevorzugten Ziel professioneller Angreifer. Gleichzeitig steigen die regulatorischen Anforderungen durch NIS-2, CRA und sektorspezifische Standards.

Das kommende Heft widmet sich daher der Frage, wie Industrie, Energieversorger und Betreiber kritischer Infrastrukturen ihre OT-Landschaften widerstandsfähig machen können. Im Schwerpunkt erwarten Sie unter anderem:

- Spezifische OT-Herausforderungen: Warum veraltete Anlagen, unsichere Feldbusprotokolle und hybride IT/OT-Netze neue Risikoarchitekturen erfordern.
- Segmentierung und Zugriffskontrolle in industriellen Netzwerken: von Zonenmodellen über Zero Trust in der OT bis hin zu sicheren Remote-Access-Konzepten für Wartungsfirmen
- Firewalls und IDS/IPS für OT-Umgebungen: Welche Lösungen haben sich etabliert, wie funktioniert industrielle Anomalieerkennung – und wie lassen sich IT-Security-Tools in OT-Prozesse integrieren?
- Business Continuity und Notfallplanung: von Redundanzstrategien über Krisenkommunikation bis hin zu Wiederanlauf-Szenarien für Produktionsanlagen
- Best Practices und Standards: IEC 62443, ISO 27019, branchenspezifische Vorgaben – und wie Unternehmen diese pragmatisch implementieren.

Weitere Beiträge in der Ausgabe:

- Überblick Cyber Resilience Act (CRA)
- Dreiklang KI, IT, IoT
- Mythos Innovationsbremse: eine Verteidigung des EU AI Acts

Erscheinungstermin: 13. April 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)

32. Jahrgang 2026 · ISSN: 1868-5757

Wir erreichen Verantwortliche für die IT-Sicherheit

- Newsletter
- Content-Marketing
- Webinare & Webkonferenzen

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

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