2026 /// WWW.DIGITALBUSINESS-MAGAZIN.DE

D, A, CH: 11,50 | weitere EU-Länder: 13,70 | ISSN 2510-344X

DIGITAL BUSINESS

EXPERTENMAGAZIN FÜR DIGITALE TRANSFORMATION

SONDERHEFT SECURITY

Eine Publikation der WIN Verlag GmbH & Co. KG |

EU-Richtlinie NIS2

Neues Denken über Informationssicherheit

ZERO-TRUST

Wie KI-gestütztes Identity & Access Management den kompromisslosen Schutz vor Deepfake-Identitäten meistert.

SOVEREIGN AI

Nur die konsequente Begrenzung der Zugriffsrechte auf das wirklich Notwendige legt Agenten an die kurze Leine.

ADVANCED CYBER DEFENSE

Warum konsolidierte Detektion und automatisierte Response den Unterschied zwischen Incident und Desaster machen.

TAROX

VERSTEHEN.
ABSICHERN.
HANDELN.

Cyber-Resilienz ist das neue Fundament für Business-Kontinuität. NIS2 setzt den regulatorischen Rahmen – entscheidend ist jedoch, wie gut Ihr Unternehmen darauf vorbereitet ist.

Wir unterstützen Sie dabei, Vorbereitung in Stärke zu verwandeln:

- → Risiken strukturiert zu analysieren und zu verstehen
- → Sicherheitsmaßnahmen strategisch aufzubauen
- → im Ernstfall handlungsfähig zu bleiben

Machen Sie Resilienz zu Ihrem Wettbewerbsvorteil – nicht erst im Krisenfall.

Mehr erfahren auf tarox.de

Bitdefender ENGINSIGHT HORNETSECURITY BY proofpoint.

EDITORIAL

Liebe Leserin, lieber Leser

vielleicht kennen Sie das klassische Märchen vom Hasen und dem Igel? Der Hase hält sich für unschlagbar schnell und fordert den vermeintlich behäbigen Igel zum Wettlauf auf dem Feld heraus. Was er nicht weiß: Der Igel hat sich vorher clever positioniert: Seine Frau, ihm zum Verwechseln ähnlich, wartet bereits am anderen Ende der Ackerfurche. Bei jedem Durchlauf ruft einer der beiden „Ick bün all hier" – bis der Hase nach dem vielen Hin-und-Her-Rennen erschöpft zusammenbricht. Die Pointe ist nicht, dass der Igel schwindelt. Sondern, dass er gewinnt, weil er an jedem Punkt der Strecke bereits präsent ist, während der Hase auf rohes Tempo setzt.

Schwachstellen in Millisekunden finden

Wer heute Unternehmensnetzwerke verteidigt, kennt dieses Gefühl. Angreifer nutzen KI, um in Millisekunden Schwachstellen zu finden, Stimmen zu klonen und Angriffe zu automatisieren. Wer als Verteidiger versucht, diesem Tempo hinterherzurennen, verliert wie der Hase: erschöpft und stets einen Schritt zu spät. Die eigentliche Lehre des Märchens ist deshalb keine Beruhigungspille, sondern eine Strategie: Nicht schneller sein als der Angreifer, sondern an jedem relevanten Punkt der Angriffsfläche bereits vorbereitet stehen – durch Automatisierung, durch 24/7-Abdeckung, durch Prävention statt Reaktion.

Der KI-Wettlauf-Check als roter Faden

Genau das greift unser Security-Tachometer auf, der Sie durch dieses Heft begleitet. An den passenden Stellen zeigen wir im direkten Vergleich, wo der Hase – also die Angreiferseite – die Nase vorn hat, und wo der Igel längst an Ort und Stelle wartet: bei automatisierter Bedrohungserkennung, bei Identitätsschutz gegen Deepfakes, bei selbstheilenden Systemen. Die KI_Wettlauf-Grafik ist bewusst keine exakte Momentaufnahme, sondern eine spielerische Einladung zur Selbstprüfung: Steht Ihr Unternehmen schon am Ziel, bevor der Angriff überhaupt gestartet ist?

Kompetenz aus der Praxis

Von der Titelstrecke über Zero Trust und digitale Souveränität bis zur Vision 2030 zieht sich dieser Gedanke durch alle Kapitel. Unser Expertentalk versammelt kompetente Stimmen aus der Praxis, die genau diese Frage beantworten: Welcher Trick lässt Sie schon dort stehen, wo der Angriff erst hinwill? Und unsere Sicherheits-Agenda 2027 übersetzt all das in eine konkrete Checkliste. Denn das nächste Budgetgespräch kommt bestimmt.

Auch dafür sind Sie mit dieser Ausgabe bestens gewappnet. Denn wie schon gesagt: Der Hase mag schneller sein. Aber der Igel war schon immer da, wo es zählte.

Lassen Sie sich inspirieren und bleiben Sie gesund.

Ihr

HEINER SIEGER, Chefredakteur
DIGITAL BUSINESS
heiner.sieger@win-verlag.de

HUMAN RISK MANAGEMENT
18 **Der Mensch delegiert, das Risiko bleibt**
Fehler, Fehlkonfigurationen oder missbräuchliche Zugriffe können sich automatisiert und schnell über verbundene Systeme ausbreiten.

ZERO-TRUST & IDENTITY FIRST SECURITY
22 **Der Spagat**
Da Angreifer mit generativer KI Schwachstellen ausnutzen, müssen IT-Security-Teams fortlaufend prüfen, wer hinter einer Sitzung steht.

06

Titelstory / Compliance, Governance, Resilience

NIS2 zwingt Unternehmen zum Umdenken:
Informationssicherheit wird zur Pflicht. Ein digitales ISMS bringt Cybersecurity direkt in den Arbeitsalltag – effizient, sicher und praxisnah.

ADVANCED CYBER DEFENSE
46 **Die Kontext-Lücke**
Erst die Verknüpfung mit Endpoint, Cloud-Umgebung und Netzwerk zeigt, ob aus einem Klick ein Sicherheitsvorfall oder eine Krise wird.

SOVEREIGN AI & PRIVATE LLMS
54 **Agenten an die kurze Leine legen**
Nicht die Leistungsfähigkeit eines Agenten entscheidet über seine Sicherheit, sondern die konsequente Begrenzung seiner Zugriffsrechte.

SECURE COMMUNICATIONS

42 **Chefsache Dokumentenaustausch**
Sichere Geschäftskommunikation entsteht nicht durch einzelne Funktionen, sondern durch das Zusammenspiel integrierter Prozesse.

DIGITAL BUSINESS

Sonderheft Security 2026

COMPLIANCE, GOVERNANCE & RESILIENCE

06 KI ersetzt keine Security-Experten
08 NIS2 erfüllt, Sicherheit gewonnen: Das Potenzial eines digitalen ISMS
12 Digital Trust braucht Beweise: KI ohne Zertifizierung funktioniert nicht
14 Experten-Talk: Wer gewinnt den KI-Wettlauf 2026?

HUMAN RISK MANAGEMENT

18 Der Mensch delegiert, das Risiko bleibt
20 Human Risk Management im KI-Zeitalter

ZERO-TRUST & IDENTITY-FIRST SECURITY

22 Identität: Der Spagat zwischen Nutzererlebnis und Deepfake-Abwehr
24 Von Legacy zu „Never Trust, Always Verify"

ENDPOINT, HARDWARE & AI-INFRASTRUCTURE

26 Die dunkle Seite der Autonomie
28 Von Zero Trust zu Zero Trust Plus: Vertrauen allein reicht nicht mehr
30 Der resiliente Arbeitsplatz kennt keinen festen Standort
32 VS-NfD sorgenfrei mobil bearbeiten
34 Raus aus der Kill-Switch-Falle

DIGITAL SOVEREIGNTY & CLOUD INFRASTRUCTURE

36 So stoppen Unternehmen Cyberangriffe in Minuten statt Tagen
38 Mehr als Firewalls: Was Rechenzentren resilient macht
40 Identitäten als Compliance-Pflicht

SECURE COMMUNICATIONS & COLLABORATION

42 Digitale Business Compliance: Warum sicherer Dokumentenaustausch zur Chefsache wird

POST QUANTUM CRYPTOGRAPHY

44 „2030 ist keine Zukunft mehr“

ADVANCED CYBER DEFENSE & INCIDENT RESPONSE

46 Die Kontext-Lücke: Warum separierte Tools zum Desaster führen
48 Warum XDR zum Effizienzfaktor in der IT-Sicherheit wird
50 Keine Pause für die Cyberabwehr
52 Wie Unternehmen Compliance für Cyberversicherungen erreichen

SOVEREIGN AI & PRIVATE LLMS

54 Agenten an die kurze Leine legen
56 KI ohne Kontrollverlust

SUPPLY CHAIN SECURITY & SBOM

58 SBOM: Warum Sichtbarkeit allein nicht schützt

60 Security Agenda 2027
62 Vision 2030: Das autonome Immunsystem

03 Editorial
63 Impressum

KI ersetzt keine Security-Experten

Security Operations ohne Automatisierung stoßen an ihre Grenzen. Warum KI dabei aber „nur“ zum Enabler und nicht zum Ersatz für Experten wird und wo der Mensch die Kontrolle behalten muss, erklärt Thimo Holst, Head of Brand Strategy der it-sa Expo&Congress. /// von Heiner Sieger

Herr Holst, die it-sa ist der Seismograph der Branche. Wenn Sie auf die aktuelle Bedrohungslage im Herbst 2026 blicken: Haben wir den Übergang von der reaktiven IT-Sicherheit zur proaktiven Cyber-Resilienz im Mittelstand mittlerweile geschafft, oder hinken die Unternehmen der Realität noch hinterher?
Thimo Holst | Wir sehen durchaus Fortschritte. Viele mittelständische Unternehmen haben erkannt, dass IT-Sicherheit heute kein reines IT-Thema mehr ist, sondern ein wesentlicher Bestandteil der Unternehmensstrategie. Themen wie Business Continuity, Incident Response oder Cyber-Resilienz stehen deutlich stärker im Fokus als noch vor wenigen Jahren.

Gleichzeitig wäre es verfrüht zu sagen, der Wandel sei abgeschlossen. Die Bedrohungslage entwickelt sich mit hoher Geschwindigkeit weiter. Gerade durch den Einsatz von KI auf Angreiferseite steigen Reichweite und Professionalität von Cyberangriffen. Viele Unternehmen bauen ihre Schutzmaßnahmen aus, kämpfen aber weiterhin mit begrenzten Ressourcen, komplexen IT-Landschaften und regulatorischen Anforderungen. Deshalb lautet die zentrale Aufgabe heute: Sicherheit von Anfang an mitdenken und Resilienz kontinuierlich weiterentwickeln. Die gute Nachricht ist, dass das Bewusstsein dafür im Mittelstand deutlich gewachsen ist.

Die Umsetzungsfristen für NIS2 und den EU AI Act fordern die Unternehmen massiv. Ist Regulierung für den Mittelstand aktuell eher ein wirksamer Schutzwall oder ein schier unüberwindbarer bürokratischer Berg?
TH | Regulierung wird häufig zunächst als Belastung wahrgenommen. Tatsächlich bedeuten neue Vorgaben zunächst zusätzlichen Aufwand, insbesondere für mittelständische Unternehmen ohne große Compliance-Abteilungen. Langfristig sehe ich NIS2 und den AI Act jedoch als wichtige Orientierungshilfe. Sie schaffen klare Anforderungen, fördern ein einheitliches Sicherheitsniveau und helfen Unternehmen dabei, Risiken systematisch zu identifizieren und zu adressieren. Entscheidend ist, Regulierung nicht als isolierte Pflichtübung zu betrachten, sondern als Teil einer nachhaltigen Sicherheitsstrategie.

Auf der it-sa erleben wir, dass viele Unternehmen den Austausch mit Experten suchen, um genau diese Vorgaben praxisnah umzusetzen. Hier zeigt sich, wie wichtig Plattformen für Wissenstransfer und Erfahrungsaustausch sind. Die it-sa versteht sich als „Home of IT Security“ und bietet dafür den passenden Rahmen.

Wir beobachten im Markt einen permanenten Wettlauf: Angreifer nutzen KI in Lichtgeschwindigkeit („der Hase“), während Unternehmen durch Prozesse und Compliance gebremst werden („der Igel“). Wie kann der Mittelstand diesen Geschwindigkeitsnachteil ausgleichen, ohne die Kontrolle zu verlieren?
TH | Unternehmen werden Angreifer nie dadurch schlagen, dass sie einfach nur schneller werden. Entscheidend ist, intelligenter zu werden. Das bedeutet, Prozesse zu automatisieren, Risiken zu priorisieren und Entscheidungen auf einer soliden Datenbasis zu treffen.

KI kann dabei ein entscheidender Hebel sein. Sie unterstützt beispielsweise bei der Erkennung von Anomalien, der Analyse von Sicherheitsereignissen oder der Priorisierung von Warnmeldungen. Gleichzeitig müssen Unternehmen nachvollziehbare Prozesse und klare Verantwortlichkeiten beibehalten. Automatisierung darf nicht zu einem Kontrollverlust führen.

Ich denke, die erfolgreichsten Unternehmen werden diejenigen sein, die das Beste aus beiden Welten kombinieren: die Geschwindigkeit moderner Technologien und die strategische Steuerung durch den Menschen.

Der Fachkräftemangel in der IT-Security ist chronisch. Auf der it-sa sehen wir immer mehr Automatisierungs- und

XDR-Ansätze. Erleben wir gerade den Wendepunkt, an dem Security Operations ohne KI-gestützte Automatisierung überhaupt nicht mehr machbar sind?
TH | In vielen Bereichen erleben wir diesen Wendepunkt bereits. Die Menge an Sicherheitsdaten, Alarmen und potenziellen Angriffen ist so groß geworden, dass rein manuelle Prozesse an ihre Grenzen stoßen.

Automatisierung und moderne XDR-Plattformen helfen dabei, Sicherheitsereignisse effizienter zu korrelieren und schneller zu reagieren. KI wird dabei zunehmend zum Enabler. Sie ersetzt jedoch keine Security-Experten. Vielmehr ermöglicht sie ihnen, sich auf komplexe Analysen und strategische Aufgaben zu konzentrieren.

Der Fachkräftemangel wird uns noch lange begleiten. Deshalb wird intelligente Automatisierung künftig nicht nur ein Wettbewerbsvorteil, sondern in vielen Unternehmen eine Grundvoraussetzung für effektive Sicherheitsarbeit sein.

Das Thema „Souveräne Cloud" und der Wunsch nach Unabhängigkeit von außereuropäischen Hyperscalern treibt viele um. Spüren Sie auf der Messe ein echtes Umdenken hin zu europäischen Lösungen, oder siegt am Ende doch meist der Preis und die Bequemlichkeit?
TH | Das Interesse an digitaler Souveränität hat in den vergangenen Jahren spürbar zugenommen. Themen wie Datensouveränität, Resilienz und geopolitische Abhängigkeiten beschäftigen inzwischen nicht mehr nur Behörden oder kritische Infrastrukturen, sondern weite Teile der Wirtschaft. Auf der it-sa beobachten wir daher ein wachsendes Interesse an europäischen Anbietern und souveränen Cloud-Konzepten. Gleichzeitig treffen Unternehmen ihre Entscheidungen weiterhin auf Basis verschiedener Faktoren. Neben Sicherheits- und Compliance-Aspekten spielen Wirtschaftlichkeit, Skalierbarkeit und bestehende Ökosysteme natürlich eine wichtige Rolle.

Es geht deshalb zunehmend nicht um ein entweder-oder, sondern um die Frage, wie sich Sicherheitsanforderungen, Souveränität und wirtschaftliche Rahmenbedingungen sinnvoll miteinander verbinden lassen.

KI agiert immer autonomer. Welche neuen Sicherheitsrisiken bringt das für die Unternehmens-Infrastruktur mit sich – und wo muss die Abwehr ansetzen, direkt auf der Hardware oder in der Cloud?
TH | Mit zunehmender Autonomie von KI-Systemen steigt auch die Komplexität der Risikolandschaft. Unternehmen müssen sich mit neuen Angriffsszenarien beschäftigen, etwa der Manipulation von Trainingsdaten, kompromittierten Modellen oder missbräuchlich genutzten KI-Agenten. Deshalb darf Sicherheit nicht erst an einer einzelnen Stelle ansetzen. Notwendig ist ein ganzheitlicher Ansatz über die gesamte Wertschöpfungskette hinweg. Dazu gehören sichere Hardware, geschützte Infrastrukturen, vertrauenswürdige Datenquellen, robuste Identitäts- und Zugriffsmodelle sowie kontinuierliches Monitoring.

Die Frage lautet daher weniger „Hardware oder Cloud", sondern vielmehr „Hardware und Cloud". Sicherheitskonzepte müssen künftig alle Ebenen gleichermaßen berücksichtigen.

Wenn Sie den Ausblick auf das kommende Jahr 2027 wagen: Was ist das eine Thema, mit dem sich jeder Geschäftsführer und CISO jetzt sofort beschäftigen muss, um im nächsten Jahr nicht kalt erwischt zu werden?
TH | Wenn ich mich auf ein Thema festlegen müsste, dann wäre es die sichere und strategische Integration von Künstlicher Intelligenz in Unternehmensprozesse.

KI wird in den kommenden Jahren nahezu alle Geschäftsbereiche verändern. Wer ihre Potenziale nicht nutzt, verliert an Wettbewerbsfähigkeit. Wer sie unkontrolliert einsetzt, schafft neue Risiken. Genau dieses Spannungsfeld wird Unternehmen 2027 beschäftigen. Geschäftsführer und CISOs sollten deshalb bereits heute Governance-Strukturen, Sicherheitsrichtlinien und Kompetenzaufbau rund um KI etablieren. Die zentrale Frage wird nicht mehr sein, ob Unternehmen KI einsetzen, sondern wie sie dies sicher, verantwortungsvoll und wirtschaftlich erfolgreich tun.

DER GESPRÄCHSPARTNER
Thimo Holst
ist Head of Brand Strategy it-sa Expo&Congress.

> „ Intelligente Automatisierung wird künftig nicht nur ein Wettbewerbsvorteil, sondern in vielen Unternehmen eine **Grundvoraussetzung für effektive Sicherheitsarbeit** sein.
>
> *Thimo Holst*

Die it-sa Expo&Congress als Europas führende Fachmesse für IT-Sicherheit bringt dazu die relevanten Anbieter, Experten und Anwender zusammen und zeigt Jahr für Jahr, welche Lösungen und Strategien den Markt bewegen. •

NIS2 erfüllt, Sicherheit gewonnen: Das Potenzial eines digitalen ISMS

NIS2 zwingt Unternehmen zum Umdenken: Informationssicherheit wird zur Pflicht. Ein digitales ISMS bringt Cybersecurity direkt in den Arbeitsalltag – effizient, sicher und praxisnah. Wie das gelingt, zeigt ConSense GmbH mit seiner Lösung ConSense GRC, die sich bereits beim österreichischen Biopharma-Unternehmen Single Use Support bewährt hat. /// von Dr. Stephan Killich

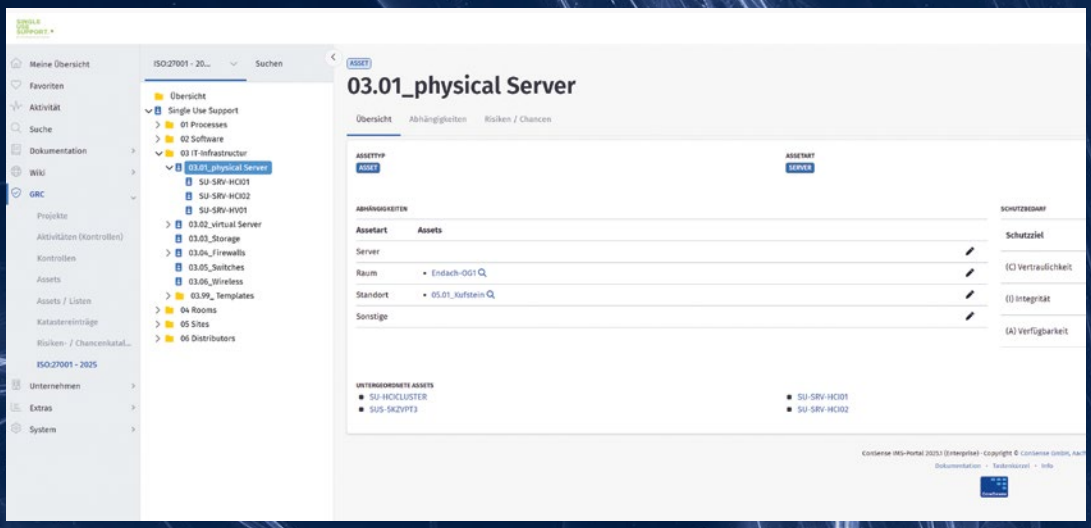
> Die Uhr tickt: **Um Bußgelder zu vermeiden, sind die Betriebe gefordert**, schnell für klare Zuständigkeiten, ausreichende Ressourcen und eine kontinuierliche Überprüfung der Sicherheitsmaßnahmen zu sorgen.
>
> *Dr. Stephan Killich*

DER AUTOR
Dr. Stephan Killich
ist Mitglied der Geschäftsführung der ConSense GmbH.
Bild: Consense

EIN ARBEITSTAG, AN DEM ALLES ANDERS LÄUFT ALS GEPLANT: Mitarbeitende können nicht auf zentrale Systeme zugreifen, wichtige Daten sind verschlüsselt und Prozesse stehen still. Ein solches Szenario gehört heute zu den realen Risiken vieler Unternehmen. Daten sind längst zu einem entscheidenden Wirtschaftsfaktor geworden. Damit steigt auch ihre Gefährdung. Cyberangriffe treffen längst nicht mehr nur internationale Konzerne, auch mittelständische Unternehmen geraten zunehmend ins Visier von Angreifern. Die Folgen gehen weit über technische Störungen hinaus. Unternehmen müssen sich deshalb nicht nur fragen, wie sie technische Schutzmaßnahmen verbessern können, sondern auch, wie sie Informationssicherheit dauerhaft in ihren Arbeitsabläufen verankern können.

NIS2 erhöht den Handlungsdruck

Mit dem EU-Cybersecurity-Package gewinnt dieses Thema zusätzlich an Bedeutung. Die verbindliche EU-Richtlinie NIS2 erweitert den Kreis der betroffenen Unternehmen, erhöht die Anforderungen und rückt technische Maßnahmen und organisatorische Prozesse gleichermaßen in den Mittelpunkt. Neben präziseren Regelungen zum Geltungsbereich umfasst die Richtlinie neue Kategorien wie die sogenannten „Small Mid-Caps“ – mittelgro-



oben:
Single Use Support GmbH
Systematischer Aufbau des Informationssicherheits-Managements mithilfe von ConSense GRC: Alle Informationen für Audits mit wenigen Klicks verfügbar, schnelle Zertifizierung nach ISO 27001.

links:
Single Use Support GmbH
Systematisches Risikomanagement mit ConSense GRC im Integrierten Managementsystem: Assets, zum Beispiel Geräte, werden digital erfasst, Risiken bewertet, Maßnahmen zugewiesen und dokumentiert.

ße Unternehmen mit bis zu 750 Beschäftigten – sowie zusätzliche sektorbezogene Anforderungen, zum Beispiel für Energie, Gesundheit, Wasserstoff oder Chemie. Insbesondere mittelständische Unternehmen geraten dadurch stärker in den Kreis der betroffenen Branchen. Das verpflichtet sie, angemessene organisatorische und technische Maßnahmen für mehr Cybersicherheit zu ergreifen. Dazu gehören unter anderem ein systematisches Risikomanagement, klare Verantwortlichkeiten und nachweisbare Sicherheitsprozesse. Zudem stehen Führungskräfte künftig stärker in der Verantwortung. Damit verändert sich insgesamt die Rolle der Informationssicherheit: Sie ist nicht länger nur ein technisches Thema der IT-Abteilung, sondern wird zur Aufgabe der Unternehmenssteuerung.

Seit dem 6. März 2026 ist nun die Registrierungsfrist für Unternehmen, die von der verbindlichen EU-Richtlinie NIS2 für mehr Cybersicherheit betroffen sind, offiziell abgelaufen. Dass sich von ihnen bisher nur ein Teil registriert hat, belegt die herrschende Unsicherheit. Doch die Uhr tickt: Um Bußgelder zu vermeiden, sind die Betriebe gefordert, schnell für klare Zuständigkeiten, ausreichende Ressourcen und eine kontinuierliche Überprüfung der Sicherheitsmaßnahmen zu sorgen. Gerade kleinere und mittlere Organisationen verfügen jedoch häufig nicht über die notwendigen Strukturen, um Informationssicherheit systematisch zu steuern.

Moderne Software-Lösungen wie die der Aachener ConSense GmbH unterstützen dabei wirkungsvoll. ConSense entwickelt Software zum Aufbau moderner Qualitätsmanagementsysteme (QMS) und Integrierter Managementsysteme (IMS) und hat sich auf die neuen Herausforderungen rund um die Informationssicherheit eingestellt. Mit ConSense GRC stellt das Unternehmen eine Lösung zum Aufbau eines effizienten Informationssicherheits-Managementsystems (ISMS) bereit, das sich in bestehende Strukturen integrieren lässt. „Der Fokus liegt dabei nicht nur auf der Technik. Entscheidend ist, dass Sicherheitsprozesse von den Mitarbeitenden verstanden, akzeptiert und im Alltag gelebt werden“, sagt Harald Lenders, Senior Reklamations- und Incident Manager bei der ConSense GmbH.

Vom Einzelwerkzeug zum Integrierten Managementsystem

Viele Unternehmen arbeiten heute mit unterschiedlichen Systemen für einzelne Anforderungen: Qualitätsmanagement, Datenschutz, Compliance oder Informationssicherheit werden getrennt betrachtet. Dadurch entstehen oft doppelte Arbeit, Medienbrüche und fehlende Transpa-

Single Use Support GmbH
Einführung von ConSense GRC bei Single Use Support: Einbindung des Informationssicherheits-Managements in das bestehende QMS auf Basis von ConSense GxP.

renz. ConSense verfolgt hier einen anderen Ansatz. Die Software-Lösungen der Aachener Entwickler führen verschiedene Managementbereiche in einem Integrierten Managementsystem zusammen. Informationen sind damit übergreifend verfügbar, Verantwortlichkeiten werden zentral gesteuert und Synergien werden genutzt.

Mit ConSense GRC, der Software-Lösung für Governance, Risk & Compliance, können Unternehmen ein ISMS strukturiert aufbauen und weiterentwickeln. Anforderungen aus Standards wie der NIS2-Richtlinie oder der ISO 27001 lassen sich mit organisatorischen Strukturen und konkreten Maßnahmen verbinden. Ein zentraler Bestandteil von ConSense GRC ist das Asset-Management. Unternehmen erhalten damit einen Überblick über schutzrelevante Werte, zum Beispiel Systeme, Anwendungen oder Geräte. Die vorhandenen Assets werden systematisch erfasst und ihre Schutzwürdigkeit eingestuft. Darauf aufbauend lassen sich Risiken bewerten, Maßnahmen festlegen und Fortschritte nachvollziehen. Automatisierte Workflows und Erinnerungsfunktionen helfen dabei, festgelegte Abläufe zuverlässig einzuhalten. Im System sind Verantwortlichkeiten transparent hinterlegt, Dokumentationen werden nachvollziehbar gepflegt.

„Ein digitales ISMS ist damit kein zusätzlicher bürokratischer Aufwand, sondern schafft Orientierung. Es legt eindeutige Zuständigkeiten und klare Maßnahmen fest und unterstützt dabei, Risiken systematisch zu erkennen, zu bewerten und steuerbar zu machen. Dabei geht es nicht nur um Firewalls und Zugriffsberechtigungen, sondern vor allem um die Frage, wie sich Sicherheitskultur ganzheitlich im Unternehmen verankern lässt“, so Experte Harald Lenders.

Praxisbeispiel Single Use Support: In kurzer Zeit zur ISO 27001-Zertifizierung

Wie ein solcher Ansatz in der Praxis funktioniert, zeigt die österreichische Single Use Support GmbH aus Kufstein. Das biopharmazeutische Unternehmen entwickelt Single-Use-Systeme für die Herstellung von Medikamenten und arbeitet in einem streng regulierten Umfeld. Mit dem starken Wachstum des Unternehmens – innerhalb von vier Jahren stieg die Zahl der Mitarbeitenden von 50 auf 220 an – vermehrten sich auch die Anforderungen an Dokumentation und Compliance. Die bisherigen Lösungen reichten nicht mehr aus, um die notwendige Transparenz für Audits und Zertifizierungen sicherzustellen. Darum setzte das Unternehmen zunächst im Qualitätsmanagement auf die Softwarelösung ConSense GxP, mit denen sich die besonderen Anforderungen von Unternehmen aus streng regulierten Branchen effizient und transparent managen lassen. „Mit Excel und Word konnten wir irgendwann einfach nicht mehr die Transparenz und Nachvollziehbarkeit sicherstellen, die wir für Zertifizierungen und Audits brauchen. Daher wollten wir ein digitales System, das verschiedene Managementthemen abbildet und mit uns wächst“, erzählt Markus Lentsch, Leiter IT und Information Security Officer bei Single Use Support.

Als die Informationssicherheit immer stärker in den Fokus rückte, ergänzte Single Use Support das bestehende System um ConSense GRC. Vor der Einführung der Software-Lösung war das Risikomanagement des Unternehmens eine Sammlung aus Tabellen, Dateien und teilweise auch Papierdokumenten. „Das hat funktioniert, solange wir klein waren, aber mit zunehmender Komplexität wurde die Gefahr von Fehlern zu groß“, sagt Markus Lentsch. Heute laufen alle Informationen auf einer zen-

tralen Plattform, dem Integrierten Managementsystem auf Basis von ConSense Software, zusammen: Assets wie Serverräume, Applikationen oder Geräte werden digital erfasst, Risiken bewertet, Maßnahmen zugewiesen und dokumentiert. So weiß im Ernstfall jeder der 220 Mitarbeitenden, was zu tun ist. Vorgegebene Workflows sorgen dafür, dass festgelegte Abläufe eingehalten werden, Änderungen werden automatisch versioniert, Nachweise lückenlos archiviert. Der Information Security Officer gibt ein Beispiel aus dem Arbeitsalltag: „Wird einer unserer Server gewartet, so sind im System alle zugehörigen Schritte, Sicherheitsmaßnahmen und Verantwortlichkeiten hinterlegt. Das klingt banal, aber es schafft enorme Sicherheit. Wir wissen jetzt jederzeit, welche Abhängigkeiten bestehen."

Abteilungen verbinden, Synergien nutzen, Akzeptanz gewinnen

Die Veränderungen, die die Einführung von ConSense GRC mit sich gebracht hat, lassen sich besonders in der internen Zusammenarbeit spüren. So sind Qualität und Informationssicherheit zwar zwei verschiedene Disziplinen, aber sie greifen an vielen Stellen ineinander. Durch die Einbindung des Informationssicherheits-Managements in das bestehende QMS nutzen beide Abteilungen das gleiche System, „sprechen die gleiche Sprache", profitieren von Synergien und sparen dadurch viel Zeit. „Früher hatten wir klar getrennte Aufgabenbereiche, heute arbeiten wir eng zusammen. Das Integrierte Managementsystem hat uns geholfen, das auch organisatorisch zu leben", meint Markus Lentsch.

Einer der größten Vorteile der softwarebasierten Lösung zeigt sich bei Audits. In der Vergangenheit bedeuteten sie tagelange Vorbereitung. Heute genügen wenige Klicks: Alle relevanten Informationen sind im digitalen Managementsystem zentral hinterlegt, Änderungen lassen sich über den Audit-Trail nachvollziehen. Weil mit dem Integrierten Management auf Basis von ConSense GxP das Fundament schon vorhanden war, gelang dem Unternehmen die Zertifizierung nach ISO 27001 in einem kurzen Zeitraum: Im August 2025 wurde die Softwarelösung ConSense GRC eingeführt, bereits im Oktober des Jahres bestand das Biopharma-Unternehmen erfolgreich das Zertifizierungsaudit. Markus Lentsch berichtet: „Die Auditoren haben gesehen, dass unser System gelebt wird. Das schafft Vertrauen und hat entscheidend zur schnellen Zertifizierung nach ISO 27001 beigetragen. Unsere Auditorin lobte ganz besonders, dass viele Informationen aus dem bestehenden Managementsystem für das Compliance- und Risikomanagement weiterverwendet werden konnten."

Informationssicherheit muss im Unternehmen ankommen

Das Beispiel Single Use Support belegt, dass der Nutzen eines digitalen ISMS sich besonders dann zeigt, wenn viele Menschen an der Umsetzung von Informationssicherheit beteiligt sind. Denn mehr Cybersecurity entsteht nicht allein durch Richtlinien, sie muss im Alltag im Unternehmen gelebt werden und zu den Arbeitsweisen der Menschen passen. Das bedeutet, dass eine erfolgreiche Informationssicherheitsstrategie mehr braucht als Software. Sie darf sich nicht nur an Normen orientieren, sondern auch an den Bedürfnissen der Menschen, die mit ihr arbeiten. „Denn am Ende entscheidet nicht allein die Technik über die Sicherheit", meint Harald Lenders. „Entscheidend ist, ob Menschen Prozesse verstehen, Verantwortung übernehmen und gemeinsam handeln. Damit wird ein ISMS nicht zu einem Kontrollelement, sondern zu einem Werkzeug für bessere Zusammenarbeit und nachhaltige Sicherheit."

Unternehmen, die Informationssicherheit heute systematisch aufbauen, schaffen damit nicht nur die Grundlage für regulatorische Anforderungen wie die NIS2-Richtlinie oder die ISO 27001, sondern stärken auch ihre eigene Widerstandsfähigkeit. „Das endet übrigens nicht mit der Einführung eines ISMS. Wir legen unseren Kunden immer nahe, Cybersecurity nicht als Projekt mit einem festen Enddatum zu verstehen, sondern eine kontinuierliche Weiterentwicklung im Blick zu behalten", meint der Experte abschließend. •

> „ Die verbindliche EU-Richtlinie NIS2 erweitert den Kreis der betroffenen Unternehmen, erhöht die Anforderungen und rückt technische Maßnahmen und organisatorische Prozesse in den Mittelpunkt.
>
> *Dr. Stephan Killich*

KI-WETTLAUF-CHECK

KI-Angreifer nutzen Schwachstellen aus, während viele Unternehmen NIS2 noch nicht umgesetzt haben.

Digitales ISMS mit Audit-Trail schafft Vorsprung – Zertifizierung in zwei Monaten möglich.

Digital Trust braucht Beweise: KI ohne Zertifizierung funktioniert nicht

KI-Entscheidungen sind oft eine Blackbox – doch Vertrauen entsteht daher nicht durch Eigenauskünfte, sondern durch unabhängige Audits. ISO 27001 und ISO 42001 werden zur neuen Vertrauensarchitektur für Unternehmen. /// von Marko Hoffmann

KÜNSTLICHE INTELLIGENZ IST MITTLERWEILE FESTER BESTANDTEIL VIELER GESCHÄFTSPROZESSE. In der Industrie erkennen KI-gestützte Kamerasysteme Qualitätsabweichungen in Echtzeit, in Handel und Logistik optimieren Algorithmen Warenströme und im Vertrieb analysieren KI-Anwendungen Kundenverhalten. Mit dem wachsenden Einsatz von KI wird ein Thema immer wichtiger: **Vertrauen.**

Kunden, Geschäftspartner, Investoren und Behörden müssen sich darauf verlassen können, dass digitale Technologien sicher, transparent und regelkonform funktionieren, obwohl die Entscheidungen der zugrundeliegenden KI-Modelle immer schwerer nachvollziehbar sind. Regulatorische Anforderungen durch den EU AI Act, NIS-2 oder DORA sowie global-vernetzte Lieferketten verlangen Nachweise für Risikopräventionsmaßnahmen. „Digital Trust" ist längst kein „Nice-to-have" mehr, sondern entwickelt sich zum Wettbewerbsfaktor und in vielen Märkten zur Voraussetzung für Geschäftsbeziehungen. Die entscheidende Frage lautet daher nicht mehr, wer KI einsetzt, sondern wer nachweisen kann, dass er sie sicher und verantwortungsvoll betreibt und seine IT-, OT- und Daten-Risiken unter Kontrolle hat.

Wenn das KI-Modell entscheidet, reicht Vertrauen allein nicht mehr

Vertrauen in einer digitalen Wirtschaft kann nicht auf Eigenauskünften beruhen. Überprüfbare Nachweise mit klaren Prüfkriterien werden daher immer wichtiger. Viele Unternehmen verbinden ein Audit vor allem mit Dokumenten und Richtlinien. Externe Auditoren prüfen jedoch auch deren praktische Umsetzung. Oftmals sprechen Auditoren mit Mitarbeitenden oder beziehen Fachabteilungen ein, um offene Fragen direkt vor Ort zu klären. Dadurch entsteht ein realistisches Bild davon, wie wirksam Prozesse tatsächlich funktionieren.

Ein Beispiel aus der ISO 27001-Praxis: Trotz dokumentierter Sicherheitsvorgaben und Mitarbeiterschulungen stellt ein Auditor während einer Betriebsbegehung fest, dass Mitarbeiter ihre Rechner beim Verlassen des Arbeitsplatzes nicht sperren. Solche Beobachtungen zeigen ihm den Unterschied zwischen dokumentierter Compliance und gelebter Sicherheitskultur und führen zu Beanstandungen im Auditbericht.

ISO/IEC 27001 und ISO/IEC 42001: Die neue Vertrauensarchitektur für KI

Während klassische Informationssicherheitsmanagementsystem-Audits Risikobewertungen, Incident-Management oder Lieferantenkontrollen untersuchen, kommen im KI-Umfeld weitere Fragestellungen, etwa zu Trainingsdaten, Risikobewertung, Modelländerungen, Transparenz und dem Umgang mit Fehlentscheidungen, hinzu.

Um diesen Themen zu begegnen, gewinnt die Kombination aus ISO/IEC 27001 und ISO/IEC 42001 an Bedeutung. Während ISO 27001 Informationssicherheit adressiert, unterstützt ISO 42001 den verantwortungsvollen Einsatz von KI. Gemeinsam schaffen sie eine belastbare Grundlage für Vertrauen in digitale Geschäftsmodelle.

> „ **‚Digital Trust' ist längst kein ‚Nice-to-have' mehr**, sondern entwickelt sich zum **Wettbewerbsfaktor** und in vielen Märkten zur Voraussetzung für Geschäftsbeziehungen.
>
> *Marko Hoffmann*

Viele Anforderungen der KI-Governance bauen auf etablierten Prinzipien des Informationssicherheitsmanagements auf, etwa Risikomanagement, Lieferantenbewertung und Incident Management. Hinzu kommen jedoch neue Prüffelder wie Daten-Governance, Modellrisiken und Transparenz.

Ein Überblick über gängige Standards für IT, OT und KI

- ISO/IEC 27001 gilt weltweit als führender Standard für Informationssicherheitsmanagement. Die Norm unterstützt Unternehmen dabei, Risiken systematisch zu be-

werten, Sicherheitsmaßnahmen umzusetzen und Informationswerte zu schützen. Gleichzeitig fördert sie Prozesse wie Incident Management, Lieferantenmanagement und Business Continuity.

- ISO/IEC 42001 ergänzt diesen Ansatz um die Perspektive der KI-Governance. Die Norm definiert Anforderungen an den verantwortungsvollen Einsatz von KI, an Risikomanagement, Transparenz und die kontinuierliche Verbesserung von KI-Managementsystemen.
- IEC 62443 ist eine Normreihe, die Sicherheitsanforderungen für industrielle Automatisierungs- und Steuerungssysteme (IACS) definiert. Sie umfasst Maßnahmen zur Cybersicherheit, um die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen und Daten in Industrieanlagen zu gewährleisten.
- SOC wurde vom American Institute of Certified Public Accountants entwickelt. Der freiwillige Standard richtet sich vor allem an Unternehmen, die Kundendaten verarbeiten und gegenüber Auftraggebern Transwparenz über ihre Sicherheitsmaßnahmen schaffen müssen. Das freiwillige Assessment ist eine wichtige Grundlage für den Marktzugang in den USA.
- TISAX, kurz für Trusted Information Security Assessment Exchange, wurde speziell für die Automobilindustrie entwickelt. TISAX hat einen klaren Fokus auf die Lieferkette in der Automobilindustrie und insbesondere den Schutz der Kundendaten der Unternehmen.

Darüber hinaus gibt es weitere branchenspezifische Standards, insbesondere im Bereich der kritischen Infrastrukturen. Die Wahl des Zertifizierschemas hängt davon ab, in welchem Markt und in welcher Branche ein Unternehmen tätig ist. Auch die gesetzlichen Vorgaben, die zu erfüllen sind, sollten im Auswahlprozess berücksichtigt werden.

WER PRÜFT EIGENTLICH DIE PRÜFER?

Ein Zertifikat ist nur so glaubwürdig wie die Stelle, die es ausstellt. Deshalb werden akkreditierte Zertifizierungsstellen selbst regelmäßig überwacht und auditiert.

Diese Aufgabe übernimmt beispielsweise die Deutsche Akkreditierungsstelle (DAkkS) oder die amerikanische ANSI National Accreditation Board (ANAB). Sie kontrolliert, ob Zertifizierungsstellen nach internationalen Vorgaben arbeiten und Auditoren ausreichend qualifiziert sind.

Woran Unternehmen seriöse Zertifikate erkennen

- Die Zertifizierungsstelle verfügt über eine gültige Akkreditierung.
- Das Zertifikat enthält Zertifikatsnummer, Geltungsbereich und Gültigkeitsdauer.
- Die Gültigkeit lässt sich über eine Zertifikatsdatenbank überprüfen.
- Regelmäßige Überwachungs- und Rezertifizierungs-Audits stellen sicher, dass Anforderungen dauerhaft erfüllt werden.

Vertrauen entsteht nicht durch das Zertifikat selbst, sondern durch ein mehrstufiges System unabhängiger Prüfungen, das auch die Zertifizierungsstellen einschließt.

Vertrauen braucht Nachweise

Der Wert eines Zertifikats, sei es als Nachweis des eigenen Risikomanagements oder des Risikomanagements eines Lieferanten, liegt nicht im Dokument selbst, sondern in der unabhängigen Prüfung dahinter. Sie bestätigt die Wirksamkeit von Prozessen und Kontrollen. In einer zunehmend KI-geprägten Wirtschaft werden Audits und Zertifizierungen damit zum entscheidenden Vertrauensbeweis für Sicherheit, Verlässlichkeit und Verantwortungsbewusstsein. Gesetzliche Bestimmungen in der EU oder der Marktdruck in den USA, der einen Nachweis nach SOC quasi zur Bedingung für eine Geschäftstätigkeit dort macht, zeigen, dass Zertifizierungen heute ein wichtiger Faktor für die Haftungssicherheit und globale Marktfähigkeit von Unternehmen sind. •

DER AUTOR
Marko Hoffmann
ist Lead Auditor ISO/IEC27001/TISAX & Information Security Officer bei der TÜV SÜD Management Service GmbH.

Bild: TÜV SÜD

Wer gewinnt den KI-Wettlauf 2026?

Die Cybersicherheitslandschaft 2026 gleicht mehr denn je dem alten Wettlauf zwischen Hase und Igel, nur dass der Hase heute mit KI-Geschwindigkeit läuft. Wir haben Experten befragt: „Im KI-Wettlauf 2026 schlägt der ‚Hase' (Angreifer) in Lichtgeschwindigkeit zu. Welcher konkrete ‚Igel-Trick' – welche Strategie oder Technologie – entscheidet heute im Mittelstand darüber, ob man dem Angreifer diesen einen entscheidenden Schritt voraus bleibt, statt nur dem Schaden hinterherzulaufen?" /// von Konstantin Pfliegl

ARIS KOIOS
Senior Technology Strategist bei CrowdStrike
Bild: Crowdstrike

Künstliche Intelligenz hat die Spielregeln in der Cyberkriminalität grundlegend verändert. Angreifer können heute Schwachstellen identifizieren, Angriffe automatisieren und Unternehmen mit einer Geschwindigkeit kompromittieren, mit der herkömmliche Security Operations schlicht nicht Schritt halten können. Wenn Schwachstellen innerhalb weniger Stunden ausgenutzt werden und Angreifer innerhalb von Minuten von der Account-Kompromittierung zum Datendiebstahl übergehen können, reichen traditionelle Patch-Zyklen und fragmentierte Sicherheitslösungen nicht mehr aus.

KI-Agenten als neue Verteidigungslinie
Für den deutschen Mittelstand ist es entscheidend, die Zeit zwischen Angreiferaktivität und Abwehrreaktion zu verkürzen. Dafür braucht es eine einheitliche Sichtbarkeit über Identitäten, Endpoints, Cloud, Daten und KI hinweg, die durch ein Operating Model unterstützt wird, welches Security-Teams ermöglicht, mit Maschinengeschwindigkeit zu reagieren. Genau das ist das Konzept des Agentic SOC: KI-Agenten automatisieren hochvolumige Aufgaben wie Detection, Triage und Response, während sich menschliche Analysten auf Strategie, Urteilsvermögen und komplexe Entscheidungen konzentrieren, die Erfahrung erfordern. Um Angreifern einen Schritt voraus zu bleiben, benötigen Unternehmen eine kontinuierliche, KI-gestützte und angreiferorientierte Priorisierung. •

DR. BEVERLY MCCANN
Director of Analysis für EMEA bei Darktrace
Bild: Darktrace

Wenn mittelständische Unternehmen KI in ihre täglichen Abläufe integrieren, wird diese selbst zu einem Teil der Angriffsfläche, die es zu schützen gilt. Angreifer können Veränderungen bei KI-bezogenen Zugriffsrechten, Anwendungen und Datenflüssen in Maschinengeschwindigkeit ausnutzen. Dadurch wird es für Sicherheitsteams schwieriger, legitime Aktivitäten von ersten Anzeichen eines Angriffs zu unterscheiden. Um Angreifern einen Schritt vorauszubleiben, braucht es Sicherheitstechnologien, die den normalen digitalen Kontext eines Unternehmens verstehen und reagieren können, während sich ein Angriff noch entwickelt.

Aufbau einer widerstandsfähigen Sicherheitsarchitektur
Der „Igel-Trick" besteht darin, der Geschwindigkeit der Angreifer mit Kontextwissen zu begegnen. Eine widerstandsfähige Sicherheitsarchitektur setzt im gesamten digitalen Umfeld – Infrastruktur, Menschen und KI – auf verhaltensbasierte KI. Sie lernt, welche Vorgänge im Unternehmen normal sind, welche Zugriffsmuster typischerweise auftreten und welche Kommunikationswege zum Arbeitsalltag gehören. So kann sie auch bislang unbekannte Angriffe erkennen. Der entscheidende Vorteil entsteht durch die Verbindung von Erkennung und präziser autonomer Reaktion. Verhaltensbasierte KI kann sofort und selbstständig handeln, weil sie weder auf bekannte Signaturen oder bereits dokumentierte Angriffsmuster noch auf eine menschliche Bestätigung warten muss. •

KI-WETTLAUF-CHECK

KI-Agenten automatisieren Angriffe – vom Zugriff zum Datendiebstahl in unter einer Minute.

Agentic SOCs und KI-Priorisierung stehen schon dort, wo der Angriff erst hinwill.

PETER SCHILL
Senior Manager Systems Engineering bei Fortinet
Bild: Fortinet

MICHAEL LOCHER-TJOA
Leiter des Mittelstandsgeschäfts von Microsoft DACH
Bild: Microsoft

Im KI-Wettrennen 2026 besteht der entscheidende „Igel-Trick" für KMU nicht darin, Angreifern mit mehr Sicherheitstools zu entkommen. Vielmehr geht es darum, die Komplexität durch eine einheitliche, KI-gestützte Cybersecurity-Plattform zu reduzieren, die Netzwerk, Sicherheit, Transparenz und automatisierte Reaktionen vereint. Da Angreifer KI nutzen, um ihre Erkundung zu beschleunigen, Schwachstellen auszunutzen und Angriffe zu skalieren, müssen KMU in der Lage sein, Bedrohungen mit maschineller Geschwindigkeit zu erkennen und einzudämmen. KI-gesteuerte Cybersecurity kann Signale in der gesamten Umgebung analysieren, die kritischsten Risiken priorisieren und Reaktionsmaßnahmen automatisieren, bevor ein Vorfall eskaliert.

Automatisierung von Routineaufgaben

Dies ist besonders wichtig für Firmen, die mit einem Mangel an Fachkräften im Bereich Cybersecurity zu kämpfen haben. Eine einheitliche Plattform hilft Teams, mit weniger Ressourcen mehr zu erreichen, indem sie Abläufe vereinfacht und Routineaufgaben automatisiert. Gleichzeitig bleibt Schulung auf allen Ebenen des Unternehmens unerlässlich. Nicht nur, um das Bewusstsein für Cybersecurity zu stärken, sondern auch, um die Risiken von Shadow AI zu mindern, da Mitarbeiter KI-Tools zunehmend in ihre tägliche Arbeit integrieren, manchmal ohne formelle Governance-Rahmenbedingungen. Letztendlich beruht Resilienz nicht auf einer einzelnen Technologie oder Taktik. •

Künstliche Intelligenz ermöglicht Angreifern, schneller Schwachstellen zu finden, Angriffe zu automatisieren und ihre Reichweite massiv zu vergrößern. Gleichzeitig können die meisten Mittelständler ihre Sicherheitsteams nicht beliebig vergrößern, denn der Fachkräftemangel bleibt eine der größten Herausforderungen in der Cybersicherheit. Den Wettlauf im Security-Bereich kann der Mittelstand aber gewinnen, wenn er seine Verteidigung genauso verstärkt wie die Angreifer ihre Attacken: mit der Hilfe von KI.

Der Vorsprung entscheidet

Die nächste Generation der IT-Sicherheit basiert nicht mehr nur auf menschlichem Know-how, sondern auf intelligenten Agentensystemen. Sie arbeiten wie ein eingespieltes Security-Team: Spezialisierte KI-Agenten suchen aktiv nach Schwachstellen, bewerten Risiken im jeweiligen Unternehmenskontext und unterstützen menschliche IT-Sicherheitsspezialisten bei Gegenmaßnahmen, bevor aus der Schwachstelle ein Sicherheitsvorfall wird. Microsoft hat erst kürzlich so ein agentisches Sicherheitssystem vorgestellt: Bei „Project Perception" arbeiten spezialisierte Red-, Blue- und Green-Team-Agenten zusammen, um kontinuierlich Risiken zu erkennen, zu bewerten und auszuräumen.

Wer KI nicht nur den Angreifern überlässt, sondern auch seine Verteidigung in Echtzeit damit organisiert, verschafft sich den entscheidenden Vorsprung. •

Wer gewinnt den KI-Wettlauf 2026?

THOMAS HEINZ
Senior Manager Solutions Engineering bei Okta
Bild: Okta

Der Igel gewinnt in der Fabel durch kluge Positionierung, denn den Wettlauf mit dem Hasen würde er verlieren. Daher sollte der Mittelstand mit seinen knappen Ressourcen für IT-Sicherheit ebenfalls strategisch vorgehen. Ein Wettrüsten wäre sinnlos, denn die KI-gestützten Angriffe, ob personalisiertes Phishing oder massenhaftes Credential Stuffing, erfolgen automatisiert und blitzschnell. Somit sind die bewährten Sicherheitskonzepte, wie Firewalls, Security-Suites, verschiedene Lösungen unterschiedlicher Anbieter, On-Premise-Sicherheitskonzepte, überholt, da zu langsam.

Identität als Burgmauer

Der Mittelstand sollte daher das Identitätsmanagement sowie die Identitätssicherheit als seine Burgmauer betrachten und angesichts der knappen Ressourcen als as-a-Service-Lösung besorgen. Wichtig: Hacker attackieren oft nicht mehr direkt, sondern sie übernehmen ein Benutzerkonto und melden sich an. Somit muss eine strikte Verwaltung aller digitalen Identitäten erfolgen - gemäß Zero Trust und dem Prinzip der Geringsten Zugriffsrechte - sowie eine lückenlose Aufdeckung im Netzwerk, damit weder verwaiste Konten noch Schatten-KI durch unregistrierte KI-Agenten zum Einfallstor werden können.

Der eigentliche „Igel-Trick“ ist dabei der Einsatz eines modernen, KI-gestützten IAM. Dieses bewertet Zugriffe nicht nur einmalig bei der Anmeldung, sondern kontinuierlich in Echtzeit. Es analysiert im Hintergrund hunderte Kontext-Signale - wie unbekannte Geräte, ungewöhnliche Standorte oder atypisches Nutzerverhalten. •

ANDY SCHNEIDER
CSO EMEA Central bei Palo Alto Networks
Bild: Palo Alto Networks

2026 wird der Hase immer erfolgreicher, weil er mittels KI-gestützter Angriffe jede Lücke sofort finden kann. Und im Mittelstand gibt es davon meist mehr als gedacht: Tools für Endpoints, für Identitäten, für die Cloud – allerdings spricht keines wirklich mit dem anderen. Wie schnell Angriffe heute ablaufen, zeigt ein Blick auf die Praxis: Zwischen erstem Zugriff und Datenexfiltration vergeht im Extremfall keine Minute. Kein Team kann so schnell reagieren, wenn es erst zwischen mehreren Konsolen hin- und herwechseln muss.

Lücken vermeiden statt Tempo jagen

Der Igel-Trick ist deshalb kein Wettrüsten um Geschwindigkeit, das lässt sich gegen KI-gestützte Angreifer ohnehin nicht gewinnen. Er besteht darin, die Lücken gar nicht erst entstehen zu lassen und dort, wo sie trotzdem auftreten, genauso schnell zu reagieren wie der Angreifer selbst. Dafür braucht es eine Sicherheitsarchitektur, in der Identität, Endpoint, Cloud und KI-Anwendungen an einer Stelle zusammenlaufen und in Echtzeit sichtbar sind. Dazu gehört auch, KI-Agenten wie Mitarbeiter mit klar definierten Berechtigungen und kontinuierlicher Verifizierung jeder Aktion zu behandeln. Niemand gäbe einer neuen Aushilfskraft am ersten Tag Zugriff auf alle Finanzkonten. Bei KI-Agenten ist genau das noch viel zu oft der Fall.

Für den Mittelstand heißt das: weg von Excel-Listen und Einzeltools, hin zu einer Plattform, die Bedrohungen erkennt und stoppt, bevor der Hase sie ausnutzt. •

ROGER SCHEER
Regional Vice President Central Europe bei Tenable
Bild: Tenable

Im KI-Zeitalter gegen Angreifer ein Wettrennen gewinnen zu wollen? Reine Utopie. Vor allem für den Mittelstand, wo Budget und Security-Personal ohnehin knapp sind. Aber Geschwindigkeit ist auch gar nicht der Punkt. Im klassischen Bild von Hase und Igel gewinnt der Igel nicht durch Tempo, sondern durch Taktik. Er läuft nicht hinterher, er steht schon da.

Silos aufbrechen, Risiken erkennen

Genau darum geht es: Angreifer ins Leere laufen lassen, statt nur auf den nächsten Einschlag zu reagieren. Das bedeutet in der Praxis: Weg mit den alten Security-Silos. Wer Cloud-Workloads, IT-Infrastruktur, Identitäten und neue KI-Tools getrennt voneinander betrachtet, verliert schnell den Überblick. Gefragt ist stattdessen eine risikobasierte Perspektive auf die gesamte Angriffsfläche – denn bei dieser enormen Komplexität ist es unmöglich, jede einzelne Schwachstelle zu schließen. Das muss man aber auch gar nicht. Die Kunst liegt darin, das Rauschen herauszufiltern. Hier schlagen wir die Angreifer mit ihren eigenen Waffen: KI-gestützte Analysen decken präzise die brandgefährlichen Kombinationen und kritischen Pfade auf, auf die es Hacker wirklich abgesehen haben. Wenn wir genau diese Einfallstore präventiv schließen, verpufft der Geschwindigkeitsvorteil der Angreifer. Am Ende schützt uns vor KI-gestützten Attacken nicht die hektische Jagd nach immer schnelleren Reaktionszeiten. Die beste Verteidigung ist und bleibt eine vorausschauende Strategie, die Gefahren entschärft, bevor überhaupt Schaden entsteht. •

CHRISTOPH SCHUHWERK
CISO in Residence bei Zscaler
Bild: Zscaler

In mittelständischen Unternehmen kommen gleich mehrere kritische Faktoren hinsichtlich KI-basierter Cyberangriffe zusammen: Budget und Security-Fachkräfte sind stark limitiert, während die Geschwindigkeit und Frequenz von Attacken stark zunehmen.

Um die Abwehr gegen moderne Angriffsszenarien effizient zu gestalten, empfehle ich drei technologische Ansätze, die letztlich auf eine Automatisierung hinauslaufen und damit die IT-Sicherheitsteams entlasten. Erstens lässt sich hinter einem Zero Trust-Broker ein großer Teil der Angriffsoberfäche eines Unternehmens verstecken. Und was die Angreifer-KI nicht sieht, kann sie auch nicht attackieren.

Falsche Fährten mit Deception

Schafft es ein Malware-Akteur dennoch in die IT- oder OT-Infrastruktur des Unternehmens einzudringen, zum Beispiel durch gestohlene Zugangsdaten, dann sind Deception-Technologien ein wichtiges Mittel für Sicherheitsteams. Einerseits werden Angreifer auf die falsche Fährte gelockt und geben sich zu erkennen, wenn sie auf Honeypots hereinfallen. Anderseits erkaufen sich IT-Sicherheitsteams Zeit, um den Angriff zu analysieren und zu stoppen. Am wichtigsten ist aus meiner Sicht allerdings die Automatisierung der Abwehrmaßnahmen, um mit der Angriffsgeschwindigkeit mitzuhalten. Ein Automated SOC kann auf Angriffe mit Hilfe von KI autonom reagieren und zum Beispiel kompromittierte Accounts sperren oder das Nachladen von Malware unterbinden. •

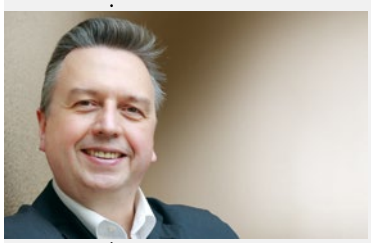
Der Mensch delegiert, das Risiko bleibt

Wer KI-Agenten handeln lässt, muss Verantwortung neu organisieren. /// von Alexander Peters

GENERATIVE KI GIBT ANTWORTEN. KI-AGENTEN HANDELN. Fehler, Fehlkonfigurationen oder missbräuchliche Zugriffe können sich dadurch automatisiert und schnell über verbundene Systeme ausbreiten.

Menschen und Agenten bilden eine Risikofläche

Menschen definieren Aufgaben und Berechtigungen von KI-Agenten. Deren Risiko wird daher nicht allein durch die Technik, sondern auch durch den menschlichen und organisatorischen Kontext bestimmt: Wer hat den Agenten zu welchem Zweck eingerichtet, und worauf darf er zugreifen? KI-Agenten sollten deshalb als Erweiterung des Human Risk in das Human Risk Management einbezogen werden. Ein Agent übernimmt Aufgaben, nicht aber die organisatorische Verantwortung. Er braucht einen eindeutigen Owner für den genehmigten Anwendungsfall.



DER AUTOR
Alexander Peters
ist Senior Manager Sales Engineering für die Regionen DACH und Northern Europe bei Mimecast.

> „ Ein Agent übernimmt Aufgaben, nicht aber die organisatorische Verantwortung. Er braucht einen **eindeutigen Owner** für den genehmigten Anwendungsfall.
>
> *Alexander Peters*

Klar geregelt sein müssen die Vergabe und Prüfung von Berechtigungen, Änderungen am Einsatz und menschliche Freigaben bei kritischen Aktionen. Die Bedeutung dieser Strukturen zeigt eine IDC-Prognose: Bis 2029 sollen weltweit mehr als eine Milliarde KI-Agenten täglich rund 217 Milliarden Aktionen ausführen.

Ohne Sichtbarkeit keine Kontrolle

Unternehmen müssen wissen, welche Agenten aktiv sind, wer sie eingerichtet hat, welchem Zweck sie dienen und welche Identität sie nutzen. Auch Verbindungen zu Anwendungen, Datenquellen und MCP-Servern sowie Zugriffe und Aktionen müssen bekannt sein. Erst diese Transparenz zeigt den „Blast Radius" eines kompromittierten oder fehlerhaft handelnden Agenten. Da Beschäftigte meist umfassendere Zugriffsrechte benötigen, sollten Agenten nicht sämtliche Berechtigungen ihrer Nutzer übernehmen. Sie brauchen eine eigene, überprüfbare und zweckgebundene Identität.

Kontrolle und Nachvollziehbarkeit

Auch ein zunächst sicher konfigurierter Agent kann durch neue Aufgaben, Systemverbindungen oder Datenzugriffe sein Risikoprofil verändern. Seine Freigabe darf nicht einmalig bleiben: Unternehmen müssen kontinuierlich prüfen, ob Verhalten und Berechtigungen noch dem genehmigten Zweck entsprechen.

Human Risk Management verknüpft den menschlichen Kontext mit Agentenaktivitäten und technischen Risikosignalen. Um Vorfälle rekonstruieren zu können, braucht jeder Agent einen Audit Trail: Er dokumentiert Identität, Verantwortliche, Zugriffe und Aktionen. Das gilt über den gesamten Lebenszyklus: Bei Austritt oder Rollenwechsel des Owners, Projektende oder entfallenem Einsatzzweck ist zu prüfen, ob der Agent noch benötigt wird.

Aufgaben lassen sich delegieren, Verantwortung nicht

Agenten nur als Software-Inventar zu erfassen und ihre Governance bis zum nächsten Audit aufzuschieben, genügt nicht. Unternehmen sollten jederzeit beantworten können: Welche Agenten laufen? Wer verantwortet sie? Was dürfen sie erreichen? Aufgaben lassen sich delegieren. Verantwortung nicht. •

Zu niedriger KI-Reifegrad

Organisationen in Deutschland vertrauen zu sehr ihrer KI-Agenten-Sicherheit, obwohl die Realität bei der Governance anders aussieht. ///

DEUTSCHE CISOS HABEN LAUT DEM CISO INSIGHTS REPORT VOM JULI 2026 Angst vor KI-gestütztem Phishing (81 Prozent, der höchste einer einzelnen Bedrohung zugeschriebene Wert). Hinzu kommt, dass der Reifegrad bei der KI-Absicherung hierzulande gering ist (58 Prozent stufen ihr Unternehmen als ‚in Entwicklung' oder ‚reaktiv' ein). Sie sehen dabei organisatorische Silos als größte Hürde (50 Prozent), danach folgen geringe Transparenz bei KI-Identitäten, ungenügende Industriestandards und knappe Budgets. Außerdem zeigte sich, dass deutsche Geschäftsführungen die KI-Sicherheit vor allem als regulatorische oder Compliance-Aufgabe betrachten. Dennoch legen deutsche Teilnehmer das weltweit höchste Vertrauen in ihre Maßnahmen zum KI-Schutz. Ein Trugschluss.

Das deutsche Compliance-Paradoxon

In Deutschland werden bei einer Authentifizierung 28 Prozent als Bedrohung bewertet – der höchste Wert gemäß einer Studie. 32 Prozent der deutschen Befragten gaben im Rahmen eines weiteren Berichts zu, KI ohne Genehmigung am Arbeitsplatz zu nutzen (14 Prozent regelmäßig, 18 Prozent gelegentlich) und damit Schatten-KI zu schaffen. Außerdem geben 14 Prozent vertrauliche Dokumente an KI-Tools weiter. Das klingt vielleicht nach viel, ist aber der zweitniedrigste Wert weltweit. Jedoch: 68 Prozent hatten im vergangenen Jahr mit einem KI-Sicherheitsproblem zu tun und 44 Prozent mit einer Sicherheitsverletzung – die höchste Quote global.

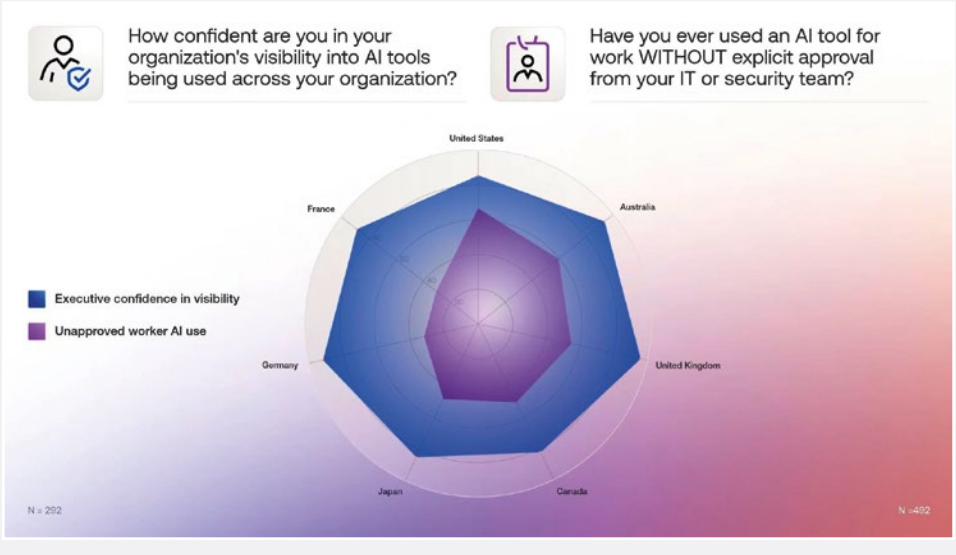
Die Grundlagen schaffen

Das Fundament im Falle der KI-Sicherheit bildet das Identitätsmanagement (IAM), denn mithilfe eines modernen Verständnisses von Identitätssicherheit lassen sich KI-Agenten und KI-Tools registrieren, als digitale Identitäten einbinden und mittels der bewährten IAM-Palette verwalten. So gelingt es den deutschen Entscheidungsträgern, die Kontrolle zurückzuerlangen, damit Realität und Wahrnehmung nicht auseinandergehen. Als Einstieg bietet es sich an, auf drei präzise Fragen eine Antwort zu finden: Wo sind meine KI-Agenten? Was dürfen sie tun? Womit können sie sich verbinden? Die KI-Agenten sollten somit als Virtuelle Mitarbeiter betrachtet werden, die Zugriffsrechte benötigen – am besten nach dem Prinzip der Geringsten Privilegien sowie gemäß dem Zero-Trust-Konzept – und einen Not-Aus-Schalter, um jeglichen Zugriff bei Ungerreimtheiten sofort zu unterbrechen. Außerdem braucht es verantwortliche Eigentümer, eine komplette Dokumentation der Aktivitäten, die Fähigkeit zum Audit und die Einhaltung der Europäischen Compliance-Regularien. Wer das nicht aus eigener Kraft schafft, der kann auf einen SaaS-Anbieter setzen, der die Identitätssicherheit bereitstellt – am besten KI-getrieben, um mit Echtzeit-Maßnahmen auf der Höhe der KI-Angriffsversuche zu sein.

Fazit

Künstliche Intelligenz soll ein Business-Beschleuniger sein, kein Sicherheitsrisiko oder eine bloße Idee. Notwendig ist dafür eine andere Betrachtungsweise. Es handelt sich nicht um Dienstleistungsprogramme, sondern um virtuelle Mitarbeiter, die so abgesichert werden müssen, wie die digitalen Identitäten von menschlichen Angestellten. Daher müssen diese KI-Mitarbeiter durchweg über IAM-Sicherheitslösungen kontrolliert werden, um Zugriffsrechte granular verwalten und kontinuierlich mittels Authentifizierung überwachen zu können. •

Thomas Heinz,
Senior Manager Solutions Engineering bei Okta.



Deutsche Geschäftsführer und Vorstände haben hohes Vertrauen in ihre Netzwerk-Transparenz und deutsche Angestellte nutzen wenig Schatten-KI - Fakten, die in falsche Sicherheit wiegen

Human Risk Management im KI-Zeitalter

KI verändert Human Risk: Sie macht Angriffe glaubwürdiger, ermöglicht aber auch gezieltere Abwehr. Entscheidend sind Menschen, Technik und Zugriffsrechte. /// von Dr. Yvonne Bernard

Wenn Vertrauen selbst zum Angriffsvektor wird

Mindestens acht von zehn Unternehmen setzen auf Microsoft 365 oder Microsoft Teams. Zugleich fürchten 55 Prozent der im AI-Security-Report 2026 von Hornetsecurity by Proofpoint befragten Unternehmensentscheider KI-gestützte Phishing-Angriffe. 51 Prozent der befragten Mitarbeitenden schätzen ihre Handlungssicherheit bei sicherheitsrelevanten Vorfällen in Microsoft 365 oder Teams als begrenzt oder gar nicht vorhanden ein. Nur zwölf Prozent fühlen sich sehr gut vorbereitet.

Die Sorge vor KI-gestützten Angriffen trifft auf Unsicherheit im digitalen Arbeitsalltag. Human Risk Management muss deshalb gezieltes Training, technische Schutzmechanismen und klar geregelte Zugriffsrechte verbinden.

KI verändert die Spielregeln des Social Engineering

Generative KI hilft Angreifern, überzeugende Phishing-Nachrichten schnell zu erstellen und auf einzelne Empfänger zuzuschneiden. Damit verlieren Warnzeichen wie Grammatikfehler an Aussagekraft. Deepfakes können Stimmen oder Bilder imitieren und etwa einen Anruf einer Führungskraft glaubwürdiger erscheinen lassen.

Noch schwieriger wird es, wenn Angreifer mehrere Kanäle kombinieren. Auf eine Phishing-Mail folgt eine SMS – Smishing – oder ein Anruf – Vishing. Ein vermeintlicher IT-Support kann dazu drängen, eine MFA-Anfrage zu bestätigen. QR-Codes können Nutzer aus einer geschützten Umgebung auf manipulierte Seiten führen.

Damit reicht es nicht mehr, einzelne verdächtige Merkmale zu erkennen. Beschäftigte müssen den gesamten Kommunikationskontext prüfen: Passen Absender, Kanal, Zeitpunkt und Handlungsaufforderung zusammen?

Das ist anspruchsvoll, wenn jemand zwischen Meetings E-Mails scannt oder unterwegs eine dringende Anfrage beantwortet. Sicherheit darf nicht voraussetzen, dass jeder Mensch immer richtig entscheidet.

Wenn Angriffe individueller werden, muss Training nachziehen

Ein Standardtraining für alle passt immer weniger zu Angriffen, die sich gezielt auf Empfänger und Kontext zuschneiden lassen.

Awareness Trainings sollten berücksichtigen, wie sicher einzelne Beschäftigte bereits handeln. Wer in Simulationen souverän reagiert, braucht andere Impulse als jemand, der bei bestimmten Angriffsmustern unsicher ist. KI kann helfen, Trainingsbedarf, Lerninhalte und Schwierigkeitsgrad individuell anzupassen.

Auch Phishing-Simulationen können sich KI-basiert am individuellen Sicherheitsniveau orientieren. Einfache Szenarien testen Grundlagen. Anspruchsvollere Varianten beziehen etwa Unternehmensinformationen, berufliche Rollen oder bekannte Personen ein. So üben Beschäftigte den Umgang mit zunächst plausiblen Nachrichten und trainieren dort weiter, wo Unsicherheit besteht.

KI muss auch Teil der Abwehr sein

Auch das beste Training verhindert nicht jeden Fehler. Sicherheitskonzepte dürfen deshalb nicht voraussetzen, dass Menschen immer richtig entscheiden. Technische Schutzmechanismen müssen Security Awareness ergänzen und direkt im Arbeitsablauf unterstützen. Dabei spielt KI auch auf der Abwehrseite eine wichtige Rolle:

> „ Modernes Human Risk Management verbindet deshalb drei Ebenen: **Adaptive Trainings** stärken die Handlungssicherheit. **Technische Leitplanken** fangen riskante Situationen im Arbeitsablauf ab. **Least Privilege** begrenzt die Reichweite kompromittierter Konten.
>
> *Dr. Yvonne Bernard*

Sie kann Kommunikationsmuster analysieren, Auffälligkeiten erkennen und Schutzmechanismen gezielter auslösen. In M365 müssen Systeme zudem neue Angriffswege berücksichtigen. Bei Quishing steckt der schädliche Link etwa im QR-Code. Deshalb müssen Sicherheitsmechanismen auch visuelle Inhalte analysieren können.

Im Verdachtsfall sollten Beschäftigte auffällige Nachrichten direkt per Klick melden und prüfen lassen können. So erreicht der Vorfall schnell das Security-Team, während technische Kontrollen helfen, die Folgen eines Fehlers zu begrenzen.

DIE AUTORIN
Dr. Yvonne Bernard
ist Chief Technology Officer bei Hornetsecurity by Proofpoint, wo sie die technologische Vision und Innovationsstrategie für die Hornetsecurity-Produkte verantwortet.

55 Prozent der im AI-Security-Report 2026 befragten Unternehmensentscheider fürchten KI-gestützte Phishing-Angriffe.

Zugriffsrechte entscheiden über die Reichweite

Human Risk Management endet nicht mit der Abwehr eines Angriffs. Erhält ein Angreifer Zugriff auf ein Benutzerkonto, bestimmen dessen Berechtigungen mit, wie weit er kommt. Doch diese Risiken stehen weniger im Fokus: Nur 25 Prozent der für den AI-Security-Report Befragten sehen Risiken durch kompromittierte Benutzerkonten, 24 Prozent bei externen Freigaben und Gastzugriffen.

Deshalb gilt Least Privilege: Nutzer erhalten nur die Rechte, die sie benötigen. In dynamischen Microsoft-365-Umgebungen verlangt dies laufende Kontrolle. Teams entstehen, Rollen wechseln, Dateien werden geteilt. Was gestern nötig war, kann heute überflüssig sein.

Unternehmen sollten regelmäßig prüfen: Welche Konten besitzen zu viele Rechte? Welche Freigaben werden nicht mehr gebraucht? Welche sensiblen Daten sind unnötig zugänglich? So begrenzt Berechtigungsmanagement den möglichen Schaden.

Sichere KI beginnt bei den Zugriffsrechten

Mit KI-Assistenten wird das noch wichtiger. KI kann Informationen aus großen Datenbeständen in Sekunden finden und zusammenführen. Sind Zugriffsrechte zu großzügig, kann sie bestehende Fehlberechtigungen sichtbar machen: Tief in Ablagen verborgene Informationen lassen sich plötzlich leicht finden. AI Readiness beginnt deshalb nicht mit der Wahl eines KI-Modells. Unternehmen müssen vorher ihre Daten und Rechte beherrschen: Wer darf worauf zugreifen? Welche Freigaben sind noch nötig? Welche Daten dürfen Beschäftigte mit welchen KI-Werkzeugen verarbeiten? Erst dann lässt sich KI kontrolliert in Arbeits- und Sicherheitsprozesse integrieren.

Human Risk ist auch eine Frage der Architektur

Der Mensch ist nicht automatisch das schwächste Glied. Beschäftigte handeln innerhalb der Systeme, Prozesse und Rechte, die ein Unternehmen vorgibt.

Modernes Human Risk Management verbindet deshalb drei Ebenen: Adaptive Trainings stärken die Handlungssicherheit. Technische Leitplanken fangen riskante Situationen im Arbeitsablauf ab. Least Privilege begrenzt die Reichweite kompromittierter Konten. •

IDENTITÄT –
Der Spagat zwischen Nutzererlebnis und Deepfake-Abwehr

Identität wird bei zahlreichen Prozessen geprüft, wie beim Onboarding, bei Transaktionen oder beim Zurücksetzen von Zugangsdaten. Zu oft gelten diese Prüfungen als isolierte Einzelschritte statt als zusammenhängende Verteidigung. Da Angreifer generative KI nutzen, um Schwachstellen automatisiert auszunutzen, genügt es nicht mehr zu wissen, worauf ein Konto zugreifen darf. Daher müssen IT-Security-Teams fortlaufend prüfen, wer hinter einer Sitzung steht. /// von Matt Berzinski

DER AUTOR
Matt Berzinski
ist Field Chief Technology Officer, EMEA bei Ping Identity.
Bild: Ping Identity

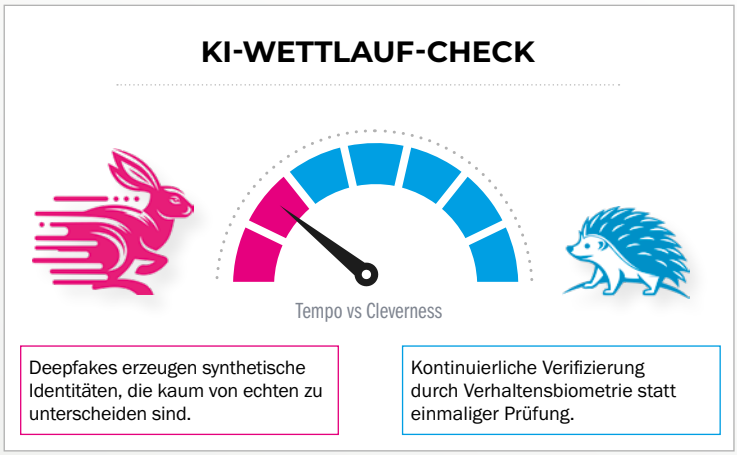
DIE IT-ARCHITEKTUR IN UNTERNEHMEN HABEN SICH GEWANDELT: Autonome KI-Agenten, Coding-Assistenten und automatisierte Desktop-Werkzeuge steuern heute Arbeitsabläufe, schreiben Code und konfigurieren die IT-Infrastruktur. Damit ist die Identität zur zentralen Kontrollebene geworden. Modernes, KI-gestütztes Identity & Access Management (IAM) muss dieser doppelten Realität gerecht werden: Es bewertet das Laufzeitrisiko im Zugriffspfad dynamisch und stellt zugleich eine AI-first, headless administrierbare Ebene bereit, über die menschliche Entwickler wie autonome Agenten die Sicherheitsinfrastruktur in Maschinengeschwindigkeit konfigurieren, prüfen und anpassen.

Komfort und Sicherheit sind kein Widerspruch mehr
Jahrelang galt, dass mehr Sicherheit mehr Reibung bedeutet. Diese Logik ist überholt. Der Grundpfeiler einer wirksamen Verteidigung ist eine risikobasierte Authentifizierung, die jede Sitzung in Echtzeit bewertet und aufdringliche Prüfungen den risikoreichen Auffälligkeiten vorbehält. Für die große Mehrheit legitimer Nutzer erfolgt die Bestätigung nahtlos im Hintergrund, sodass Sicherheitsteams ihre Aufmerksamkeit dorthin lenken, wo das Risiko tatsächlich liegt.

Angetrieben wird diese unsichtbare Ebene von passiven, die Privatsphäre schonenden Signalen. Verhaltensbiometrie erfasst Muster wie Tipprhythmus und Wischdynamik, Gerätetelemetrie liefert einen anonymisierten Fingerabdruck der Konfiguration, und Geo-Velocity-Prüfungen erkennen physisch unmögliche Ortswechsel. Diese Eingaben speisen eine KI-gestützte Risiko-Engine: Vertrauenswürdige Sitzungen laufen ungehindert durch, grenzwertige lösen eine zusätzliche Prüfung aus, klare Bedrohungen werden sofort blockiert. Reibung ist nicht länger die Grundeinstellung, sondern eine gezielte Reaktion, die Nutzerbindung und Konversionsraten schützt.

Passwörter allein genügen nicht mehr
Statische Zugangsdaten sind von Natur aus kompromittiert, leicht per Phishing abzugreifen und über automatisierte Angriffswege wiederzuverwenden. Moderne Authentifizierung verzichtet vollständig auf geteilte Geheimnisse und bindet den Zugriff an ein vertrauenswürdiges Gerät und kryptografische Biometrie (etwa FIDO2 oder Passkeys). Für europäische Unternehmen entscheidend: Fortgeschrittene IAM-Architekturen vereinen robuste Sicherheit mit strenger DSGVO-Konformität. Indem sie auf zentrale biometrische Datenspeicher verzichten und auf

> Der Grundpfeiler einer wirksamen Verteidigung ist eine risikobasierte Authentifizierung, **die jede Sitzung in Echtzeit bewertet** und aufdringliche Prüfungen den risikoreichen Auffälligkeiten vorbehält.
>
> *Matt Berzinski*



dezentrale Verifizierung setzen, etwa über Zero-Knowledge-Proofs und nutzerkontrollierte digitale Identitäts-Wallets, eliminieren sie das Risiko eines „Honeypots" und geben Nutzern die souveräne Kontrolle über ihre Daten.

Deepfakes verlangen den Nachweis eines echten Menschen

Die größte Verschiebung 2026 ist die Demokratisierung synthetischer Identitäten. Früher genügten die Authentifizierung des Kontos und dessen Berechtigungen als Mittel der Sicherheit. In der Welt der Deepfakes lässt sich nicht mehr darauf vertrauen, dass ein Konto tatsächlich vom rechtmäßigen Inhaber kontrolliert wird. Nun muss die Identitätsprüfung feststellen, ob der tatsächliche Mensch anwesend ist. Einmal etabliert, lässt sie sich jedes Mal wiederverwenden, wenn eine vollständige Authentifizierung nötig ist, und bestätigt, dass dieser Mensch berechtigt ist, in genau diesem Moment diese Aktion auszuführen.

Fortgeschrittene Identitätsprüfung kombiniert heute mehrschichtige passive Liveness Detection, Abwehr von Injection-Angriffen und einen Echtzeitabgleich mit offiziellen Registern. Die Prüfergebnisse werden zu wiederverwendbaren, kryptografisch signierten Identitätssignalen. So bleibt die reibungsintensive erneute Prüfung risikoreichen Aktionen vorbehalten, was Sicherheit und Effizienz zugleich wahrt.

Von der einmaligen Prüfung zum kontinuierlichen Vertrauen

Der wichtigste Wandel betrifft den Zeitpunkt der Prüfung. Identität ist kein einmaliges Ereignis, sondern eine fortlaufende Kette. Eine Verifizierung bei der Registrierung genügt nicht, wenn danach niemand mehr sicherstellt, dass dieselbe Person das Konto bedient. Genau diese Lücke nutzen Kontoübernahmen und gekaperte Sitzungen. In einem Modell des kontinuierlichen Vertrauens wird die Identität an allen kritischen Türen erneut bestätigt, bei Anmeldung, Transaktion, Wiederherstellung und im Helpdesk-Kontakt, statt nach einer einzigen Prüfung als gegeben angenommen zu werden. Verhält sich eine vertrauenswürdige Sitzung plötzlich auffällig, erhöht das System die Anforderungen in Echtzeit oder unterbricht den Zugriff.

Identität als durchgängige Kontrollebene

Sicherheit wird nicht mehr durch einen statischen Netzwerkperimeter definiert, sondern durch Identitätsentscheidungen in Echtzeit: Wer oder was handelt gerade, ist der Kontext vertrauenswürdig, und ist diese Aktion autorisiert? Indem Organisationen kontinuierliche Bedrohungsabwehr mit einer AI-first, headless administrierbaren Kontrollebene vereinen, verwandeln sie IAM von einer statischen Sicherheitslast in einen agilen operativen Wegbereiter. 2026 ist Identität das Schlachtfeld. Unternehmen, die sie als kontinuierliche, intelligente und vollständig programmierbare Kontroll-Engine begreifen, gewinnen zugleich das Vertrauen ihrer Nutzer und die volle Kontrolle über ihre digitale Infrastruktur. •

Von Legacy zu „Never Trust, Always Verify"

Zero Trust wurde lange als vorwiegend reines IT-Thema angesehen, bei dem es vor allem um die Überprüfung von Identitäten oder den Schutz vor unberechtigten Zugriffen zur Sicherung von Daten und Netzwerken ging. /// von Moritz Schmidt

DER ZERO-TRUST-ANSATZ REICHT JEDOCH WEIT DARÜBER HINAUS. In einer zunehmend regulierten und vernetzten Welt wird Zero Trust immer mehr zur strategischen Transformationsaufgabe, die alle Ebenen der IT-Infrastruktur durchdringt. Mit dem wachsenden Einsatz von KI-Agenten, die als technische Akteure untereinander kommunizieren und eigenständig auf Anwendungen, Daten und Prozesse zugreifen, kommen neue Anforderungen an Authentifizierung, Autorisierung und Nachvollziehbarkeit hinzu.

Unternehmen müssen sicherstellen, dass sowohl menschliche als auch maschinelle Identitäten ausschließlich auf die Ressourcen zugreifen können, die sie für eine konkrete Aufgabe tatsächlich benötigen. Das Grundprinzip von Zero Trust bleibt unverändert: Es gilt, Zugriffe nicht selbstverständlich zu gewähren, sondern nachvollziehbar, angemessen begrenzt und überprüfbar zu gestalten. Dabei besteht die Kunst darin, eine optimale Balance zwischen Compliance und Produktivität zu erreichen.

Priorisierung der Risiken statt Aktionismus

In der Praxis liegt die Herausforderung weniger in der Zielarchitektur, sondern darin, Sicherheit kontinuierlich zu verbessern und Legacy-Systeme schrittweise in eine „Never Trust, Always Verify"-Strategie zu überführen. Solche Vorhaben scheitern oft am Versuch, alles gleichzeitig umzusetzen und verursachen dann Überforderung, Widerstände sowie operative Störungen. Erfolgreiche Unternehmen setzen stattdessen auf Priorisierung. Sie starten dort, wo Risiken und die Wirkung am größten sind: bei Identitäten, privilegierten Berechtigungen, kritischen Daten und besonders sensiblen Anwendungen. Darauf folgen die Segmentierung von Umgebungen und schrittweise Integration von Legacy-Systemen in moderne Sicherheitsarchitekturen. Dabei geht es nicht darum, vom ersten Tag an eine perfekte Zielarchitektur zu erreichen. Entscheidend ist vielmehr ein realistischer Migrationspfad, der operative Abhängigkeiten berücksichtigt und die Möglichkeit bietet, Ausnahmen transparent zu steuern.

Governance und Transparenz als Erfolgsfaktoren

Damit die Umsetzung einer Zero-Trust-Strategie gelingt, werden eindeutige Verantwortlichkeiten, messbare Ziele, geeignete Kennzahlen und eine genau definierte Governance benötigt. Die Transformation betrifft nicht nur die IT, sondern ebenso Management, Fachbereiche, Datenschutz, Betrieb und Risikomanagement. Der Schlüssel liegt darin, Sicherheit als unternehmensweite Aufgabe zu verstehen. Zero Trust wirkt nur dann, wenn technische Maßnahmen, organisatorische Prozesse und regulatorische Anforderungen zusammen betrachtet werden.

Neben all den Herausforderungen bietet die Umsetzung des Zero-Trust-Ansatzes aber auch eine oft unterschätzte Chance: Indem Unternehmen einen Überblick über Altlasten bei Identitäten und Berechtigungen gewinnen und diese beseitigen, stärken sie nicht nur ihre Sicherheitsarchitektur, sondern schaffen die Grundlage für eine resilientere, transparentere und zukunftsfähige IT. •

DER AUTOR
Moritz Schmidt
ist Managing Consultant bei Axians magellan. In dieser Rolle berät er Kunden bei der strategischen Weiterentwicklung ihrer IT-Sicherheitsarchitektur, der Bewertung von Risiken und Umsetzung nachhaltiger Maßnahmen zur Stärkung der Cyberresilienz.
Bild: Axians magellan

> „ Bei der Umsetzung von Zero Trust besteht die Kunst darin, eine **optimale Balance zwischen Compliance und Produktivität** zu erreichen. *Moritz Schmidt*

SECURITY
braucht mehr als starke Firewalls

Cybersecurity dominiert die Sicherheitsdebatte. Doch wer digitale Geschäftsprozesse, Daten und Anwendungen schützen will, muss weiterdenken: bis zum Serverraum, zum Edge-Standort und zum Rechenzentrum. Denn eine Firewall verhindert keinen Wasserschaden, keine manipulierte Hardware und keinen unbefugten Zutritt.

GERADE BETREIBER KRITISCHER INFRASTRUKTUREN STEHEN VOR DER AUFGABE, Sicherheit ganzheitlich zu betrachten. NIS-2 und das KRITIS-Dachgesetz rücken Resilienz, Risikomanagement und Schutzmaßnahmen stärker in den Fokus. Dabei geht es nicht nur um Angriffe aus dem Netz. Auch physische Gefahren können digitale Systeme lahmlegen – mit Folgen für Versorgung, Produktion, Verwaltung oder Gesundheitswesen.

Physische Sicherheit als Teil der Cyberresilienz

Drohnenangriffe, Sabotage, Abhör- und Kompromittierungsversuche, Hardwarediebstahl oder gezielte Beschädigungen betreffen längst nicht mehr nur militärische Einrichtungen. Unternehmen aller Branchen und Größen können zum Ziel werden: aus wirtschaftlichen, politischen oder kriminellen Motiven. Je stärker Geschäftsmodelle von Daten, Cloud-Anwendungen und vernetzten Prozessen abhängen, desto kritischer wird die Infrastruktur, auf der diese Systeme laufen. Physische IT-Sicherheit beginnt deshalb nicht erst bei der Zutrittskontrolle. Sie umfasst Standort- und Risikoanalysen, Schutzkonzepte für Serverräume und Rechenzentren, gesicherte Hardware-Umgebungen, Brandschutz, Klimatisierung, Energieversorgung, Monitoring, Notfallhandbücher und klare Betriebsprozesse. Entscheidend ist, dass technische, organisatorische und bauliche Maßnahmen ineinandergreifen.

„Cybersecurity und physische Sicherheit dürfen nicht getrennt gedacht werden. Wer kritische Systeme schützen will, muss wissen, wo die eigenen Risiken liegen, welche Infrastruktur wirklich geschäftskritisch ist und wie der Betrieb auch im Störfall gesichert bleibt“, sagt Christian Raab, Leiter Vertrieb Mitte bei der Data Center Group.

Vom Risiko zur belastbaren Schutzstrategie

Für Unternehmen aus KRITIS-Sektoren zählt vor allem eines: Schutzmaßnahmen müssen nachvollziehbar, wirksam und belastbar sein. Sicherheitskonzepte sollten deshalb nicht auf Einzelmaßnahmen beruhen, sondern auf einer strukturierten Analyse. Welche Systeme sind unverzichtbar? Welche physischen Bedrohungen bestehen am Standort? Wer hat Zugriff? Wie wird auf Störungen reagiert? Und wie schnell kann der Betrieb wiederhergestellt werden? Aus diesen Antworten entsteht eine Schutzstrategie, die Beratung, Risikoanalyse, bauliche und technische Sicherheit, Zugriffsschutz, Hardware-Schutz, Betriebskonzepte und Notfallprozesse miteinander verbindet. Erst wenn diese Ebenen sauber aufeinander abgestimmt sind, entsteht ein Sicherheitsniveau, das nicht nur regulatorische Anforderungen adressiert, sondern auch im Ernstfall trägt.

Das Ziel ist nicht mehr Sicherheit um ihrer selbst willen. Es geht um Verfügbarkeit, Handlungsfähigkeit und Vertrauen. In einer vernetzten Wirtschaft endet Security nicht an der digitalen Schnittstelle. Sie beginnt dort, wo die digitale Infrastruktur physisch steht. •

Christian Raab
Vertriebsleiter Mitte
Data Center Group

Rechenzentrums-Container mit Perimeterschutz, Videoüberwachungsanlage, Brandfrüherkennung, unterbrechungsfreier Stromversorgung und reduntanter freier Kühlung.

Kontakt und weitere Informationen:

Christian Raab,
Vertriebsleiter Mitte
Data Center Group
Mobile: +49 151 22504 128
christian.raab@datacenter-group.com
www.datacenter-group.com

Data Center Group

ÜBER DIE DATA CENTER GROUP

Die Data Center Group ist ein führender Anbieter für die Entwicklung, Beratung, Planung, Bau und Betrieb von Rechenzentren sowie für Hochsicherheits-Produkte rund um sichere und hochverfügbare IT-Infrastrukturen. Seit der Gründung 2005 hat das Unternehmen sein Portfolio stetig erweitert und beschäftigt heute rund 250 Mitarbeiter an mehreren Standorten in ganz Deutschland. Der Hauptsitz im Westerwald liegt strategisch günstig nahe den wichtigen Internetknoten DE-CIX Frankfurt und DE-CIX Düsseldorf. Weitere Büros befinden sich in Berlin, Frankfurt, München und Köln.

Die dunkle Seite der Autonomie

Agentic AI verändert die Spielregeln der Cybersicherheit nicht, weil plötzlich völlig neue Schwachstellen entstehen. Das eigentliche Problem ist, dass bekannte Angriffsmethoden eine neue Qualität erreichen. Gelingt es den Kriminellen, die zugrunde liegende Infrastruktur zu kompromittieren, erlangen sie die Kontrolle über die gesamte Umgebung und somit auch über die KI-Agenten. /// von Peter Dümig

EIN UNTERNEHMEN INVESTIERT GROSSE SUMMEN IN AGENTIC AI. Sicherheitsrichtlinien sind definiert, Identitäten sauber verwaltet und Prompt-Injection-Filter aktiviert. Trotzdem gelingt es einem Angreifer, die Umgebung zu übernehmen – nicht über das Sprachmodell, sondern über eine kompromittierte Firmware tief unterhalb des Betriebssystems. Von dort aus bewegt er sich nahezu unbemerkt durch die Infrastruktur, kapert Zugriffsrechte und nutzt schließlich die vorhandenen KI-Agenten, um Angriffe zu automatisieren, Daten zu exfiltrieren oder ganze Prozesse lahmzulegen.

KI macht Angriffe zum Kinderspiel

Noch vor wenigen Jahren benötigte eine professionelle Hackergruppe Wochen oder sogar Monate, um eine Unternehmensumgebung auszukundschaften. Systeme mussten identifiziert, Schwachstellen recherchiert, Berechtigungen analysiert und Angriffspfade manuell aufgebaut werden. Heute erledigen KI-gestützte Werkzeuge große Teile dieser Arbeit innerhalb weniger Minuten. Sie durchsuchen Netzwerke nach verwundbaren Systemen, gleichen Konfigurationen automatisiert mit bekannten CVEs ab, generieren passende Exploits und schlagen den nächsten Angriffsschritt vor. Mit Agentic AI entwickelt sich dieser Prozess zur nahezu autonomen Angriffskette: Mehrere spezialisierte Agenten können parallel Informationen sammeln, Entscheidungen treffen und Aktionen koordinieren. Genau darin liegt die eigentliche Herausforderung in puncto Sicherheit. Agentic AI erzeugt keine grundlegend neuen Schwachstellen. Im Gegenteil: Eine ungepatchte Firmware stellt nach wie vor die gleiche Schwachstelle dar wie vor fünf Jahren. Ein fehlerhaft konfigurierter Management-Controller oder ein kompromittiertes UEFI waren schon immer attraktive Angriffsziele. Neu ist jedoch die Geschwindigkeit, mit der solche Schwachstellen gefunden, ausgenutzt und für komplexe Angriffe kombiniert werden können.

Wer einmal drin ist, hat Zugriff auf alles

KI macht Cyberkriminalität skalierbar, wodurch sich zwangsläufig der Blick auf die Verteidigung verändern muss. Unternehmen diskutieren derzeit vor allem über Prompt Injection, Guardrails oder die sichere Entwicklung von KI-Agenten. Diese Themen sind zweifellos wichtig. Häufig wird Agent-Hijacking jedoch „nur" als Angriff auf das Sprachmodell verstanden. Tatsächlich beginnt eine erfolgreiche Kompromittierung oft deutlich früher. Werden Schwachstellen in der Hardware ausgenutzt, arbeitet der Schadcode unterhalb des Betriebssystems und bleibt für klassische Sicherheitstools in der Regel unsichtbar.

Die Folgen reichen dabei weit über den Zugriff auf einen einzelnen Server hinaus. Von einer kompromittierten Infrastruktur aus lassen sich Identitäten übernehmen, privilegierte Berechtigungen ausweiten und weitere Systeme infiltrieren. Genau an diesem Punkt entsteht die Verbindung zu Agentic AI. KI-Agenten besitzen nämlich häufig weitreichende Zugriffe auf Unternehmensdaten, APIs, Automatisierungsplattformen oder Geschäftsanwendungen. Wer diese Infrastruktur kontrolliert, kann nicht nur Daten stehlen oder Systeme verschlüsseln. Er kann die Agenten auch für eigene Zwecke instrumentalisieren und ihre Fähigkeit zur Automatisierung missbrauchen.

Damit entsteht gewissermaßen ein Botnetz der nächsten Generation. Während klassische Botnetze kompromittierte Rechner für DDoS-Angriffe oder Spam-Kampagnen nutzen, können autonome Agenten künftig komplexere Aufgaben übernehmen: Informationen sammeln, Geschäftsprozesse manipulieren, Finanztransaktionen vorbereiten oder koordinierte Angriffe auf weitere Systeme durchführen.

KI-Sicherheit muss als Gesamtsystem gedacht werden

Genau deshalb gewinnt das Konzept der „Security below the OS" an Bedeutung. Dabei handelt es sich nicht um ein einzelnes Sicherheitsprodukt, sondern um ein Architekturprinzip. Das Ziel besteht darin, die Integrität einer Plattform bereits vor dem Start des Betriebssystems sicherzustellen. Hardwarebasierte Root-of-Trust-Mechanismen, kryptografisch signierte Firmware, Secure Boot oder Remote Attestation bilden dabei eine durchgängige Vertrauenskette. Bei jedem Bootvorgang wird überprüft, ob Firmware, BIOS beziehungsweise UEFI sowie weitere Systemkomponen-

Mit Agentic AI verschiebt sich die Vertrauensgrenze von der Anwendung auf die Infrastruktur. Die Integrität von Hardware, Firmware und Betriebssystem wird zur Voraussetzung für sichere autonome Entscheidungen.
(Quelle: Gettyimages / Marco VDM)

ten unverändert sind. Manipulierte Software wird erkannt, bevor sie aktiv werden kann. Ebenso wichtig sind kontinuierliche Integritätsprüfungen während des Betriebs. Diese machen unautorisierte Änderungen an Firmware oder sicherheitskritischen Komponenten sichtbar.

Für Unternehmen bedeutet das einen Perspektivwechsel. Die Infrastruktur stellt nicht nur Rechenleistung für die KI bereit. Sie wird vielmehr selbst zum Fundament der Sicherheitsarchitektur. Letztlich muss jede autonome Entscheidung eines Agenten auf der Annahme basieren, dass die zugrunde liegende Plattform vertrauenswürdig arbeitet. Fällt diese Annahme weg, verlieren sämtliche darüberliegenden Sicherheitsmaßnahmen an Bedeutung. Die Einführung von Agentic AI verändert deshalb nicht nur technische Architekturen, sondern auch Verantwortlichkeiten. Infrastruktur-, Plattform-, Security- und KI-Teams dürfen nicht länger isoliert arbeiten.

Fazit: Agentic AI ist nur so sicher wie ihre Infrastruktur

Das heißt, wer KI-Agenten produktiv einsetzt, muss sicherstellen, dass Firmware, Betriebssystem, Virtualisierung, Identitäten und Anwendungen als zusammenhängende Vertrauenskette abgesichert werden. Dazu gehören selbstverständlich weiterhin etablierte Security-Prinzipien wie Least Privilege, Zero Trust, Netzwerksegmentierung oder eine konsequente Härtung der Plattform. Jede KI-Plattform benötigt aber auch nachvollziehbare Integritätsprüfungen, kontinuierliche Firmware-Updates, kryptografisch abgesicherte Boot-Prozesse sowie die Fähigkeit, Manipulationen an der Infrastruktur zuverlässig zu erkennen. Erst auf dieser Basis lassen sich autonome Systeme sicher betreiben. •

KI-WETTLAUF-CHECK

KI-Tools finden Schwachstellen unterhalb des Betriebssystems, unsichtbar für Standard-Tools.

Hardware-Root-of-Trust prüft die Plattform, bevor Agentic AI überhaupt startet.

DER AUTOR
Peter Dümig
ist Senior Server Product Manager bei Dell Technologies in Deutschland.
(Quelle: Dell Technologies)

Von Zero Trust zu Zero Trust Plus: Vertrauen allein reicht nicht mehr

Zero Trust beantwortet die Frage, wem Unternehmen vertrauen können. Der Ansatz Zero Trust Plus geht weiter und beschreibt, was passiert, wenn dieses Vertrauen missbraucht wird. /// von Michael Klatte

MULTI-FAKTOR-AUTHENTIFIZIERUNG, IDENTITY MANAGEMENT, ZERO-TRUST-INITIATIVEN: Viele Unternehmen haben in den vergangenen Jahren erheblich in ihre Sicherheitsarchitektur investiert. Trotzdem lesen wir fast jede Woche von erfolgreichen Angriffen auf Organisationen, die eigentlich nach modernen Standards abgesichert sind. Denn Angreifer versuchen heute seltener, Schutzmechanismen frontal zu überwinden. Stattdessen nutzen sie, was bereits vorhanden ist, nämlich gültige Konten, bestehende Sitzungen oder legitim vergebene Rechte.

Ein Fall aus der Praxis: Anmeldedaten stimmen, MFA wurde erfolgreich durchlaufen, das Gerät ist bekannt. Aus Sicht vieler Sicherheitslösungen sieht alles normal aus. Die entscheidende Frage lautet deshalb nicht mehr nur, wer Zugriff erhält, sondern was nach der Anmeldung geschieht. Genau hier stößt die klassische Zero Trust-Interpretation an ihre Grenzen.

Zero Trust als Fundament

Der Grundgedanke von Zero Trust bleibt richtig. Vertrauen darf nicht automatisch vergeben werden, jeder Benutzer, jedes Gerät und jede Anwendung muss seine Legitimität fortlaufend nachweisen. Klassische Netzwerkgrenzen sind durch Cloud-Dienste, mobiles Arbeiten und hybride Infrastrukturen längst aufgelöst. Deshalb rückte die Identität in den Mittelpunkt: MFA, Least Privilege, Privileged Access Management und kontextabhängige Zugriffsentscheidungen bilden bis heute das Fundament jeder Zero-Trust-Strategie. Viele Unternehmen betrachten die MFA-Einführung bereits als Abschluss ihrer Zero-Trust-Initiative. Tatsächlich beginnt die eigentliche Arbeit erst danach, denn auch ein legitim angemeldeter Nutzer kann zum Risiko werden.

Wenn Angreifer legitime Identitäten nutzen

Ein Mitarbeiter klickt auf einen Phishing-Link, Zugangsdaten werden abgegriffen, die Sitzung kompromittiert und schon meldet sich ein Angreifer mit denselben Rechten an wie der echte Nutzer. Noch heikler sind Angriffe auf bestehende Sitzungen. Cyberkriminelle stehlen keine Passwörter mehr, sondern übernehmen gültige Session-Tokens. Für Sicherheitsmechanismen erscheint der Angreifer dann als bereits authentifizierter Benutzer, denn die MFA wurde längst erfolgreich abgeschlossen und greift nicht mehr. Konto, Rechte und Umgebung wirken legitim, alle klassischen Zero-Trust-Kontrollen wurden passiert. Jetzt beginnt die Phase, in der sich Angreifer ausbreiten, weitere Systeme kompromittieren oder Daten abziehen. Selbst die beste Zugangskontrolle kann nicht verhindern, dass ein bereits kompromittiertes Konto missbraucht wird.

Warum Sichtbarkeit noch wichtiger wird

Viele Sicherheitsvorfälle blieben tage- oder wochenlang unentdeckt. Nicht nur wegen fehlender Tools, sondern weil relevante Informationen verstreut lagen und niemand das Gesamtbild erkannte. Unternehmen müssen deshalb nachvollziehen können, welche Identitäten auf welche Systeme zugreifen, welche Anwendungen kommunizieren und welche Aktivitäten vom Normalverhalten abweichen. Besonders in Cloud-Umgebungen, wo Identitäten den Zugriff auf verteilte Dienste steuern, bleiben

DER AUTOR
Michael Klatte
ist Security-Experte bei Eset.
Bild: Eset

> **Der Zero-Trust-Plus-Ansatz ersetzt die bewährten Prinzipien von Zero Trust nicht**, sondern erweitert sie um die Fähigkeiten, die Unternehmen heutzutage benötigen, weil erfolgreiche Angriffe trotz aller Schutzmaßnahmen jederzeit möglich sind.
>
> *Michael Klatte*

Fehlkonfigurationen oder missbrauchte Berechtigungen ohne kontinuierliches Monitoring oft lange unbemerkt. Es reicht nicht mehr, den Zugang zu kontrollieren. Unternehmen müssen verstehen, was in ihrer Umgebung tatsächlich passiert.

Detection und Response schließen die Lücke

Während die erste Generation von Zero Trust-Projekten vor allem auf Identitäten und Berechtigungen setzte, rücken heute Erkennung und Reaktion in den Mittelpunkt. Endpoint-, Extended- und Managed Detection and Response (EDR, XDR, MDR) analysieren Aktivitäten, korrelieren Ereignisse aus verschiedenen Quellen und erkennen verdächtige Muster. Vor allem schauen sie auch dort, wo einzelne Signale harmlos wirken. Ein ungewöhnlicher Login allein ist kein Problem; in Kombination mit plötzlichem Datenabzug oder auffälligen Netzwerkverbindungen entsteht ein ganz anderes Bild.

Mit Identity Threat Detection and Response (ITDR) rücken zudem Identitäten selbst in den Fokus der Überwachung. So werden kompromittierte Konten und missbrauchte Rechte gezielt erkannt. Threat Intelligence liefert den Kontext, um Risiken schneller einzuordnen und Prioritäten zu setzen. Für diese Weiterentwicklung hat sich der Begriff Zero Trust Plus etabliert.

Was Zero Trust Plus bedeutet

Zero Trust Plus ist kein Ersatz und kein neues Framework, sondern die konsequente Weiterentwicklung eines Modells, das lange vor allem Identitäten und Zugriffsentscheidungen im Blick hatte. Vier Aspekte stehen im Zentrum:

- Identität: MFA, Least Privilege und kontextabhängige Zugriffsrichtlinien als Basis.
- Sichtbarkeit: Durchgängige Transparenz über Identitäten, Endgeräte und Cloud-Ressourcen.
- Detection & Response: Frühzeitiges Erkennen und Eindämmen von Angriffen mittels EDR, XDR, MDR und ITDR.
- Cyber Resilience: Die Fähigkeit, Vorfälle schnell zu bewältigen und den Betrieb aufrechtzuerhalten.

Der Fokus verschiebt sich damit von der Frage, ob ein Angriff stattfindet, hin zur Frage, wie schnell er erkannt und eingedämmt wird.

Cyber Resilience als neue Messgröße

Auch regulatorische Vorgaben wie NIS2 oder DORA beschleunigen diesen Wandel. Gefordert werden längst nicht mehr nur Präventionsmaßnahmen, sondern kontinuierliche Überwachung, strukturierte Reaktionsprozesse und belastbare Incident Response-Fähigkeiten. Die entscheidende Frage lautet nicht mehr nur „Wie verhindern wir einen Angriff?", sondern zunehmend „Wie schnell erkennen wir ihn, und wie wirksam begrenzen wir die Folgen?" In modernen IT-Umgebungen lässt sich nicht jeder Angriff verhindern. Viel relevanter ist die Frage, , wie schnell ein Unternehmen erkennt, dass etwas nicht stimmt.

Genau hier liegt die Bedeutung von Zero Trust Plus. Der Ansatz ersetzt die bewährten Prinzipien von Zero Trust nicht, sondern erweitert sie um die Fähigkeiten, die Unternehmen heutzutage benötigen, weil erfolgreiche Angriffe trotz aller Schutzmaßnahmen jederzeit möglich sind. Vertrauen darf auch künftig nicht vorausgesetzt werden. Die eigentliche Herausforderung besteht darin, verdächtige Aktivitäten rechtzeitig zu erkennen und die richtigen Konsequenzen daraus zu ziehen. •

Der resiliente Arbeitsplatz
kennt keinen festen Standort

Ein global skalierbarer Sicherheitsansatz für hybride Arbeitsumgebungen entkoppelt das Schutzniveau heute vollständig vom physischen Standort des Endgeräts. Diese Strategie vereint kompromisslose Compliance-Standards mit der notwendigen Agilität moderner Belegschaften und sorgt durch die Zentralisierung der Sicherheitsverwaltung für eine signifikante Entlastung der internen IT-Ressourcen. /// von Gerald Eid

BEIM KLASSISCHEN ARBEITSPLATZ GAB ES EINEN KLAREN MITTELPUNKT. Im Büro standen die Geräte, und dort griffen die Sicherheitskontrollen für den Zugang zu den Anwendungen. Für hybride Arbeitsmodelle trägt diese Logik nicht mehr. Ein Notebook läuft heute im Unternehmensnetz, im Homeoffice, im Hotel oder in einem fremden WLAN, und für die Sicherheit darf dieser Ortswechsel keinen Unterschied machen. Sicherheitsfunktionen verlagern sich damit auf das Endgerät selbst, das seinen Zustand melden und Richtlinien auch ohne Verbindung zum Unternehmensnetz durchsetzen muss.

Angreifer wissen das. Nach dem ENISA Threat Landscape 2025 entfallen 60 Prozent der Erstzugriffe auf Phishing und 21,3 Prozent auf ausgenutzte Schwachstellen. Beide Wege setzen an Zugangsdaten und Gerät einzelner Beschäftigter an, nicht an der Netzgrenze. Ransomware bleibt die folgenreichste Bedrohung für Organisationen in der EU, und ihr Angriffspunkt liegt dort, wo die klassische Perimeterkontrolle am wenigsten greift.

Endpoint-Schutz und Identitätsmanagement

Ein resilienter Arbeitsplatz setzt deshalb auf Kontrollen, die sich an der konkreten Zugriffssituation orientieren, an der Identität des Benutzers und am Zustand des Geräts. Genau hier setzt Zero Trust an. Das NIST beschreibt in SP 800-207 eine Architektur, in der weder Benutzer noch Geräte allein aufgrund ihres Standorts oder einer früheren Authentifizierung als vertrauenswürdig gelten. Zugriffe werden bei jeder Sitzung geprüft und auf die erforderlichen Ressourcen begrenzt.

In der Praxis müssen dafür Endpoint-Schutz und Identitätsmanagement eng zusammenarbeiten. Ein verwaltetes Gerät meldet seinen Sicherheitsstatus kontinuierlich an die zentrale Verwaltung, und fehlende Updates oder ungewöhnliche Aktivitäten fließen in die Entscheidung über den weiteren Zugriff ein. Die Richtlinien werden zentral festgelegt und gelten unabhängig vom Standort des Geräts. Das verschärft sich, sobald Unternehmen Cloud-Anwendungen beziehen und generative KI einbinden. KI-Dienste greifen im Namen des Benutzers auf Dokumente und Fachanwendungen zu und verarbeiten sensible Unternehmensdaten. Sie brauchen deshalb dieselben Regeln für Identität und Berechtigungen wie jede andere Ressource. Entstehen diese Regeln erst nachträglich, wächst die Zahl der Sonderfälle schneller als die der Anwendungen, und die Infrastruktur verliert ihre Skalierbarkeit.

DER AUTOR
Gerald Eid
ist Regional Managing Director DACH bei Getronics.

Welche Instanz entscheidet über Identität und Gerätezustand?

Eine zentral gesteuerte Architektur zahlt sich weniger über einzelne Funktionen aus als über die Einheitlichkeit der Durchsetzung. Die interne IT konfiguriert und überwacht zentral, statt an jedem Arbeitsplatz eigene Kontrollen zu unterhalten, und kann im Ereignisfall von dort reagieren. Der Standort des Endgeräts bestimmt das Sicherheitsniveau dann nicht mehr, er ist nur noch eine Variable in der Zugriffsentscheidung. Für hybride Umgebungen ist das entscheidend, denn Ausnahmen für einzelne Standorte oder Gerätegruppen sind die Stelle, an der Sicherheitsarchitekturen im Betrieb auseinanderfallen.

Der wichtigste Prüfschritt ist deshalb, bei jeder neuen Anwendung und besonders bei jedem KI-Dienst vorab festzulegen, welche Instanz über Identität und Gerätezustand entscheidet. Nachträglich lässt sich das nur mit Ausnahmen nachbilden, und jede Ausnahme überlebt das Projekt, in dem sie entstanden ist. •

„AI ist längst Teil der Angriffslandschaft"

Elisabetta Castiglioni,
CEO A1 Digital

2026 wird für die Cybersicherheit ein Jahr, in dem künstliche Intelligenz die Bedrohungslage maßgeblich prägt.

AI ist längst fixer Bestandteil der Angriffslandschaft: Ein großer Teil der Phishing Kampagnen wird automatisiert erstellt, und auch weniger versierte Angreifer erhalten Fähigkeiten, die früher professionellen Gruppen vorbehalten waren. Fehlerfreier Code, überzeugende Phishing Mails oder automatisierte Angriffsschritte senken die Einstiegshürden und erhöhen das Schadenspotenzial – besonders bei Insider Risiken.

Zugleich entsteht eine neue Qualität von Angriffen: hochgradig personalisiertes Spear Phishing, lernende Web Exploits und AI Agenten, die sich in Echtzeit anpassen. Klassische, rein reaktive Schutzmechanismen reichen dafür nicht mehr aus. Unternehmen müssen ihre Sicherheitsarchitekturen automatisieren, adaptiv gestalten und Threat Intelligence in Echtzeit integrieren.

AI ist für mich jedoch nicht nur Teil des Problems, sondern ein zentraler Baustein der Defensive. Intelligente Systeme erkennen Muster, die Menschen verborgen bleiben, und reagieren nahezu in Echtzeit. Bei **A1 Digital** entwickeln wir Lösungen, die menschliche Expertise mit maschineller Intelligenz verbinden – von AI gestützter Anomalieerkennung über automatisierte Incident Response bis zu sicherem Edge Computing und dem Schutz industrieller Systeme und kritischer Infrastrukturen.

Nur durch diesen integrierten Ansatz können Unternehmen den Anforderungen des Jahres 2026 gerecht werden. •

MEHR ERFAHREN AUF DER IT-SA 2026

- **Live-Vortrag: Stayin' Alive – Wie das WAN resilient wird**

  Datum und Zeit: 27.10.2026 | 14:00-14:15
  Ort: Halle 9 Forum F
  Vortragender: Holger Hartwig

  Resilienz-Bestrebungen vergessen oft die WAN-Infrastruktur, obwohl Verfügbarkeitszusagen der Provider bei größeren Störungen nicht ausreichen. Ein resilientes WAN auf SD-WAN-Basis hält Verbindungen auch bei Teilausfällen aufrecht. Wir zeigen, was A1 Digital dafür auf Anwendungs- und Transportschicht leistet.

- **Live-Vortrag: Netzwerke nach Bedarf – Was Sie brauchen. Nicht was wir haben.**

  Datum und Zeit: 28.10.2026 | 12:30-12:45
  Ort: Halle 9 Forum F
  Vortragender: Bernd Lohr

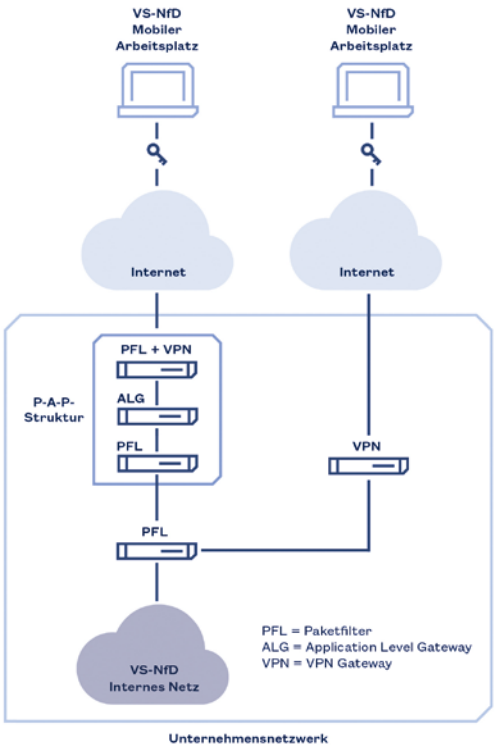
  Der klassische Ansatz aus einem SD-WAN-Hersteller und einem großen Carrier ist oft nicht mehr zeitgemäß. Anhand von Praxisbeispielen zeigen wir, wie carrierneutrales Sourcing und die Kombination verschiedener Provider Verfügbarkeit erhöhen und Time-to-Service verkürzen – für IT-Entscheider, die internationale Standorte resilienter vernetzen wollen.

VS-NfD sorgenfrei mobil bearbeiten

Moderne Arbeitswelten sind geprägt von dezentralen Teams, die mobil zusammenarbeiten. Immer häufiger begegnen Akteure dabei Dokumenten, die als „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD) eingestuft sind – und damit strengen regulatorischen Vorgaben unterliegen. Lassen sich mobile Arbeitsplätze rechtskonform, sicher und gleichzeitig praxistauglich konzipieren?

FÜR DEN ZUGRIFF AUF VS-NFD HAT DAS BUNDESAMT FÜR SICHERHEIT in der Informationstechnik (BSI) klare Vorgaben festgelegt: VS-NfD-eingestufte Dokumente dürfen ausschließlich in dafür freigegebenen Netzen verarbeitet und gespeichert werden.

Diese Anforderungen gilt es auch für mobile Arbeitsplätze umzusetzen. Dabei müssen die Lösungen einfach bedienbar sein, sonst droht die Gefahr unsicherer Workarounds. Eine lösungsorientierte und nutzerfreundliche Architektur ist daher unerlässlich, um Sicherheit und Produktivität zu vereinen.



Mobilität trifft auf Geheimschutz
Grundvoraussetzung sind mobile Endgeräte, die die strengen Vorgaben des BSI für einen sicheren Telearbeitsplatz erfüllen. Diese umfassen einen zugelassenen VPN-Client, idealerweise zukunftssicher mit quantensicherer Verschlüsselung ausgestattet, sowie eine sichere Multi-Faktor-Authentifizierung mittels Smartcard. Sollen VS-NfD auch lokal bearbeitet und gespeichert werden, ist zudem eine zugelassene Festplattenverschlüsselung Pflicht. Diese Voraussetzungen stellen sicher, dass die vertraulichen Daten in jeder Situation geschützt sind.

P-A-P-Struktur segmentiert Netze
Natürlich funktionieren die Endgeräte nicht im luftleeren Raum. Auf Unternehmensseite terminieren sie auf einem ebenfalls zugelassenes VPN-Gateway, das den Zugang zum internen VS-NfD-Netz kontrolliert.

Soll aus dieser sicheren VS-NfD-Enklave heraus ein Zugriff auf ein Netz mit geringerem Schutzniveau erfolgen – etwa auf das allgemeine Firmen-LAN oder das Internet – fordert das BSI eine sichere Netzsegmentierung per P-A-P-Struktur. Diese mehrschichtige Firewall-Architektur besteht aus einem äußeren Paketfilter, einem Application Layer Gateway (ALG) und einem inneren Paketfilter. Dieses „Sandwich“-Prinzip kontrolliert Protokolle, Inhalte sowie Verbindungsabläufe strikt. Das ALG fungiert dabei als Proxy auf Anwendungsebene, der direkte Zugriffe blockiert und das interne Netzwerk zuverlässig vor unerwünschter Exposition schützt.

Sichere mobile Arbeitsplätze für dezentrale Teams
Je nach Unternehmensgröße, Budget und Auslastung lässt sich die Architektur flexibel skalieren: Von einer Minimallösung, bei der das mobile Endgerät auf den äußeren Paketfilter terminiert (sofern dieser ein VPN-Gateway beinhaltet), bis hin zu leistungsfähigeren, zukunftssicheren Setups. Bei Letzteren sorgen dedizierte VPN-Gateways in einer demilitarisierten Zone (DMZ) in Kombination mit einem weiteren internen Paketfilter für eine bestmögliche Lastverteilung und entlasten die P-A-P-Struktur.

Vertrauen durch zugelassene Lösungen
Die sichere Handhabung digitaler Verschlusssachen im mobilen Arbeitsumfeld ist kein Hindernis für moderne Arbeitskonzepte, sondern eine Frage der richtigen Strategie und Technologie. Mit BSI-zugelassenen Lösungen „Made in Germany“, die Sicherheit und Nutzerfreundlichkeit vereinen, können Unternehmen in der geheimschutzbetreuten Industrie die Anforderungen von VS-NfD erfüllen – ohne auf Flexibilität verzichten zu müssen. •

genusecure Suite vereint den hochsicheren VPN-Client genuconnect mit einer Festplattenverschlüsselung und Smartcard-Middleware. Die Lösung erfüllt alle Anforderungen des BSI an einen VS-NfD-konformen Telearbeitsplatz.
(Bild: genua GmbH)

Managed Detection and Response boomt

MDR liefert SOC-Sicherheitsniveau für den Mittelstand

Auf der it-sa 2026 zeigt ESET, warum Managed Detection and Response bei Kunden so beliebt ist. Und wie sich MDR mit KI, Threat Intelligence und menschlicher Expertise zu einem vorausschauenden Sicherheitsansatz verbinden lässt.

MANAGED DETECTION AND RESPONSE ERFREUT SICH IM MITTELSTAND GRÖSSTER BELIEBTHEIT. Kein Wunder, denn es verbindet IT-Sicherheit rund um die Uhr auf dem Niveau eines Security Operation Centers (SOC) mit überschaubaren Kosten. Inzwischen greifen auch immer mehr Organisationen, die unter NIS2 oder KRITIS fallen, zu MDR. Das zeigt beispielsweise eine aktuelle Studie von ESET unter 165 Gesundheitseinrichtungen. Mehr als 85 Prozent der befragten Krankenhäuser wollen in den kommenden zwölf Monaten moderne Lösungen zur Angriffserkennung und -abwehr einführen oder ausbauen. Dazu zählen auch die Lösungen und Dienstleistungen von ESET „Made in EU", die sich im Alltag von Organisationen jeglicher Größe bewähren.

ESET MDR: Effizienter Schutz durch KI, rund um die Uhr
Mit ESET MDR erhalten Anwender einen vollständig automatisierten Einstieg in Managed Detection and Response. Der Service basiert auf einer KI-gestützten Analyse, die sicherheitsrelevante Ereignisse kontinuierlich erkennt, bewertet und priorisiert. Auffälligkeiten werden direkt in der zentralen ESET PROTECT-Konsole gemeldet, übersichtlich und in Echtzeit. Besonders für kleine und mittlere Unternehmen ist das eine ideale Lösung, um ein professionelles Sicherheitsniveau zu erreichen.

ESET MDR Ultimate: Mensch und Maschine im Duett
ESET MDR Ultimate baut auf den Funktionen von ESET MDR auf und ergänzt sie um eine tiefere Analyse durch erfahrene Sicherheitsexperten. Sobald ein Vorfall die automatisierte Bewertung übersteigt oder eine manuelle Einschätzung sinnvoll ist, übernehmen Analysten von ESET die Detailanalyse. Sie identifizieren Ursachen, geben fundierte Empfehlungen zur Reaktion und begleiten Partner bei Bedarf direkt beim Umgang mit kritischen Bedrohungen. Ideal für Unternehmen mit hohen Anforderungen an Compliance, Transparenz und Nachvollziehbarkeit.

ESET PROTECT MDR: Das Rundum-sorglos-Paket
Mit ESET PROTECT MDR stellt ESET ein Komplettpaket bereit, das Endpoint-Schutz, Extended Detection and Response sowie den MDR-Service in einer Lösung vereint. Die Steuerung erfolgt über die zentrale ESET PROTECT-Konsole, die Transparenz, Automatisierung und einfache Verwaltung ermöglicht. Kunden profitieren von regelmäßigen Reports, klar definierten Reaktionszeiten und direkter Analystenunterstützung bei kritischen Vorfällen.

ESET PROTECT MDR Ultimate: Maximum an Security
ESET PROTECT MDR Ultimate geht noch ein Stück weiter in puncto Sicherheit und Features. Es nutzt KI-gestützte Technologien, um Anomalien zu erkennen, proaktives Threat Hunting durchzuführen und automatisierte Reaktionen auf Sicherheitsvorfälle zu ermöglichen. Zusätzlich profitieren Kunden vom MDR Ultimate-Service, vom Premium-Support und erweiterten Funktionen. Zudem überwacht der ESET AI Advisor kontinuierlich das Netzwerk und schlägt präventive Maßnahmen vor.

„Made in EU": Vertrauen inklusive
Unternehmen, Behörden und öffentliche Auftraggeber legen zunehmend Wert auf Herkunft, Datenhaltung und Transparenz. Mit der Kampagne „Made in Europe" setzt ESET ein starkes Zeichen. Alle zentralen Technologien werden in Europa entwickelt, betrieben und kontrolliert. Es gibt keine Hintertüren, keinen politischen Zugriff und keinen Datenabfluss ins Ausland. Das ist für viele Kunden ein strategischer Faktor. Denn im Kontext von Gesetzen und branchenspezifischen Anforderungen wird digitale Souveränität zur Pflicht: für Hersteller und Anwender.

www.eset.de

In strategischer Zusammenarbeit

NATO OTAN | eset Cybersecurity Progress. Protected.

Raus aus der Kill-Switch-Falle

Digitale Souveränität ist längst mehr als eine Compliance-Frage – sie entscheidet über die Handlungsfähigkeit im Ernstfall. Stefan Schäfer von OVHcloud erklärt warum Kill-Switch-Szenarien und Anbieter-Lock-in zu echten Sicherheitsrisiken werden und wie Unternehmen sich mit einer schrittweisen Strategie absichern. /// von Heiner Sieger

DIGITALE SOUVERÄNITÄT WAR LANGE EIN THEMA FÜR STARK REGULIERTE BRANCHEN UND DEN ÖFFENTLICHEN SEKTOR. Das hat sich geändert. „Das Interesse kommt inzwischen aus der Breite des Marktes", beobachtet Stefan Schäfer, Marketing Director Central & Eastern Europe bei OVHcloud. Auslöser sind geopolitische Spannungen, Diskussionen um den US CLOUD Act – und ein Aspekt, der für CISOs besonders brisant ist: sogenannte „Kill-Switch"-Szenarien, bei denen Unternehmen im Ernstfall den Zugriff auf ihre eigene Infrastruktur verlieren könnten.

Souveränität als Sicherheitsfrage, nicht nur als Rechtsfrage

Viele Unternehmen reduzieren das Thema zunächst auf die Frage, ob sie vollständig der DSGVO unterliegen. Schäfer warnt davor, hier stehenzubleiben: Technologische Souveränität bedeute, Systeme ohne große Hürden migrieren oder wechseln zu können. „Wenn ein Anbieterwechsel mit erheblichen technischen oder finanziellen Barrieren verbunden ist, entsteht eine neue Abhängigkeit" – ein klassisches Lock-in-Risiko, das im Krisenfall zum handfesten Sicherheitsproblem wird. Hinzu kommt die operative Dimension: Wo werden Daten verarbeitet, wer betreibt die Systeme, wer hat im laufenden Betrieb Zugriff? Erst das Zusammenspiel aller drei Ebenen – rechtlich, technologisch, operativ – ergibt echte Kontrolle.

Der EU Data Act verschärft die Lage – zugunsten der Unternehmen

Mit der Abschaffung von Egress Fees und der Pflicht zu standardisierten Wechselprozessen senkt die Regulierung gezielt die technischen und finanziellen Hürden für einen Anbieterwechsel. Für Schäfer ein wichtiger Baustein, um die sogenannte Exit-Fähigkeit von Unternehmen zu stärken – also die Fähigkeit, im Notfall tatsächlich handlungsfähig zu bleiben, statt an einen einzigen Anbieter gekettet zu sein.

Kein „Big Bang", sondern ein kontrollierter Rückzug aus der Abhängigkeit

Ein vollständiger, sofortiger Cloud-Wechsel sei weder realistisch noch sinnvoll, so Schäfer. Stattdessen empfiehlt er einen strukturierten Einstieg über Disaster Recovery: Unternehmen schaffen zunächst eine unabhängige Ausweichumgebung bei einem alternativen Anbieter, bevor weitere Workloads migriert werden. Der Charme dieser Strategie liegt aus Security-Sicht auf der Hand: Sie liefert im gleichen Zug eine belastbare Wiederherstellungsoption für den Ernstfall – unabhängig davon, ob dieser durch einen Cyberangriff, einen Providerausfall oder politische Eingriffe ausgelöst wird.

Open Source als zusätzlicher Hebel gegen Abhängigkeit

Auch offene Technologien gewinnen laut Schäfer an Bedeutung, um Lock-in-Effekte zu reduzieren – ein Ansatz, den öffentliche Institutionen in Frankreich und Schleswig-Holstein bereits verfolgen. Für Unternehmen, die ihre Souveränitätsstrategie 2027 überarbeiten, ergibt sich daraus eine klare Reihenfolge: erst die eigene Architektur auf Abhängigkeiten prüfen, dann eine unabhängige Recovery-Umgebung aufbauen, und erst danach schrittweise weitere Systeme migrieren – ohne die Geschäftsfähigkeit auch nur für einen Moment zu gefährden. •

DER GESPRÄCHSPARTNER

Stefan Schäfer

Marketing Director Central & Eastern Europe bei OVHcloud und beschäftigt sich intensiv mit Cloud-Souveränität, Open Source und digitalen Transformationsstrategien im europäischen Kontext.

Sicherer Dokumentenaustausch:

Warum KRITIS-Organisationen und -Unternehmen und ihre Zulieferer handeln müssen

KRANKENHÄUSER, ENERGIEVERSORGER, FINANZINSTITUTE UND BEHÖRDEN stehen unter wachsendem regulatorischen Druck, ihre Kommunikationswege abzusichern. Mit dem KRITIS-Dachgesetz, der NIS2-Richtlinie und der BSI-KRITIS-Verordnung ist der Rahmen für einen rechtssicheren, nachvollziehbaren Austausch sensibler Dokumente gesteckt. Diese Pflichten betreffen längst nicht mehr nur KRITIS-Betreiber selbst: Auch Zulieferer und Dienstleister rücken in den Fokus, denn Schwachstellen in der Lieferkette gelten als häufiges Einfallstor für Angriffe auf kritische Infrastrukturen.

Vertraulichkeit und Manipulationsschutz als Priorität

Eine der größten Herausforderungen für IT-Prozesse besteht im rechtskonformen Austausch sensibler Dokumente und Daten im Hinblick auf DSGVO, NIS2, KRITIS und DORA. Bei der Digitalisierung der Kommunikation müssen Vertraulichkeit und Manipulationsschutz oberste Priorität haben. Klassische Kanäle wie unverschlüsselte E-Mail-Anhänge oder Cloud-Speicherdienste erfüllen diese Anforderungen häufig nicht: Ein gerichtsfester Nachweis über Versand und Empfang fehlt meist, Dokumente werden zudem über zahlreiche Knotenpunkte geroutet, was das Risiko einer Kompromittierung erhöht.

NGDX als Standard für rechtssicheren Austausch

Eine Antwort auf diese Herausforderungen bietet der von Ferrari electronic entwickelte Standard Next Generation Document Exchange (NGDX). Er basiert auf Vorgaben der Internationalen Fernmeldeunion ITU. NGDX ermöglicht einen rechtssicheren, direkten Dokumentenaustausch: Dokumente werden Ende-zu-Ende und mehrfach verschlüsselt als PDF mit Metadaten und Verschlagwortung direkt in das E-Mail-Postfach oder Informationssystem des Empfängers übertragen, ohne zentrale Cloud-Instanzen. Ein qualifizierter Sendebericht bestätigt den Transfer.

Version 9 der OfficeMaster Suite: aktuelle Antworten

Wie sich diese Anforderungen technisch umsetzen lassen, zeigt die im April 2026 vorgestellte Version 9 der OfficeMaster Suite von Ferrari electronic. Die Unified-Messaging-Lösung integriert NGDX neben Voicemail, SMS und nun auch RCS sowie Fax auf einer Plattform und unterstützt die aktuellen Microsoft- und HCL-Domino-Plattformen – wichtig für Stabilität und Ausfallsicherheit.

Neu ist die Funktion OfficeMaster Speech AI, die Sprachnachrichten automatisiert in Text umwandelt. Die Verarbeitung erfolgt konsequent im lokalen Netzwerk, ohne externe Cloud-Dienste. Das stärkt die Digitale Souveränität der Anwender und ist wichtig für KRITIS- und NIS2-pflichtige Organisationen, da sensible Daten innerhalb der eigenen IT-Grenzen bleiben. Mit RCS lassen sich zudem verschlüsselte PDFs direkt auf Android- und iOS-Smartphones senden, dort ausfüllen und zurücksenden, etwa für Formulare im Gesundheitswesen oder in der Verwaltung. Ergänzt wird die Suite um den automatisierten Versand von XRechnungen an das PEPPOL-Netzwerk für den gesetzeskonformen Rechnungsversand an Behörden und B2B-Unternehmen.

Fazit

Für KRITIS-Betreiber und ihre Zulieferer wird der sichere, nachvollziehbare Dokumentenaustausch zur Pflichtaufgabe. Lösungen wie die OfficeMaster Suite 9 mit NGDX zeigen, wie sich regulatorische Vorgaben und praktikable Kommunikation verbinden lassen. •

Ferrari electronic AG

https://www.ferrari-electronic.de/
E-Mail: info@ferrari-electronic.de

Telefon: +49 3328 455 90
Ruhlsdorfer Str. 138, 14513 Teltow

Ferrari electronic

So stoppen Unternehmen Cyberangriffe in Minuten statt Tagen

Sekundenschnell zuschlagen, tagelang unentdeckt bleiben: So arbeiten moderne Cyberangriffe. Ein Managed SOC verkürzt die Reaktionszeit – doch wann lohnt es sich und worauf kommt es bei der Partnerwahl an? /// von Stefan Tiefel

CYBERANGRIFFE LAUFEN RUND UM DIE UHR, WERDEN GEZIELTER UND BLEIBEN OFT WOCHENLANG UNBEMERKT: Laut dem Report Mandiant M-Trends 2026 stieg die globale mediane Verweildauer von Angreifern im Netz 2025 auf 14 Tage. Im Jahr zuvor betrug sie noch elf Tage. Zugleich schrumpft die Reaktionszeit der Verteidiger. Wie meistern Unternehmen den Schritt von der reaktiven zur proaktiven Abwehr mithilfe eines Security Operations Center (SOC)?

Moderne Angriffe sind arbeitsteilig und schnell. Zwischen erstem Zugriff und der Übergabe an eine zweite Angreifergruppe lagen 2025 im Median nur noch 22 Sekunden, gegenüber mehr als acht Stunden im Jahr 2022. Wer wartet, bis ein Angriff sichtbare Spuren hinterlässt, reagiert auf bereits entstandenen Schaden; ohne kontinuierliche Überwachung bleibt die entscheidende Frühphase unsichtbar.

Warum bleiben Angriffe lange unentdeckt?
Die entscheidenden Hinweise liegen verstreut: in Logs, im Netzwerkverkehr, in Endpunktsignalen und in Cloud-Umgebungen. Einzeln betrachtet ergeben sie kein Bild, wie Dutzende Überwachungskameras, deren Monitore niemand auswertet. Erst wenn diese Signale in Echtzeit zusammengeführt und korreliert werden, treten Anomalien hervor, bevor sie sich zu einem Vorfall summieren.

Was leistet ein Security Operations Center?
Ein Security Operations Center (SOC) ist kein Produkt, sondern das Zusammenspiel aus Technologie, Prozessen und spezialisierten Teams. Es führt Sicherheitssignale zusammen, bewertet sie und greift bei Bedarf ein. Das Ziel: eine Bedrohung in Minuten erkennen und eindämmen, wo früher Tage vergingen.

Warum überfordert der Eigenbetrieb die meisten Unternehmen?
Ein eigenes SOC verlangt spezialisiertes Personal, einen Schichtbetrieb rund um die Uhr und hohe laufende Kosten. Qualifizierte Fachkräfte sind rar. In Deutschland berichteten laut der 2025 Cybersecurity Workforce Study des Verbands ISC2 92 Prozent der befragten Unternehmen von mindestens einem Vorfall infolge fehlender Cybersicherheitskompetenz im eigenen Haus. Ein Inhouse-Betrieb ist für viele damit personell und wirtschaftlich kaum darstellbar.

WAS IST EIN SOC?

Ein Security Operations Center (SOC) ist eine zentrale Stelle, die sicherheitsrelevante Daten aus IT Systemen fortlaufend sammelt, korreliert und bewertet. Spezialisierte Teams erkennen verdächtige Aktivitäten, priorisieren sie und leiten Gegenmaßnahmen ein. Betrieben wird ein SOC rund um die Uhr, im eigenen Haus oder als Managed Service über einen externen Dienstleister.

Wann ist ein Managed SOC die bessere Wahl?
Über einen Managed Service erhalten Unternehmen Zugang zu erfahrenen Analysten, eingespielten Prozessen und leistungsfähigen Erkennungswerkzeugen, ohne selbst eine vollständige Sicherheitseinheit aufzubauen. So betreibt etwa Noris Network ein eigenes SOC im Dauerbetrieb und stellt forensische Kompetenz sowie aktive Incident Response bereit.

Woran erkennt man einen verlässlichen Partner für ein Managed SOC?
Entscheidend sind nachweisbare Standards und klar geregelte Abläufe. Darauf sollten Verantwortliche achten:

- Zertifizierungen wie ISO 27001 und BSI C5
- Betrieb in deutschen Rechenzentren unter deutschem Recht
- Festgelegte Wege für Eskalation und Meldung
- Nachgewiesene Erfahrung in Threat Hunting und Incident Response

Gerade in regulierten Branchen bleibt die Datensouveränität ein zentrales Kriterium.

Fazit Managed SOC:
Der Weg zur proaktiven Abwehr
Der Übergang vom reaktiven Sicherheitsmanagement gelingt schrittweise: kontinuierliche Überwachung etablieren, Sichtbarkeit über alle Umgebungen herstellen und Erkennung sowie Reaktion in geübte Prozesse überführen. Proaktive Abwehr ist kein einmaliges Projekt, sondern ein dauerhafter Kreislauf aus Überwachung, Erkennung und Reaktion. Wo eigene Kapazitäten fehlen, kann ein Managed SOC die Lücke schließen. •

> „ Proaktive Abwehr ist kein einmaliges Projekt, sondern ein dauerhafter Kreislauf aus Überwachung, Erkennung und Reaktion. **Wo eigene Kapazitäten fehlen, kann ein Managed SOC die Lücke schließen.** *Stefan Tiefel*

DER AUTOR
Stefan Tiefel
ist Senior Market Development Manager bei Noris Network.
Bild: Noris Network

Mehr als Firewalls: Was Rechenzentren resilient macht

Ein modernes Rechenzentrum muss mehr leisten, als leistungsfähige IT-Systeme sicher zu betreiben. Entscheidend ist die Umgebung, in der diese Systeme arbeiten – von der physischen Absicherung bis zur Ausfallsicherheit der Infrastruktur. /// von Leon Weise

VIELE UNTERNEHMEN INVESTIEREN IN FIREWALLS UND VERSCHLÜSSELUNG und lassen dabei nicht nur im übertragenen Sinne die Kellertür offen: der Serverraum ohne geregelten Zutritt, nur eine Stromleitung, kein Plan B für den Ausfall des Netzbetreibers. Rechenzentren können sich solche blinden Flecken nicht leisten. Die dringend benötigte Verfügbarkeit hat dabei – grob unterteilt – zwei Feinde, den Angreifer und den Ausfall. Wirksame Maßnahmen und resiliente Strategien können daher in der Praxis auch nur greifen, wenn verschiedene Ebenen in einer ganzheitlichen Betrachtung zusammenlaufen.

Physische Absicherung in drei Stufen

Wenig überraschend beginnt ein wirksamer physischer Schutz am Perimeter nicht erst an der Serverraumtür. Zäune, kontrollierter Werksverkehr und Videoüberwachung verhindern, dass Unbefugte überhaupt erst auf das Gelände gelangen. Im Inneren sollte ein abgestuftes Zonenkonzept zum Einsatz kommen, bei dem Biometrie oder RFID-gestützte Personenschleusen sicherstellen, dass sich nur autorisiertes Personal in vulnerablen Bereich aufhält und jeder Ein- und Ausgang protokolliert wird. Auch hier gilt allerdings, dass der größte Risikofaktor der Mensch bleibt, etwa wenn beispielsweise eine Tür für den nachfolgenden Kollegen offengehalten wird. Regelmäßige Schulungen zur Zutrittsdisziplin und Aufklärung über Social Engineering gehören deshalb ebenso zum Konzept wie Schleusen und Kameras.

Ausfällen vorbeugen durch Redundanz auf allen Ebenen

Der zweite Gegner einer problemlosen Verfügbarkeit der Infrastruktur ist der technische Ausfall. Die notwendigen Gegenmaßnahmen folgen dabei derselben Logik einer gestaffelten Absicherung. Eine einzelne Stromleitung ist ebenso ein Risiko wie eine ungesicherte Serverraumtür. USV-Systeme, redundante Stromnetze und eine Notstromversorgung können hier Unterbrechungen abfangen, bevor sie zu einem echten Problem werden. Selbstverständlich gilt dies auch für die Internetanbindung. Erst mehrere Leitungswege verschiedener Carriers bringen hier die Sicherheit. Apropos Sicherheit: Ohne eine zuverlässige, redundant ausgelegte Kühlung drohen Systeme unter Last auszufallen, auch ganz ohne böswillige Angreifer. Ergänzt wird der Schutz vor Schadensereignissen wie Brand oder Wassereintritt, etwa durch Frühwarnsysteme und Löschkonzepte.

Die Konsequenz: Regulatorik erfüllen ohne Eigenbetrieb

Viele der genannten Maßnahmen sind regulatorisch relevant. Für KRITIS-Betreiber gelten besondere Anforderungen an die Verfügbarkeit und Sicherheit kritischer Dienste. Mit NIS-2 steigen die Anforderungen für weitere Branchen. Auch deshalb ist ein ganzheitlicher Ansatz notwendig, der technische und physische Aspekte berücksichtigt.

Eine solche Betriebsumgebung aufzubauen und dauerhaft ausfallsicher zu betreiben ist mit erheblichem Aufwand und Kosten verbunden. Eine Alternative zum Eigenbetrieb ist daher das Konzept der Colocation. Unternehmen verlagern ihre IT-Systeme, auch teilweise, in ein nach Standards und Vorgaben gesichertes Rechenzentrum und können so eine entsprechend ausgelegte Infrastruktur nutzen.•

DER AUTOR
Leon Weise
ist Senior Development Director bei der nexspace data centers GmbH, einem Betreiber lokaler Rechenzentren im deutschsprachigen Raum.
Bild: nexspace data centers

Angreifer zielen längst auf Produktion und Logistik

WENN EINE PRODUKTIONSANLAGE AUFGRUND EINER KOMPROMITTIERTEN STEUERUNG STILLSTEHT, HILFT KEINE FIREWALL IN DER ZENTRALE. Angriffe auf die sogenannte Operational Technology (OT) treffen Unternehmen mitten im laufenden Betrieb. Maschinen stehen still, Lieferungen verzögern sich.

Cybersicherheit lässt sich schon lange nicht mehr als isolierte IT-Disziplin behandeln. Geopolitische Spannungen und die zunehmende Vernetzung der Produktion verlagern die Verantwortung dafür in die Geschäftsführung.

In den vergangenen Jahren haben klassische IT-Umgebungen erheblich an Reife gewonnen und etablierte Standards und Verantwortlichkeiten entwickelt. Die Steuerungs- und Produktionssysteme, die Fabriken und Energieversorger am Laufen halten, sind dieser Entwicklung jedoch oft nicht gefolgt. Zwar sind sie heute stärker vernetzt als früher, oft über Fernzugriffe und Cloud-Anbindungen, doch hat ihr Schutzniveau mit dieser Vernetzung nicht immer Schritt gehalten. Genau diese Lücke macht OT-Systeme für Angreifer zu einem lohnenden Ziel.

Damit verschiebt sich der Fokus der Sicherheitsarbeit. Prävention allein reicht nicht mehr aus. Künftig wird es entscheidend sein, wie schnell ein Unternehmen auf einen Vorfall reagiert und wie lange es den Betrieb trotz eines Angriffs aufrechterhalten kann, in der Fabrikhalle ebenso wie im Rechenzentrum. Improvisieren lässt sich das im Ernstfall nicht.

Resilienz bezieht sich heutzutage nicht mehr ausschließlich auf den Schutz der IT. Der Blick muss sich auf sämtliche geschäftskritischen Betriebsprozesse ausweiten. Dazu zählen klare Verantwortlichkeiten und Incident-Response-Pläne, die im Vorfeld festlegen, wer im Krisenfall Entscheidungen trifft und Maßnahmen ergreift. Ob Meldewege und Kommunikationspläne im echten Vorfall tragen, zeigt sich allerdings erst dann, wenn ein Unternehmen den Ernstfall regelmäßig durchspielt, bevor er eintritt.

Vorbereitung und Transparenz über die eigenen Systeme entstehen lange vor der Krise. Ein Unternehmen, das nicht weiß, welche Steuerungen im eigenen Werk aus dem Netz erreichbar sind, kann im Vorfall nicht entscheiden, was abgeschaltet werden muss und was weiterlaufen darf. Diese Bestandsaufnahme kostet Wochen und bindet Personal. Ohne sie bleibt jeder Notfallplan eine Annahme.

Getronics begleitet Unternehmen auf diesem Weg, von der ersten Risikoanalyse bis zur Umsetzung konkreter Schutz- und Resilienzmaßnahmen für IT und OT. Für eine erste Einschätzung der eigenen Widerstandsfähigkeit steht Getronics als Ansprechpartner zur Verfügung. •

Weitere Informationen finden Sie auf der Website von Getronics.

Joeri Barbier, Getronics

getronics

Identitäten als Compliance-Pflicht

Mit dem European Technological Sovereignty Package, dem EU AI Act und NIS2 wird digitale Souveränität von der politischen Forderung zur prüfbaren Managementaufgabe. Warum Unternehmen ihre Zugriffsrechte jetzt lückenlos dokumentieren müssen – und was das für die IT-Sicherheit bedeutet. /// von Elmar Eperiesi-Beck

MIT DEM EUROPEAN TECHNOLOGICAL SOVEREIGNTY PACKAGE und weiteren Regulierungen, darunter dem EU AI Act, schafft die EU einen unionsweit einheitlichen Bewertungsrahmen für IT-Sicherheit. Unternehmen müssen im Rahmen gestiegener Transparenzpflichten nachweisen, dass sie die Kontrolle über ihre Zugriffsrechte haben – besonders in sensiblen Bereichen wie HR, wo KI-Lösungen oft als Hochrisiko eingestuft werden. Als Anbieter für Identity- und Access-Management-Plattformen sehen wir bei Bare.ID akuten Handlungsbedarf: Unternehmen müssen jetzt ihre digitalen Identitäten absichern und gleichzeitig stufenweise strengere Compliance-Anforderungen erfüllen.

Regulatorischer Druck als Sicherheitstreiber

Die EU macht digitale Souveränität von einer politischen Forderung zur prüfbaren Managementaufgabe. Unternehmen müssen klare Inventare, Stufenmodelle und Fahrpläne vorlegen. Besonders kritisch: die Abhängigkeit von nicht-europäischen Tech-Konzernen bei der Verwaltung von Identitäten. Wer in sensiblen Bereichen nicht auf souveräne IAM-Lösungen setzt, riskiert nicht nur Compliance-Verstöße, sondern öffnet auch unkontrollierte Angriffsflächen. Wer früh auf sichere Identity- und Access-Management-Architekturen setzt, stärkt seine digitale Resilienz gegen genau jene Angriffe, die über kompromittierte Zugänge laufen.

Vier sicherheitsrelevante Handlungsfelder

Um Vorgaben aus EU AI Act, NIS2, DORA und dem Cloud and AI Development Act zu erfüllen, empfiehlt sich ein strukturiertes Vorgehen in vier Schritten:

1. **Bestandsaufnahme und Risikoklassifizierung:** Alle IAM-Lösungen, Cloud-Dienste, KI-Tools und Schnittstellen zu Drittanbietern müssen erfasst und nach Risikoklassen eingeteilt werden, insbesondere in Hochrisiko-Bereichen wie HR oder Finanzwesen. Datenflüsse sind zu analysieren, um zu erkennen, wo Identitäten und Zugriffsrechte gespeichert und weitergegeben werden.
2. **Abhängigkeiten und Rechtsräume prüfen:** Bei der IAM-Anbieterwahl zählen neben Funktionalität auch Datenstandorte, Betreiberstrukturen und Rechtsräume. Europäische Anbieter und offene Architekturen reduzieren rechtliche und operative Abhängigkeiten. Zertifizierungen wie ISO 27001, BSI C5 und BSI-Grundschutz liefern dabei überprüfbare Sicherheitsnachweise.
3. **Dokumentation und Transparenz:** Identitätsprozesse, Zugriffsrechte, Authentifizierungsmethoden und Sicherheitsmaßnahmen müssen lückenlos dokumentiert werden. Audit-Trails – protokollierte Logs über alle Zugriffe und Änderungen im IAM-System – sind essenziell, um Compliance-Prüfungen und im Ernstfall auch forensische Analysen nach einem Sicherheitsvorfall standzuhalten.
4. **Exit-Strategie und Anbieterunabhängigkeit:** Lock-in-Effekte lassen sich durch offene Standards wie SAML, OIDC oder SCIM sowie modulare Lösungen vermeiden. Klare vertragliche Regelungen zu Kündigungsfristen, Datenrückgabe und Migration sichern zudem, dass Identitätsdaten im Bedarfsfall verlustfrei portiert werden können – eine Voraussetzung, um auch bei einem Anbieterwechsel keine Sicherheitslücke entstehen zu lassen.

Wer diese vier Handlungsfelder jetzt angeht, sichert nicht nur die Einhaltung kommender Regularien, sondern schließt zugleich eine der häufigsten Angriffsflächen: unkontrollierte, undokumentierte Zugriffsrechte. •

DER AUTOR
Elmar Eperiesi-Beck ist CEO von Bare.ID.

Warum die Fabrik ein neues Identitätsmodell braucht

IN DEUTSCHEN FABRIKHALLEN BESTIMMT SCHON LANGE NICHT MEHR ALLEIN DIE LOSGRÖSSE DEN TAKT DER PRODUKTION. Während sich Arbeiter mehrmals pro Schicht an gemeinsam genutzten Terminals anmelden, erhalten externe Servicetechniker oft nur für ein einzelnes Wartungsfenster Zugriff auf die Anlagensteuerung. Zudem erledigen KI-Agenten in der Beschaffung oder Qualitätssicherung zunehmend eigenständig Teilaufgaben, ohne dass ein Mensch jeden Schritt freigibt. Die klare Grenze zwischen Mitarbeitern und Maschinen löst sich auf.

Klassische Identitäts- und Zugriffssysteme wurden jedoch für den klassischen Büroangestellten entwickelt und gehen daher von festen Rollen und stabilen Beschäftigungsverhältnissen aus. Der Fabrikbetrieb tickt anders. Wer an einem Kioskterminal in der Frühschicht Zugriff hat, ist an einer anderen Anlage womöglich nicht berechtigt. Ein Techniker eines Zulieferers darf eine Maschine oft nur innerhalb eines eng definierten Zeitfensters warten. Selbst ein Planungsagent, der eine Bestellung vorschlägt, sollte diese nicht ohne menschliche Freigabe auslösen dürfen.

Wie konkret sich dieses Problem stellt, zeigt sich an gemeinsam genutzten Geräten. Nach Angaben von **Ping Identity** müssen einzelne Beschäftigte an der Linie an manchen Tagen mehr als siebzigmal ihre Identität an einem Gerät nachweisen, etwa an Maschinen und Zeiterfassungsterminals. An anderen Arbeitsplätzen wiederum muss eine einzelne Person auf bis zu siebzig verschiedene Geräte zugreifen. Das kostet Zeit an der Linie und begünstigt Abkürzungen wie geteilte Zugangsdaten oder das gegenseitige Einstempeln von Kollegen.

Ping Identity begegnet diesem Problem mit einem Modell, das das Unternehmen „Verified Trust" nennt: Jeder Mitarbeiter an der Front kann sich an jedem gemeinsam genutzten Gerät über die Frontkamera in weniger als einer Sekunde authentifizieren. Die Lösung benötigt kein externes Gerät oder Authentifizierungstool und verzichtet auf klassische Methoden der Unternehmens-IT wie Passwörter oder Ausweiskarten. Stattdessen nutzt sie eine einzigartige, datenschutzfreundliche Form der biometrischen Authentifizierung, um Mitarbeitern an der Front sofortigen, verifizierten Zugriff auf jedes gemeinsam genutzte Gerät zu ermöglichen.

Der Effekt reicht über die IT-Sicherheit hinaus. Schnellere biometrische Anmeldung an Terminals senkt Reibungsverluste in der Schicht, und weil Handlungen auch an geteilten Geräten einzelnen Personen zugeordnet bleiben, lassen sich Audits und Haftungsfragen leichter beantworten. Ein gemeinsames Regelwerk für Beschäftigte, Zulieferer, Franchisenehmer und externe Dienstleister verhindert außerdem parallele Zugriffswege, die niemand mehr überblickt. Ohne diese Grundlage bleibt jeder weitere Schritt in der Fertigung ein Risiko. •

Henning Dittmer, Ping Identity

Mehr zu Verified Trust für die Fertigungsindustrie unter pingidentity.com

Digitale Business Compliance: Warum sicherer Dokumentenaustausch zur Chefsache wird

Digitale Business Compliance verbindet klassisches Compliance-Management mit Datenschutz, Cybersicherheit, digitalen Nachweisen und automatisierten Kontrollen bis hin zur Bewertung von KI- und Cloud-Diensten. Der digitale Austausch von Dokumenten unterstützt die Standardisierung von Geschäftsvorgängen, macht sie schneller und leichter prüfbar. Voraussetzung: Datenschutz und Datensicherheit bleiben zu jedem Zeitpunkt gewahrt. /// von Stephan Leschke

SICHERE GESCHÄFTSKOMMUNIKATION ENTSTEHT NICHT DURCH EINZELNE FUNKTIONEN, sondern durch das Zusammenspiel integrierter Prozesse. Mit NIS2, DORA, dem KRITIS-Dachgesetz und der KRITIS-Verordnung des BSI wird die rechtskonforme Digitalisierung der Kommunikation zu einer der größten Herausforderungen für IT-Prozesse – und damit zur strategischen Frage, die auf Geschäftsführungsebene entschieden werden muss.

Nachvollziehbarkeit als Grundprinzip

Wenn sich Dokumente, Versionen, Empfänger, Zeitpunkte und Freigaben automatisch protokollieren lassen, unterstützt das eine revisionssichere Dokumentation und interne Kontrollen. Ein Ansatz, der besonders für regulierte Branchen interessant ist, ist der in Deutschland entwickelte Standard Next Generation Document Exchange (NGDX), der auf Normen der Internationalen Fernmeldeunion ITU basiert.

NGDX verbindet die Rechtssicherheit des klassischen Telefaxverfahrens mit den Möglichkeiten moderner digitaler Kommunikation: Dokumente werden Ende-zu-Ende und mehrfach verschlüsselt als PDF mit Metadaten und Verschlagwortung direkt in das E-Mail-Postfach oder Informationssystem des Empfängers übertragen, ohne dass zentrale Instanzen wie Cloud-Speicher zwischengeschaltet werden.

Integrität und Beweiskraft

Jedes Dokument erhält zusätzlich einen eindeutigen Hash-Wert, mit dem sich Manipulationen sofort erkennen lassen. Nach erfolgreicher Übermittlung bestätigt ein qualifizierter Sendebericht den Transfer – ein Nachweis, der im Streitfall gerichtsfest ist und die klassische Funktion des Fax-Sendeberichts in die digitale Welt überträgt. Das ist auch juristisch relevant: Nach der eIDAS-Verordnung darf einem elektronischen Dokument seine Rechtswirkung nicht allein wegen seiner elektronischen Form abgesprochen werden, und eine qualifizierte elektronische Signatur ist der handschriftlichen Unterschrift grundsätzlich gleichgestellt.

Vertraulichkeit und lokale KI-Verarbeitung

Integrierte Services, die nur über eine Cloud-Anbindung laufen, wie KI-gestützte Datenverarbeitung, können ein Hindernis für die Beschaffung in regulierten Branchen sein. Ein Zuschlag wird oft nur noch erteilt, wenn eindeutig geklärt ist, dass die Server im Rechtsraum der EU betrieben werden, wo auch der Betreiber seinen Sitz haben muss. Die Alternative ist, die benötigten Services aus der eigenen IT-Infrastruktur bereitstellen. Moderne Unified-Messaging-Plattformen setzen deshalb auf lokale Verarbeitung: Funktionen, die Sprachnachrichten automatisiert in Text umwandeln, laufen im lokalen Netzwerk, ohne Anbindung an externe Cloud-Dienste. Zugleich lassen sich die so gewonnenen Textdaten deutlich einfacher speichern und durchsuchen als Audiodateien – ein Vorteil, der auch für die Compliance in regulierten Branchen wie dem Finanzwesen an Bedeutung gewinnt. Die Integrationsmöglichkeit in bestehende Archivierungssysteme vereinfacht die Compliance zusätzlich und stellt damit deren Umsetzung im Arbeitsalltag sicher. Diese Datenhoheit ist die Grundlage für digitale Souveränität, die in der öffentlichen Verwaltung und in KRITIS-Sektoren längst vom politischen Anspruch zum technischen Auswahlkriterium geworden ist.

Prozesskontrolle über alle Kanäle

Auch neue Kommunikationskanäle müssen sich in be-

> „ Wichtig ist, digitale Compliance nicht ausschließlich als IT-Projekt zu behandeln: Fachbereiche, Datenschutz, Informationssicherheit, Recht, Revision und gegebenenfalls der Betriebsrat müssen **gemeinsam eingebunden** werden.
>
> *Stephan Leschke*

stehende Prozesskontrollen einfügen, statt sie zu unterlaufen. Mit Rich Communication Services (RCS) als Nachfolger der klassischen SMS lassen sich verschlüsselte PDFs direkt auf aktuelle Android- und iOS-Smartphones senden, dort ausfüllen und sicher zurücksenden – eine Option, die im Gesundheitswesen, bei Behörden, Banken oder Versicherungen die Brücke zur B2C-Kommunikation schlägt.

Ähnlich verhält es sich beim automatisierten Versand von X-Rechnungen aus ERP-Systemen über das PEPPOL-Netzwerk. Dieser stellt beim digitalen Rechnungsversand an Behörden und B2B-Unternehmen sicher, dass Pflichtprüfungen und Freigaben im Rechnungsprozess gesetzeskonform und weitgehend automatisiert ablaufen.

Aufbewahrung nach GoBD

Für steuerlich relevante elektronische Unterlagen verlangen die GoBD unter anderem Nachvollziehbarkeit, Vollständigkeit, Ordnung und Unveränderbarkeit; die Dokumente müssen während der Aufbewahrungsfrist verfügbar, lesbar und maschinell auswertbar bleiben. Wenn Dokumente im PDF-Format rechtskonform übertragen werden und enthaltene Formatierungen und Auflösungen erhalten bleiben, lassen sie sich ohne Medienbruch in Dokumentenmanagement- und Archivsysteme einbinden und automatisiert weiterverarbeiten.

Fazit: Compliance durch Konvergenz

Die einzelnen Bausteine entfalten ihren Compliance-Wert erst im Zusammenspiel. Genau das ist der Kern von Unified Messaging: Statt Voicemail, SMS, RCS und digitalen Dokumentenaustausch als getrennte Insellösungen zu betreiben, bündelt eine solche Plattform alle Kanäle auf einer gemeinsamen, kontrollierbaren Infrastruktur.

Wichtig ist dabei, digitale Compliance nicht ausschließlich als IT-Projekt zu behandeln: Fachbereiche, Datenschutz, Informationssicherheit, Recht, Revision und gegebenenfalls der Betriebsrat müssen gemeinsam eingebunden werden. Wer Unified Messaging so versteht und einsetzt, dass alle Kanäle rechtssicher und nachvollziehbar zusammenlaufen, leistet damit einen wesentlichen Beitrag zur digitalen Business Compliance – und macht aus einer regulatorischen Pflicht einen belastbaren Wettbewerbsvorteil. •

DER AUTOR
Stephan Leschke
ist CEO von Ferrari electronic.

„2030 ist keine Zukunft mehr“

DigiCert-Manager Reto Scagnetti* erklärt, warum der Mittelstand beim Kryptografie-Umstieg hinterherhinkt – und was jetzt konkret zu tun ist.

/// von Heiner Sieger

Der Countdown läuft

Das Bundesamt für Sicherheit in der Informationstechnik hat im Februar 2026 erstmals feste Fristen genannt: Klassische Schlüsseleinigungsverfahren gelten nur noch bis Ende 2031, bei hohem Schutzbedarf endet die Frist bereits 2030. Parallel verpflichtet die NIS2-Richtlinie Unternehmen ab 50 Mitarbeitenden zu einem Kryptografie-Risikomanagement. Der Grund für die Eile heißt „Harvest Now, Decrypt Later“: Kriminelle und Geheimdienste sammeln schon heute verschlüsselte Daten – in der Erwartung, sie später mit Quantencomputern zu entschlüsseln. Für Unternehmen mit langlebigen Werten wie Konstruktionsplänen oder Gesundheitsdaten ist das kein fernes Risiko, sondern ein Zeitfenster, das sich schließt.

Wir sprachen mit Reto Scagnetti, Area Vice President Southern Europe & Switzerland beim digital Trust-Anbieter DigiCert, am Rande der Veranstaltung „Innovation meets Digital Trust“ in Zürich.

DER GESPRÄCHSPARTNER

Reto Scagnetti

ist Area Vice President Southern Europe & Switzerland bei DigiCert und verantwortet Vertrauensdienste für Zertifikate, PKI und IoT-Sicherheit.

> „Als Mittelständler brauchst du fast zwingend einen Dienstleister, der dir Discovery, Policy-Management und Automatisierung abnimmt – im Paket mit einem **Certificate-Lifecycle-Management-Tool**.“ *Reto Scagnetti*

Herr Scagnetti, ist das Thema Post-Quanten-Kryptografie im Mittelstand angekommen – oder halten viele das noch für ein Thema für Konzerne und Banken?

Reto Scagnetti | Erstens sind viele dieser Regelungen EU-Recht und in der Schweiz nicht direkt anwendbar. Zweitens sehen wir selbst bei multinationalen Firmen und im Bankenumfeld: Man ist sich bewusst, dass es Regeln gibt, aber die Umsetzung ist noch nicht dort, wo sie sein sollte. Beim Mittelstand sehe ich das noch weniger. Das ist ein Knowledge-Thema, es fehlt die Awareness auf Geschäftsleitungsebene. Da sind viele Unternehmen noch weit hintendran.

Wie weit reicht die Verantwortung eines Mittelständlers – auch für seine Software- und Hardwarelieferanten?

RS | Es gibt klare Regelungen. Software musst du signieren, du brauchst eine vollständige Software Bill of Materials – mit jeder ausgelieferten Software musst du offenlegen, welche Bibliotheken du verwendest, kryptografisch gesichert und signiert. Wie konsequent das in der Industrie tatsächlich umgesetzt wird, kann ich nicht sagen. Meine persönliche Wahrnehmung ist: noch nicht überall.

Ein Konzern kann ein eigenes PQC-Team aufbauen. Ein Mittelständler hat oft nur zwei, drei Leute für die gesamte IT. Was ist das realistische Minimalprogramm?

RS | Unabhängig von der Firmengröße gibt es vier Phasen, die jedes Unternehmen durchlaufen muss. Erstens: Inventar. Du musst wissen, welches kryptografische Material du überhaupt einsetzt, zentral dokumentiert in einem Repository. Zweitens: Governance. Klare Policies, wie Zertifikate ausgestellt werden – sonst entsteht Schatten-IT. Drittens: Automatisierung. Solange du alles manuell machst, bekommst du Probleme, sobald sich Algorithmen ändern.

PRAXIS-CHECK

VIER FRAGEN AN DIE EIGENE IT

1. Wissen wir, welche Zertifikate und Algorithmen bei uns im Einsatz sind – zentral dokumentiert?
2. Gibt es klare Policies für die Zertifikatsausstellung, oder wächst irgendwo Schatten-IT?
3. Können wir kryptografisches Material automatisiert austauschen – oder nur manuell?
4. Kennen wir die Brownfield-Anlagen in unserer Produktion, die sich nicht patchen lassen?

KEY TAKEAWAYS

- BSI-Fristen: klassische Verschlüsselung nur noch bis 2030/2031 zulässig.
- NIS2 verpflichtet bereits Unternehmen ab 50 Mitarbeitenden.
- Vier-Stufen-Modell: Inventar, Governance, Automatisierung, vollständige Krypto-Agilität.
- Mittelständler sollten Discovery und Automatisierung an spezialisierte Dienstleister delegieren.
- Brownfield-Anlagen brauchen Einzelfalllösungen oder Netztrennung.
- Fehlender Sicherheitsnachweis kann Versicherungsschutz und Marktzugang kosten.

Und PQC wird kein einmaliger Wechsel sein – in zwei, drei Jahren kommt der nächste. Deshalb brauchst du einen Zustand, den wir „Krypto-Agiliät" nennen: Du kannst deine Zertifikate jederzeit automatisiert austauschen. Viertens: vollständige Krypto-Agilität, die auch die gesamte Lieferkette einschließt.

Was davon kann ein Mittelständler realistisch selbst leisten – und was sollte er delegieren?
RS | Als Mittelständler brauchst du fast zwingend einen Dienstleister, der dir Discovery, Policy-Management und Automatisierung abnimmt – im Paket mit einem Certificate-Lifecycle-Management-Tool. Große Firmen machen vieles noch selbst, haben teils eigene Abteilungen. Aber auch dort setzt sich zunehmend die Erkenntnis durch, dass sich die Lage zu schnell ändert, um alles inhouse zu stemmen.

Heißt das, ein Anbieter wie DigiCert übernimmt dem Mittelstand die Arbeit komplett?
RS | Nein, nicht komplett. Es gibt zwar Dinge, von denen der Kunde nichts mitbekommt, die einfach in der Software im Hintergrund laufen. Aber er muss weiterhin bei Implementierung und Umsetzung mitwirken. Wo wir helfen können, sind Best Practices – etwa bei Policy-Strukturen, die er nicht selbst erfinden muss.

Krypto-Agilität heißt, Algorithmen austauschen zu können, ohne die Anwendung neu zu bauen. Aber viele Mittelständler haben Maschinenparks mit zwanzig Jahren Lebensdauer und fest verbauter Firmware. Was macht ein Maschinenbauer mit Systemen, die sich nicht umstellen lassen?
RS | Wir unterscheiden zwischen Greenfield und Brownfield. Der Greenfield-Ansatz ist der einfachere Fall. Brownfield ist definitiv schwierig. Wir haben dafür ein separates Modul namens Device Trust für IoT-Umgebungen – aber es ist ein langer Prozess, weil die Geräte erst fähig gemacht werden müssen, überhaupt mit kryptografischem Material umzugehen. Mit Low-Level-Code kommt man teilweise weit, das ist aber Einzelfallarbeit. Am Ende gibt es viele OT-Geräte, die sich nicht in die neue Welt migrieren lassen. Dann bleibt nur die Frage: Trennst du sie komplett vom Internet – was selbst schwierig ist – oder arbeitest du langfristig an einer Migration.

Was bedeutet das für Hersteller, die heute Maschinen verkaufen, die noch zwanzig Jahre laufen sollen?
RS | Diese Frage habe ich erwartet. Auch hier ist die Pflicht klar: Als Maschinenhersteller musst du heute sicherstellen können, dass deine Geräte sicher sind und sich die Security-Layer austauschen lassen. Im Consumer-Bereich gibt es dafür bereits Standards wie Matter. [Anm. d. Red.: ein Interoperabilitätsstandard der Connectivity Standards Alliance; DigiCert bietet dafür eigene Sicherheitslösungen an] Ich glaube, das wird sich als Best Practice durchsetzen. Aber es gibt immer noch Hersteller, die das Thema stiefmütterlich behandeln. Gleichzeitig ist der Kunde in der Pflicht, die richtigen Fragen zu stellen und das einzufordern.

Wie reagiert ein Mittelständler auf diesen Druck – zahlt er im Zweifel lieber die Strafe, oder drohen echte Wettbewerbsnachteile?
RS | Ein Beispiel: Wir arbeiten eng mit einem deutschen Hersteller für Gesundheitsgeräte zusammen. Er konnte seine Geräte nicht mehr auf den Markt bringen, weil er ohne Sicherheitsnachweis keine Versicherung mehr bekam. Es geht also nicht nur über Regulierung, sondern auch über den Versicherungsmarkt: Solange du nicht nachweisen kannst, dass deine Geräte geprüft sind, kommst du nicht mehr auf den Markt. Spätestens dann fällt der Groschen. Je kleiner ein Unternehmen ist, desto eher fällt es allerdings noch durch dieses Raster. •

Die Kontext-Lücke: Warum separierte Tools zum Desaster führen

Ein Alarm allein sagt wenig aus. Erst die Verknüpfung mit Endpoint, Cloud-Umgebung und Netzwerk zeigt, ob aus einem Klick ein einzelner Sicherheitsvorfall oder eine Krise wird.

/// von Richard Werner

DIE GRÖSSTE SCHWACHSTELLE IN UNTERNEHMEN LIEGT SELTEN IM EINZELNEN TOOL, sondern in der Lücke dazwischen. Viele IT-Umgebungen sind über Jahre gewachsen. Jede Ebene – E-Mail, Endpoint, Cloud, Netzwerk – hat ihre eigene Lösung, ihr eigenes Dashboard, ihre eigene Logik. Das Ergebnis: Sicherheitsteams sichten täglich Tausende von Signalen, ohne den gesamten Zusammenhang zu sehen.

In der Praxis zeigt sich dieses Muster immer wieder in ähnlicher Form. Über Jahre gewachsene Sicherheitsarchitekturen bestehen aus Einzellösungen mit jeweils eigenem Dashboard. Eine konsolidierte Gesamtsicht auf Risiken fehlt. Lücken lassen sich dann nur reaktiv bearbeiten, niemals proaktiv, und vieles bleibt schlicht unsichtbar, bis es zu spät ist.

> „ Wenn Unternehmen **E-Mail-Security, Endpunktschutz und XDR-Plattform-Komponenten zusammenführen**, sinkt der operative Aufwand in der Praxis – bei gleichzeitig höherer Sicherheit. *Richard Werner*

Alert Fatigue kostet Zeit

Fragmentierung erzeugt ein zweites Problem: Alert Fatigue. Analysten korrelieren Events aus unterschiedlichsten Tools manuell und entscheiden unter Zeitdruck, was kritisch ist. Zu viele Daten, zu wenig Kontext, zu wenig Zeit – relevante Signale gehen im Grundrauschen unter. Genau in diesem Fenster zwischen erster Anomalie und erkanntem Angriff entscheidet sich, ob aus einem Incident ein Desaster wird.

Häufig ist es ein einzelnes, vermeintlich kleines Symptom, das den Wandel anstößt: steigendes Spam-Aufkommen, ein auffälliger Login, ein blockierter Datei-Upload. Der eigentliche Befund liegt aber meist tiefer, in der fehlenden Korrelationsfähigkeit und Analysetiefe der eingesetzten Systeme. Das führt direkt zur Plattformfrage.

Ein Score statt vieler Dashboards

Der entscheidende Bruch mit der alten Logik: Statt isolierter Tools führt eine Plattform Telemetriedaten aus Endpunkten, E-Mail, Cloud und Netzwerk in einer zentralen Konsole zusammen und korreliert sie KI-gestützt. Ein solcher Ansatz – etwa mit TrendAI Vision One – kombiniert Endpoint Security, E-Mail- und Collaboration-Security sowie Cyber Risk Exposure Management (CREM) in einer Umgebung, die sowohl die IT-Infrastruktur als auch Cloud-Workloads abdeckt.

Das Herzstück ist ein kontinuierlich berechneter Risiko-Score von 0 bis 100, der aus allen angeschlossenen Systemen gespeist wird. Werte unter 30 gelten als geringes Risiko. Will die Geschäftsleitung den Score um fünf Punkte senken, zeigt die Plattform automatisch, welche Maßnahmen dafür nötig sind – inklusive Einschätzung des jeweiligen Impacts. Aus einer diffusen Bedrohungslage wird eine planbare Kennzahl.

Vektorübergreifend statt isoliert

Den Unterschied macht die Reichweite der Korrelation. Die XDR-Komponente von TrendAI Vision One beispielsweise analysiert Endpunkte, E-Mail und Cloud im Zusammenhang und deckt Angriffsmuster auf, die bei getrennter Betrachtung unsichtbar blieben. Besondere Aufmerk-

DER AUTOR
Richard Werner
ist Business Consultant bei TrendAI,
dem Enterprise-Geschäftsbereich von Trend Micro.

Bild: Trend Micro

> „ Wer 2026 auf Konsolidierung statt auf Einzellösungen setzt, **gewinnt vor allem Zeit:** Zwischen Erkennung und Reaktion, für das eigene Team und um Investitionen gegenüber der Geschäftsleitung zu begründen. *Richard Werner*

samkeit verdienen dabei gemeinsam genutzte virtuelle Desktop-Umgebungen, wie sie viele Unternehmen heute in der Cloud betreiben: Dort können sich Bedrohungen unter Umständen auf mehrere Nutzer gleichzeitig auswirken. Plattform-Technologie ersetzt in solchen Konstellationen keine Implementierungserfahrung, sondern setzt sie voraus.

Der Konsolidierungseffekt lässt sich auch wirtschaftlich beziffern. Wenn Unternehmen E-Mail-Security, Endpunktschutz und XDR-Plattform-Komponenten zusammenführen, sinkt der operative Aufwand in der Praxis– bei gleichzeitig höherer Sicherheit. Der Wegfall multipler Einzel-Dashboards entlastet IT-Teams spürbar, weil alle relevanten Informationen in einer Konsole zusammenlaufen. Ein naheliegender nächster Schritt ist die Erweiterung um Netzwerksicherheit als vierten Vektor, um auch hier Telemetriedaten in dieselbe Korrelation einzuspeisen.

Wenn die Plattform selbst reagiert

Erkennung allein reicht nicht – die Geschwindigkeit der Reaktion entscheidet über das Ausmaß des Schadens. Identifiziert die Plattform ein Risiko, kann sie anhand definierter Regeln automatisiert Gegenmaßnahmen auslösen, etwa Phishing-Mails isolieren oder kompromittierte Konten sperren. Standardisierte Abläufe laufen automatisch, während sich Analysten auf komplexe Fälle konzentrieren.

Das SOC wandelt sich damit von einer reaktiven Alarmzentrale zu einer Instanz, die aktiv in die Abwehrprozesse eingreift.

Der neue Vektor heißt KI

So weit die etablierten Vektoren Endpoint, E-Mail, Cloud und Netz. Parallel entsteht jedoch eine Angriffsfläche, die viele Unternehmen noch nicht im Blick haben: ihre eigenen KI-Systeme. Eine aktuelle Studie von TrendAI zeigt, dass 70 Prozent der deutschen Unternehmen KI-Projekte trotz bestehender Sicherheitsbedenken freigegeben haben. Nur 41 Prozent verfügen über umfassende Richtlinien für den sicheren KI-Einsatz. Allein 2025 wurden mehr als 2.100 neue KI-bezogene Schwachstellen dokumentiert, besonders betroffen sind agentische Systeme und neue Schnittstellen wie MCP-Server.

Für Sicherheitsverantwortliche bedeutet das: Die Plattform muss nicht nur Endpoint, Cloud und Netzwerk korrelieren, sondern auch erkennen, welche KI-Anwendungen im Unternehmen überhaupt laufen. Genau hier setzt Cyber Risk Exposure Management an – es ordnet neu entstehende KI-Risiken, etwa Schatten-KI oder riskante Datenflüsse, in den Gesamtkontext der Angriffsfläche ein, bevor daraus ein konkreter Vorfall wird.

Wer 2026 auf Konsolidierung statt auf Einzellösungen setzt, gewinnt vor allem eines: Zeit. Zeit zwischen Erkennung und Reaktion, Zeit für das eigene Team, Zeit, um Investitionen gegenüber der Geschäftsleitung zu begründen. Der Ansatz funktioniert nicht nur für Konzerne, sondern gerade für Unternehmen mit knappen Ressourcen. Der nächste Schritt liegt bei jedem Unternehmen selbst: den eigenen Flickenteppich ehrlich zu kartieren, bevor dies ein Angreifer macht. •

Warum XDR zum Effizienzfaktor in der IT-Sicherheit wird

Unternehmen stehen im Spannungsfeld aus immer komplexeren Cyberangriffen, Fachkräftemangel, einer Informationsflut aus eingesetzten Sicherheitslösungen und begrenzten Ressourcen: Einen Ausweg bietet eine Extended-Detection-and-Response-Lösung (XDR). /// von Kathrin Beckert Plewka

CYBERKRIMINELLE SETZEN BEI ANGRIFFEN HEUTZUTAGE HÄUFIG AUF AUTOMATISIERTE METHODEN. Damit infiltrieren sie Unternehmensnetzwerke, agieren darin und verschlüsseln am Ende Daten und die Systeme. Daher ist es wichtig, schädliche Vorgänge frühzeitig zu entdecken und diese zu beenden. Viele IT-Verantwortliche in Firmen setzen für eine umfassende IT-Sicherheit auf eine Vielzahl von Security Lösungen. Dabei liefern Endpoint Protection, E-Mail-Security, Netzwerküberwachung, Cloud-Sicherheit und weitere Systeme wertvolle Informationen über potenzielle Bedrohungen.

DIE AUTORIN
Kathrin Beckert-Plewka
ist Public Relations Manager bei G DATA CyberDefense.

> „ XDR überwacht Prozesse, Dateien und das über einzelne Geräte hinaus. Auf der Plattform sind die Informationen aus Vorgängen im Netzwerk **zentral korreliert**. IT-Teams haben damit alle wichtigen Daten im Blick. Hierdurch entsteht ein **deutlich klareres Bild möglicher Angriffe**.
>
> *Kathrin Beckert-Plewka*

Doch genau hier entsteht ein neues Problem: die Alarmflut. Sicherheitswerkzeuge erzeugen täglich eine große Anzahl von Meldungen, Warnungen und Ereignissen. Diese müssen analysiert, eingeordnet und bewertet werden. Viele IT-Teams in Unternehmen sind aufgrund von Personal- und Ressourcenmangel nicht in der Lage, diese Arbeit zu leisten. In der Folge werden die Informationen nur unzureichend oder gar nicht gesichtet. Hierdurch bleiben im schlimmsten Fall relevante Hinweise auf Cyberattacken in der Masse an Daten unerkannt, mit weitreichenden Folgen. Klar ist, dass nicht jeder Alarm gleich einen kritischen Sicherheitsvorfall darstellt. Trotzdem muss jeder Alarm mit der nötigen Aufmerksamkeit bedacht werden.

Wenn Komplexität zur eigentlichen Herausforderung wird
Die zentrale Herausforderung einer modernen Cyberabwehr besteht deshalb nicht mehr allein darin, Angriffe zu erkennen. Vielmehr geht es darum, Sicherheitsereignisse effizient zu verarbeiten und daraus schnell die richtigen Maßnahmen abzuleiten. Dabei stoßen klassische Sicherheitsansätze an Grenzen. Zusammenhängende Hinweise auf einen aktuell laufenden Angriff sind nicht zu erkennen, wenn die Informationen aus den unterschiedlichen Systemen isoliert betrachtet werden. Ein einzelnes Ereignis erscheint für sich gesehen harmlos. Erst die Verknüpfung mehrerer Aktivitäten zeigt, dass ein Angreifer bereits verschiedene Systeme kompromittiert oder sich seit längerer Zeit im Netzwerk bewegt.

Unternehmen benötigen daher Lösungen, die Sicherheitsinformationen nicht nur sammeln, sondern auch

intelligent zusammenführen. Genau an diesem Punkt gewinnen Extended Detection and Response (XDR)-Plattformen an Bedeutung.

XDR als Antwort auf wachsende Anforderungen an IT-Sicherheit

XDR überwacht Prozesse, Dateien und das über einzelne Geräte hinaus. Auf der Plattform sind die Informationen aus Vorgängen im Netzwerk zentral korreliert. IT-Teams haben damit alle wichtigen Daten im Blick. Ereignisse sind nicht isoliert dargestellt, sondern in einen Kontext zueinander gesetzt. Hierdurch entsteht ein deutlich klareres Bild möglicher Angriffe.

Ein weiterer Vorteil besteht darin, dass eine Flut von Alarmen ausbleibt. Extended Detection and Response zeigt nicht hunderte Einzelmeldungen, sondern priorisierte Vorfälle mit nachvollziehbaren Zusammenhängen. Das erleichtert Mitarbeitenden in Unternehmen oder bei Dienstleistern die Analyse und Bewertung der Aktionen. Ursachen sind schneller zu erkennen. Das beschleunigt die Reaktion auf schädliche Vorfälle, um ungewollte Aktivitäten und Cyberangriffe zu beenden. Dabei spielt die Automatisierung eine entscheidende Rolle. Moderne XDR-Lösungen unterstützen Unternehmen dabei, wiederkehrende Aufgaben zu automatisieren, Vorfälle vorzubewerten und erste Reaktionsmaßnahmen einzuleiten. Angesichts knapper personeller Ressourcen ist diese Entlastung zunehmend ein entscheidender Faktor.

Mehr Effizienz statt mehr Komplexität

XDR ist nicht nur nach technologischen Gesichtspunkten bedeutsam. Mit dem Einsatz von Extended Detection and Response begegnen IT-Verantwortliche vielmehr einer wirtschaftlichen und organisatorischen Herausforderung: Die dauerhafte Sicherstellung der Cyberabwehr trotz wachsender Bedrohungen und begrenzter Ressourcen. Firmen müssen ihre IT-Security so konzipieren, dass sie effizient vor Angriffen schützt.

Dabei muss die Handlungsfähigkeit des IT-Teams gewährleistet sein, selbst bei wachsenden Datenmengen aus der Sicherheitsarchitektur. Eine XDR-Lösung leistet dies und sie hilft, Fachkräfte gezielter einzusetzen und Reaktionszeiten zu verkürzen.

Gerade in Zeiten zunehmender Digitalisierung wird die Fähigkeit, Sicherheitsvorfälle effizient zu erkennen und zu bearbeiten, zu einem zentralen Erfolgsfaktor. Extended Detection and Response steht deshalb für einen Ansatz, Cyberabwehr wirtschaftlich skalierbar und organisatorisch beherrschbar zu machen. •

KI-WETTLAUF-CHECK

Automatisierte Angriffe erzeugen eine Alarmflut, in der echte Warnsignale untergehen.

XDR korreliert Signale automatisiert und entlastet knappe IT-Teams.

Keine Pause für die Cyberabwehr

Künstliche Intelligenz verändert die Bedrohungslandschaft vor allem durch einen Faktor: Geschwindigkeit. Angriffe lassen sich schneller, parallel und zunehmend autonom ausführen. Unternehmen benötigen daher umfassende Security Operations, die das Zusammenspiel zwischen Mensch und Maschine neu denken. /// von Dr. Sebastian Schmerl

KI SENKT DIE EINSTIEGSHÜRDE FÜR CYBERANGRIFFE. Dafür müssen Angreifer nicht einmal völlig neue Methoden entwickeln. Entscheidend ist, dass KI bekannte Prozesse beschleunigt und fehlende Kenntnisse ausgleicht. Wer früher detailliertes Know-how über Schwachstellen, Exploits und Angriffswerkzeuge benötigte, nutzt heute ein KI-System bei der Auswahl und Anwendung geeigneter Methoden. Mit Agentic AI geht diese Entwicklung einen Schritt weiter. Statt einzelne Aktionen durch Prompts anzustoßen, geben Angreifer ein Ziel vor, auf das ein KI-Agent weitgehend selbstständig hinarbeitet. Gleichzeitig können mehrere solcher Agenten parallel agieren. Angriffe werden damit nicht nur schneller, sondern skalierbarer. Und anders als der Mensch braucht eine Angriffs-KI weder Schlaf noch Ruhezeiten.

Das Zeitfenster schrumpft

Für die Verteidigung bedeutet das: Die Zeit zwischen Erkennung und Reaktion wird zum kritischen Faktor. Managed Detection and Response mit proaktiven, aufdeckenden und reaktiven Maßnahmen bleibt ein wesentliches Element. Es reicht nicht aus, verdächtige Aktivitäten zu erkennen und anschließend auf eine menschliche Entscheidung zu warten. Eine wirksame Verteidigung muss rund um die Uhr arbeiten. Ein externes Security Operations Center (SOC) stellt die notwendige kontinuierliche Überwachung, Erfahrung und Reaktionsfähigkeit bereit. Gerade der KI-Einsatz verlangt eine breite Datenbasis und kontinuierliches Training: Wer nur die eigene Umgebung und vergleichsweise wenige Sicherheitsvorfälle sieht, kann neue Angriffsmuster schwerer erkennen und automatisierte Reaktionen kaum weiterentwickeln.

Der Mensch als Cybersecurity-Flaschenhals

Damit verändert sich auch der Human-in-the-Loop-Ansatz. Bislang endet Automatisierung häufig dort, wo konkrete Gegenmaßnahmen beginnen. Im SOC prüft ein Analyst den Vorfall und entscheidet über die angemessene Reaktion. Muss anschließend noch ein Verantwortlicher im Unternehmen einbezogen werden, können aus Minuten schnell Stunden werden. Dadurch entsteht eine gefährliche Verzögerung. Die Grenze muss sich in Richtung automatisierter Response verschieben. Dabei geht es nicht darum, bei jedem Verdacht sofort Systeme vom Netz zu nehmen. Sinnvoll ist ein abgestuftes Modell: Maßnahmen mit geringen Auswirkungen auf den IT-Betrieb, etwa zusätzliche Authentifizierungen oder temporär verschärfte Zugriffsregeln, lassen sich früh automatisiert auslösen. Je einschneidender die möglichen Folgen einer Maßnahme sind, desto wichtiger bleibt die menschliche Entscheidung.

Mensch und KI wechseln die Rollen

Der Mensch verschwindet damit nicht aus dem SOC. Seine Aufgabe verändert sich aber. Statt jeden Alarm selbst zu prüfen, überwacht er automatisierte Entscheidungen, kontrolliert deren Qualität stichprobenartig, bewertet komplexe Fälle und verbessert mithilfe von KI die Abwehr. Auch neue Angriffsmethoden zu verstehen und geeignete Gegenstrategien zu entwickeln, bleibt eine menschliche Aufgabe. In Zukunft dürfte diese Grenze weiter wandern. Security Operations werden enger mit dem IT-Betrieb verzahnt. Gleichzeitig werden auf Angreifer- wie Verteidigerseite autonome KI-Systeme immer stärker gegeneinander antreten. Cyberabwehr wird damit zunehmend zum KI-Wettlauf, bei dem der Igel nicht erst loslaufen darf, wenn der Hase längst unterwegs ist.•

DER AUTOR
Dr. Sebastian Schmerl
ist Vice President Security Services EMEA bei Arctic Wolf.

Zwei Seiten der KI-Sicherheit:

Warum Unternehmen jetzt handeln müssen

KÜNSTLICHE INTELLIGENZ IST IM UNTERNEHMENSALLTAG ANGEKOMMEN. Mitarbeitende nutzen generative KI-Tools im Arbeitsalltag, Fachabteilungen automatisieren Prozesse und immer häufiger ist KI direkt in die Geschäftsanwendungen integriert. Auch die Cybersecurity wird durch KI-gestützte Lösungen schneller und effizienter. Somit entsteht eine neue Situation: Einerseits verbessert KI die Sicherheit, andererseits erzeugt sie aber auch eine neue Angriffsfläche. Ein Kernproblem ist fehlende Transparenz. Vielen IT- und Security-Abteilungen ist gar nicht bekannt, welche KI-Anwendungen im Unternehmen tatsächlich genutzt werden. So entsteht Schatten-KI. Um dieses Risiko überhaupt bewerten zu können, benötigen Unternehmen zunächst Transparenz: **TrendAI Vision One™** führt Daten aus den unterschiedlichsten Bereichen zusammen und macht so Schatten-KI, riskante Datenflüsse und neue Angriffswege sichtbar, bevor

Effizientere Cybersicherheit mit KI

KI wird in der Cybersicherheit immer mehr zum Produktivitätsfaktor, ermöglicht sie doch effizientere Security Operations auch mit kleinen Teams. Genau hier setzt die KI-basierte Sicherheitsplattform **TrendAI Vision One™** an: Sie konsolidiert Telemetriedaten aus Endpunkten, E-Mail, Cloud, Identitäten und Netzwerken auf einer zentralen Oberfläche. KI-Agenten korrelieren Ereignisse, priorisieren Risiken und unterstützen bei der Reaktion auf Bedrohungen. So sinkt die operative Komplexität, während Transparenz und Effizienz steigen.

Die neue Angriffsfläche heißt KI

Während Security-Teams zunehmend von KI profitieren, schafft sie an anderer Stelle jedoch auch neue Risiken. Denn KI wird oft schneller eingeführt als die dazugehörigen Sicherheitsmaßnahmen mithalten können. Eine aktuelle Studie von TrendAI zeigt: 70 Prozent der deutschen Unternehmen haben KI-Projekte trotz bestehender Sicherheitsbedenken freigegeben, nur 41 Prozent verfügen über umfassende Richtlinien für den sicheren KI-Einsatz. daraus Vorfälle entstehen. Dabei geht es längst nicht nur um Datenschutz: Prompt-Injection-Angriffe können Modelle manipulieren, agentische Systeme erhalten direkten Zugriff auf Geschäftsprozesse. Allein 2025 wurden mehr als 2.100 neue KI-bezogene Schwachstellen dokumentiert, besonders bei Agentic-AI-Systemen und MCP-Servern. Für viele Unternehmen entsteht dadurch eine Situation, die sie bereits aus der Cloud-Einführung kennen: Die Technologie wird schneller eingeführt, als Governance, Prozesse und Sicherheitsmaßnahmen nachziehen können.

Von IT-Sicherheit zu AI Security

Security-Teams werden deshalb zukünftig vermehrt Fragen beantworten müssen, wie: Welche KI-Anwendungen sind im Einsatz? Welche Risiken entstehen durch KI-Agenten? Wie lassen sich regulatorische Anforderungen erfüllen? Mit Funktionen für Cyber Risk Exposure Management unterstützt sie **TrendAI Vision One™** dabei, einen kontinuierlichen Überblick über Risiken in der gesamten IT- und KI-Landschaft zu behalten und die richtigen Antworten zu finden. •

TrendAI™ | AI Fearlessly

Wie Unternehmen Compliance für Cyberversicherungen erreichen können

Eine wachsende Sicherheitslücke macht viele Unternehmen anfällig für neue Cyberbedrohungen. Wir zeigen Ihnen, wie Sie Prämien für Cyberversicherungen senken können. /// von Kay Ernst

DER WELTWEITE MARKT FÜR CYBERVERSICHERUNGEN ist bis 2026 auf rund 20 Milliarden US-Dollar angewachsen – getrieben von Ransomware, KI-gestützten Angriffen und wachsendem regulatorischem Druck. Trotzdem hat etwa ein Fünftel der mittleren und großen Unternehmen noch keine Cyberversicherung, meist wegen der Kosten: Prämien steigen laut Marktforschung um bis zu 30 Prozent. Um sich zu qualifizieren, müssen Unternehmen technische Kontrollen wie MFA, Netzwerksegmentierung, identitätsbasierte Zugriffskontrollen und Incident-Response-Pläne nachweisen. Versicherer legen dabei zunehmend Wert auf proaktive Cyberhygiene statt reiner Mindestanforderungen.

Versicherer verlangen Netzwerksegmentierung

Ein wichtiger Hebel zur Prämiensenkung ist Mikrosegmentierung, die laterale Bewegungen von Angreifern unterbindet. Aaron Goodwin, CISO bei B. Riley Financial, betont, dass fast alle heutigen Angriffe laterale Bewegungen nutzen, um Kontrolle über die Umgebung zu erlangen – mit entsprechenden Folgekosten für Behebung und Prämien. Fast 70 Prozent der Unternehmen berichten, dass ihr Versicherer Netzwerksegmentierung verlangt, wobei automatisierte Mikrosegmentierung klassischen VLAN-Ansätzen deutlich überlegen ist. Höhere Segmentierungsreife korreliert hierbei mit niedrigeren Prämien.

Ebenso wichtig ist Least-Privilege-Zugriff über granulare, identitätsbasierte Kontrollen, da gestohlene Anmeldedaten der häufigste Angriffsweg bleiben. Jeff Bird von Marsh erklärt, dass es bei den meisten Angriffen heute nicht um das Eindringen ins System handelt, sondern um das Einloggen mit gestohlenen Zugangsdaten als vermeintlich legitimer Nutzer. Da Maschinenidentitäten wie Dienstkonten inzwischen über 70 Prozent aller vernetzten Identitäten ausmachen, wollen Versicherer den Beleg, dass ein gestohlenes Konto keine Katastrophe auslöst.

Ein dritter Baustein ist Just-in-Time-MFA für Administratorkonten und Protokolle wie RDP oder SSH, um Rechteausweitung zu verhindern, ohne den Betrieb zu stören. Christ Turek, CIO bei Evercore, beschreibt es als bahnbrechend, Auditoren zeigen zu können, dass die Zahl der Admin-Konten irrelevant wird, wenn diese ohne Zwei-Faktor-Authentifizierung nichts ausrichten können. In Kombination mit Netzwerk- und Identitätssegmentierung entsteht so eine mehrdimensionale Verteidigung.

Incident-Response-Planung senkt Kosten einer Datenverletzung

Auch Geschäftsresilienz zählt: Gute Incident-Response-Planung senkt die Kosten einer Datenverletzung um rund 250.000 US-Dollar, doch starre Pläne veralten schnell. Proaktive, automatisierte Bedrohungseindämmung überzeugt Versicherer stärker. Da Cyberpolicen oft auch Bußgelder aus Verstößen abdecken, sollten Unternehmen zudem branchenübergreifend gültige Sicherheitsstandards implementieren und laufend an Netzwerkänderungen anpassen. Letztlich setzen Versicherer eine Zero-Trust-Architektur voraus. Eine Plattform, die Netzwerk- und Identitätssegmentierung mit Zero-Trust-Netzwerkzugang und MFA kombiniert, bietet dynamischen, mehrdimensionalen Schutz – und senkt damit nachweislich die Prämien. •

DER AUTOR
Kay Ernst
ist Country Manager DACH bei Zero Networks und verantwortet die strategische und operative Entwicklung des Unternehmens in Deutschland, Österreich und der Schweiz.
Bild: Zero Networks

> „ Um sich zu qualifizieren, müssen Unternehmen technische Kontrollen wie **MFA, Netzwerksegmentierung, identitätsbasierte Zugriffskontrollen und Incident-Response-Pläne** nachweisen.
>
> *Kay Ernst*

So sichert F5 eigenen Code mit fortschrittlicher KI

MEHR ALS 80 PROZENT DER GLOBAL FORTUNE 500 NUTZEN F5-LÖSUNGEN UND ERWARTEN BESTMÖGLICHEN SCHUTZ. Entsprechend setzt F5 besonders leistungsfähige KI ein, sogenannte „Frontier AI"-Modelle, um den eigenen Quellcode systematisch auf Schwachstellen zu prüfen. Dazu verfügt F5 über eine spezielle Infrastruktur, die technische Ressourcen aus dem gesamten Unternehmen bündelt und „Security by Design" unternehmensweit mit höchster Priorität umsetzt.

KI hat inzwischen eine neue Evolutionsstufe erreicht. Frontier-Modelle von Anthropic und OpenAI, darunter Claude Mythos und GPT Cyber, können nun in Sekunden reale Schwachstellen aufdecken und Entwicklern helfen, diese zu schließen. Allerdings können Angreifer diese Modelle auch für böswillige Zwecke einsetzen, trotz entsprechender Schutzmaßnahmen. Deshalb nutzt F5 kontinuierlich modernste KI-Modelle, um Code zu prüfen und zu verbessern, damit böswillige Akteure keine Chance mehr haben.

Entwicklung von Tools, Testumgebungen und Prozessen
Inzwischen hat F5 Tools entwickelt, die einen neuartigen Ansatz bei der Fehleranalyse und dem Schwachstellenmanagement verfolgen. Die Codebasis umfasst mehrere Millionen Zeilen in den Programmiersprachen C, C++, Python, Tcl, Java, Go sowie Low-Level-C für FPGAs. Unabhängig vom jeweiligen Tool folgt die Scan-Infrastruktur diesem strengen, mehrstufigen Prozess:

1. **Einfügen:** Einspeisen des Quellcodes aus den wichtigsten Modulen und Sprachen, damit die Modelle auf Grundlage realer Implementierungsdetails Schlussfolgerungen ziehen können.
2. **Analysieren:** KI-gestützte statische Analysen, um Fehler, riskante Muster und verdächtige Abläufe zu erkennen. Dazu zählen etwa fehlerhafte Authentifizierungslogik, unsichere Kryptografie oder Probleme mit der Speichersicherheit.
3. **Klassifizierung:** Erfassung strukturierter Befunde – von CWE-Zuordnungen und Schweregrad-Bewertungen über Datei- und Zeilenreferenzen bis hin zu Angaben, unter welchen Bedingungen sich eine Schwachstelle ausnutzen lässt.
4. **Verifizierung:** Ein zweites Modell prüft die Befunde, um sie zu bestätigen, neu zu priorisieren oder zu verwerfen, bevor sie in die Entwicklung gelangen. Damit reduziert das System Fehlalarme deutlich.
5. **Beheben:** Validierte Befunde werden priorisiert behoben. Entsprechende Korrekturen folgen nach einem Test.

Die Scan-Infrastruktur von F5 folgt einem strengen, mehrstufigen Prozess
Eines der wichtigsten Ergebnisse dieses Prozesses ist die operative Stärke, welche die Entwicklungsabteilung von F5 in den letzten Monaten aufgebaut hat. Das Scannen ist nur ein Teil einer durchgängigen, neu geschaffenen Fähigkeit. F5 wechselt von einem vierteljährlichen Release-Rhythmus zu häufigeren, stabilen Releases für die gesamte Software. Dies ist eine massive operative Umstellung. Zwar verfügt das Unternehmen bereits seit Jahren über strenge Scan- und Testverfahren, jedoch verfolgt F5 nun einen neuen KI-gesteuerten Zyklus aus Scannen, Triage, Beheben, Testen, Freigabe und Wiederholung. •

Wollen Sie mehr über F5 und wirksame Strategien gegen KI-basierte Angriffe erfahren?
Dann freuen wir uns auf Ihren Besuch während der it-sa Messe in Nürnberg an unserem Stand 7A-531

Agenten an die kurze Leine legen

KI-Agenten greifen zunehmend eigenständig auf Unternehmensdaten und Systeme zu – und werden damit zum neuen Angriffsziel. Wie Ionos zeigt, entscheidet nicht die Leistungsfähigkeit eines Agenten über seine Sicherheit, sondern die konsequente Begrenzung seiner Zugriffsrechte auf das tatsächlich Notwendige. /// von Rijesh Haridas

KI-AGENTEN ENTWICKELN SICH DERZEIT VON EINER TECHNOLOGIE FÜR PILOTPROJEKTE ZU EINEM WERKZEUG, das zunehmend Einzug in den Unternehmensalltag hält. Sie analysieren Daten, greifen auf Anwendungen zu und übernehmen Aufgaben, die bislang manuell erledigt wurden. Gleichzeitig wächst das Bewusstsein für die Sicherheitsrisiken, die mit dieser Entwicklung einhergehen. Denn je enger KI-Agenten mit Unternehmensdaten und IT-Systemen verbunden werden, desto wichtiger wird die Kontrolle über ihre Zugriffsrechte.

Die Diskussion dreht sich häufig um die Fähigkeiten dieser neuen Systeme. Unternehmen stellt sich jedoch eine andere Herausforderung: Wie lassen sich KI-Agenten produktiv nutzen, ohne ihnen weitreichende Berechtigungen auf kritische Systeme einzuräumen? Nicht jede Aufgabe, die ein Agent übernehmen soll, erfordert auch die Möglichkeit, Änderungen an einer Infrastruktur vorzunehmen.

Nicht jede Aufgabe erfordert uneingeschränkten Zugriff

Viele Anwendungsfälle von Agentic AI beruhen darauf, bestehende Informationen auszuwerten. Konfigurationen lassen sich prüfen, Ressourcen analysieren oder Auffälligkeiten identifizieren, ohne dass ein Agent selbst Änderungen an einer Infrastruktur vornehmen muss. Daraus ergibt sich ein Ansatz, der zunehmend an Bedeutung gewinnt: Analyse- und Änderungsfunktionen voneinander zu trennen und KI-Agenten gezielt auf Lesezugriffe zu beschränken.

Mit dem Ionos Cloud MCP Server verfolgen wir genau diesen Ansatz. Der Open-Source-Server verbindet KI-Assistenten über das Model Context Protocol (MCP) mit einem Ionos-Cloud-Konto und beschränkt verfügbare Funktionen bewusst auf Analyse- und Abfrageoperationen. Funktionen zum Erstellen, Ändern oder Löschen von Cloud-Ressourcen sind nicht vorgesehen. Typische Einsatzszenarien reichen von Sicherheits-Audits über FinOps-Auswertungen bis hin zu Compliance- und Infrastrukturanalysen. Der Read-only-Ansatz soll Risiken durch Prompt-Injections oder fehlerhafte Agent-Schleifen strukturell begrenzen. Fehler wirken sich dadurch im schlimmsten Fall auf Analyseergebnisse aus, nicht jedoch unmittelbar auf produktive Systeme.

Gleichzeitig gewinnt die Frage an Bedeutung, wo Daten verarbeitet werden und welche Systeme an einem Agentic-AI-Workflow beteiligt sind. Unternehmen müssen nicht nur Zugriffsrechte kontrollieren, sondern auch jederzeit nachvollziehen können, wo Modelle, Prompts und Ergebnisse verarbeitet werden. In Kombination mit dem AI Model Hub können Verarbeitung, Tool-Ausgaben und Infrastrukturzugriffe innerhalb deutscher Rechenzentren verbleiben. Sicherheit, Transparenz und digitale Souveränität werden damit zu einem zentralen Bestandteil moderner Agentic-AI-Architekturen.

Was Unternehmen jetzt berücksichtigen sollten

Der aktuelle Trend zu Agentic AI zeigt, dass Sicherheit und Kontrolle bereits bei der Konzeption neuer Anwendungen berücksichtigt werden müssen. Dazu gehören insbesondere:

> „ Unternehmen müssen nicht nur Zugriffsrechte kontrollieren, sondern auch **nachvollziehen können**, wo Modelle, Prompts und Ergebnisse verarbeitet werden.
>
> *Rijesh Haridas*

- **Zugriffsrechte gezielt begrenzen:** Viele Analyse-, Monitoring- und Audit-Aufgaben lassen sich bereits mit Lesezugriffen umsetzen. Umfangreiche Systemrechte sind dafür häufig nicht erforderlich.
- **Mit überschaubaren Anwendungsfällen starten:** Analyse-, Reporting- und Audit-Szenarien eignen sich besonders für erste Agentic-AI-Projekte. Denn sie schaffen einen Mehrwert, ohne direkt in produktive Systeme einzugreifen.

- **Transparenz über Datenflüsse schaffen:** Je mehr Systeme angebunden sind, desto wichtiger ist der klare Überblick darüber, welche Daten ein Agent verarbeitet und wofür sie genutzt werden.
- **Verarbeitung bewusst steuern:** Neben den Zugriffsrechten spielt auch der Ort der Verarbeitung eine wichtige Rolle. Unternehmen müssen nachvollziehen können, wo Modelle, Prompts und Ergebnisse verarbeitet werden.

Für Unternehmen wird damit deutlich: Der erfolgreiche Einsatz von

> „ Unternehmen müssen nicht nur Zugriffsrechte kontrollieren, sondern auch **jederzeit nachvollziehen** können, wo Modelle, Prompts und Ergebnisse verarbeitet werden.
>
> *Rijesh Haridas*

Agentic AI hängt nicht allein von leistungsfähigeren Modellen ab. Ebenso wichtig ist die Frage, welche Rechte ein Agent tatsächlich benötigt. Viele Analyse-, Monitoring- und Audit-Aufgaben lassen sich bereits mit klar begrenzten Berechtigungen umsetzen. Ansätze wie Read-only-Konzepte zeigen, dass sich produktive Einsatzszenarien oft auch ohne umfassende Systemrechte realisieren lassen. Gleichzeitig gewinnt die Frage an Bedeutung, wie Unternehmen Sicherheit, Kontrolle und digitale Souveränität entlang des gesamten Datenflusses sicherstellen können. •

KI-WETTLAUF-CHECK

Prompt-Injections nutzen weitreichende Agent-Rechte für Zugriffe auf Produktivsysteme.

Read-only-Architektur begrenzt Fehler strukturell auf die Analyseebene.

DER AUTOR

Rijesh Haridas ist Product Manager Public Cloud bei Ionos.

KI OHNE KONTROLLVERLUST

Generative KI verspricht enorme Effizienzgewinne – doch wer sensible Unternehmensdaten in öffentliche Sprachmodelle einspeist, riskiert genau die Kontrolle, die Compliance und Wettbewerbsfähigkeit erst absichert. Warum private, europäisch betriebene LLM-Architekturen 2027 zum Standard werden. /// von Heiner Sieger

KAUM EINE TECHNOLOGIE HAT SICH IN DEN VERGANGENEN ZWEI JAHREN SO SCHNELL IN DEN ARBEITSALLTAG GESCHOBEN WIE GENERATIVE KI. Vertriebsteams lassen sich Angebote vorformulieren, Entwickler generieren Code, das Management fasst Reports zusammen. Journalisten recherchieren Beiträge. Was dabei oft übersehen wird: Ein erheblicher Teil dieser Anfragen läuft über öffentlich zugängliche Sprachmodelle – und damit über Infrastruktur, deren Standort, Betreiber und Datenverwendung sich der Kontrolle des Unternehmens entziehen.

Schatten-KI als unterschätztes Einfallstor

Ähnlich wie bei der Schatten-IT vor zehn Jahren entsteht heute eine neue Grauzone: Mitarbeitende nutzen öffentliche KI-Tools im Browser, ohne dass IT-Abteilungen wissen, welche Daten dabei das Unternehmen verlassen. Vertragsentwürfe, Kundendaten, interne Kennzahlen – all das kann in Trainingsdaten oder Logfiles außereuropäischer Anbieter landen.

Für CISOs ist das ein konkretes Compliance-Problem: Sowohl die DSGVO als auch NIS2 verlangen Nachweisbarkeit darüber, wo und wie geschäftskritische Daten verarbeitet werden. Eine öffentliche KI-Schnittstelle ohne definierten Verarbeitungsort erschwert genau das.

Ein Markt im geopolitischen Spannungsfeld

Die Dringlichkeit speist sich nicht allein aus der Technik, sondern aus der weltpolitischen Lage. Diskussionen um den US CLOUD Act und um mögliche regulatorische Eingriffe in die Nutzung außereuropäischer Plattformen haben das Risikobewusstsein in den Chefetagen spürbar erhöht. Wo vor zwei Jahren noch die Kosten pro API-Aufruf im Vordergrund standen, fragen Sicherheitsabteilungen heute zuerst nach dem Verarbeitungsort und der vertraglichen Absicherung im Krisenfall.

Private LLMs als Antwort auf das Kontrollproblem

Der Ausweg liegt nicht darin, auf die Produktivitätsgewinne generativer KI zu verzichten, sondern die Infrastruktur dahinter neu zu denken. Private oder auf europäischen Cloud-Umgebungen betriebene Sprachmodelle ermöglichen dieselben Funktionen, ohne dass Prompts oder Trainingsdaten das Unternehmen verlassen. Open-Weight-Modelle, die sich vollständig on-premises oder in einer souveränen Cloud betreiben lassen, gewinnen deshalb an Bedeutung – nicht als Statement gegen US-Anbieter, sondern als pragmatische Antwort auf ein reales Kontrollbedürfnis.

Drei Architektur-Fragen, die über Sicherheit entscheiden

- Erstens: Wo genau werden Modelle gehostet und wo läuft die Inferenz?

> „ Open-Weight-Modelle, die sich vollständig on-premises oder in einer souveränen Cloud betreiben lassen, gewinnen an Bedeutung – nicht als Statement gegen US-Anbieter, sondern als **pragmatische Antwort auf ein reales Kontrollbedürfnis.**
>
> *Heiner Sieger*

DER AUTOR
Heiner Sieger
ist Chefredakteur der Fachmagazine DIGITAL BUSINESS und e-commerce Magazin.

- Zweitens: Fließen Prompts oder Ergebnisse in das Training zukünftiger, öffentlicher Modellversionen ein?
- Drittens: Lässt sich der gesamte Datenfluss lückenlos dokumentieren, um im Audit-Fall Rechenschaft abzulegen? Nur wenn alle drei Fragen mit einem klaren „Ja, das wissen wir" beantwortet werden können, ist eine KI-Architektur tatsächlich auditfähig.

Erklärbarkeit wird zum Sicherheitsmerkmal

Neben der reinen Datenhoheit rückt eine zweite Dimension in den Fokus: Nachvollziehbarkeit. Wenn KI-Systeme zunehmend in geschäftskritische Entscheidungsprozesse eingebunden werden, reicht eine funktionierende Blackbox nicht mehr aus.

Der EU AI Act verlangt für bestimmte Risikoklassen explizit dokumentierte, nachvollziehbare Entscheidungswege. Private LLM-Architekturen mit überprüfbarer Modell-Governance erfüllen regulatorische Anforderungen und schaffen gleichzeitig internes Vertrauen in KI-gestützte Prozesse – ein Faktor, der über die Akzeptanz in der Belegschaft entscheidet.

Die Kostenfrage neu gedacht

Ein häufiges Gegenargument lautet, private oder europäische KI-Infrastruktur sei teurer als Hyperscaler-Angebote. Diese Rechnung greift zu kurz, wenn Folgekosten unberücksichtigt bleiben: Bei sensiblen Anwendungsfällen addieren sich zu den Rechenkosten Aufwände für Rechtsprüfung, Auftragsverarbeitungsverträge, Audit-Dokumentation und im Zweifel Bußgeldrisiken bei Verstößen gegen Datenschutz- oder Sektorregulierung. Wer diese Gesamtkosten realistisch einpreist, kommt bei geschäftskritischen Anwendungen oft zu einem anderen Ergebnis als beim reinen Preisvergleich pro Rechenoperation.

Der pragmatische Einstieg

Wie bei jeder größeren IT-Transformation empfiehlt sich kein radikaler Wechsel, sondern ein schrittweises Vorgehen: Zunächst sollten Unternehmen inventarisieren, welche KI-Tools im Alltag bereits informell genutzt werden – häufig eine ernüchternde Bestandsaufnahme. Darauf aufbauend lässt sich festlegen, welche Anwendungsfälle, etwa interne Wissenssuche, Dokumentenanalyse oder Code-Unterstützung, sich in eine kontrollierte, private Umgebung überführen lassen. Kritische Anwendungsfälle mit Zugriff auf besonders sensible Daten – etwa Personalakten oder Forschungsergebnisse – sollten dabei oberste Priorität erhalten, während unkritische Standardanwendungen zunächst in bestehenden Prozessen verbleiben können.

Am Ende steht eine einfache Erkenntnis: Digitale Souveränität bei generativer KI ist kein Verzicht auf Innovation, sondern deren Voraussetzung. Nur wer die Kontrolle über seine Daten behält, kann KI langfristig und rechtssicher in die eigenen Geschäftsprozesse integrieren – statt sich von der nächsten Änderung fremder Nutzungsbedingungen überraschen zu lassen. •

Der Beitrag wurde mit Unterstützung unserer AI-Agenten erstellt

SBOM: Warum Sichtbarkeit allein nicht schützt

Millionen fließen in Open-Source-Software, doch niemand kennt wirklich alle Bausteine im eigenen Code. Dieser Beitrag zeigt, wo das Risiko für Softwareanwendungen in Unternehmen entsteht. /// von Tal Zarfati

DAS GRÖSSTE RISIKO STECKT SELTEN IM EIGENEN CODE, sondern in fremden Komponenten, die niemand vollständig im Blick hat. Moderne Anwendungen bestehen zu großen Teilen aus Open-Source-Bibliotheken und Bausteinen von Drittanbietern. Hinter jeder direkten Abhängigkeit stecken oft Dutzende weitere, die niemand bewusst ausgewählt hat. Eine Anwendung ist nur so sicher wie ihre schwächste Komponente. Wer nicht weiß, was im eigenen Code steckt, kann Risiken weder erkennen noch beheben.

Software Bill of Materials als Fundament

Transparenz beginnt mit einer vollständigen Software-Stückliste, der Software Bill of Materials. Eine SBOM listet jede Komponente auf, samt Version, Herkunft und Abhängigkeiten. Entscheidend ist nicht die Liste selbst, sondern wann sie entsteht. Manuell gepflegte Listen veralten mit dem nächsten Build. Erst eine automatisierte und über den gesamten Lebenszyklus erzeugte SBOM zeigt den tatsächlichen Zustand der Software. Bricht eine neue Schwachstelle auf, lässt sich in Minuten beantworten, ob und wo sie in der Softwarelandschaft steckt. Sichtbarkeit allein schützt niemanden. Sie wirkt erst, wenn Entwickler eine Schwachstelle früh sehen, direkt im eigenen Workflow. Developer-First-Security verlegt die Prüfung dorthin, statt sie ans Ende zu schieben. Ein Fund im Build kostet Minuten, in der Produktion Tage. So verkürzt sich die Zeit zwischen Entdeckung und Behebung, bevor aus einer Lücke ein Vorfall wird. Wird dieser Schritt automatisiert und nachprüfbar, entsteht eine „Self-Healing Software Supply Chain“, eine Lieferkette, die erkannte Risiken selbst schließt.

Vier Kriterien für echte Transparenz

Damit Transparenz mehr ist als nur ein Bericht, muss sie vier Bedingungen erfüllen, die ihre Wirkung erst im Zusammenspiel entfalten.

Integrität: Eine Behebung darf den Build nicht brechen, sonst schalten Teams die Automatisierung nach dem ersten Fehlschlag wieder ab.

Reichweite: Ein Fix muss die Schwachstelle im gesamten Bestand schließen, nicht nur in einem einzelnen Repository, während dieselbe Komponente an anderer Stelle verwundbar bleibt.

Relevanz: Die Automatisierung muss sich auf erreichbaren und ausnutzbaren Code konzentrieren, da Teams sonst von einer Flut irrelevanter Schwachstellen-Warnungen überrollt werden.

Nachweis: Jede Änderung braucht einen signierten, kryptografischen Beleg, der zeigt, was sich wann und warum geändert hat.

SBOM-Echtzeit-Transparenz als Zustand

Einzeln erfüllt kein Werkzeug alle vier Kriterien zugleich. Genau daran scheitern die meisten Setups. Ein Tool scannt, ein zweites priorisiert, ein drittes behebt, jedes mit eigenem Datenstand und eigenem Takt. An den Nahtstellen dazwischen geht die Übersicht verloren, und genau dort bleibt das Risiko unbemerkt. SBOM-Echtzeit-Transparenz bündelt Erkennung, Priorisierung und Behebung dort, wo die Artefakte ohnehin durchlaufen. So schließt sich die Lücke, die verteilte Werkzeuge offenlassen. Transparenz in der Software-Lieferkette ist kein Bericht am Jahresende, sondern ein durchgängiger Zustand. Wer die Lücke zwischen Sichtbarkeit und Behebung ignoriert, verliert Zeit und Kapital. •

> „ Echtzeit-Transparenz bei SBOM **bündelt Erkennung, Priorisierung und Behebung** dort, wo die Artefakte ohnehin durchlaufen. So schließt sich die Lücke, die verteilte Werkzeuge offenlassen.
>
> *Tal Zarfati*

DER AUTOR
Tal Zarfati
ist Vice President, Chief Architect of AppSec bei JFrog.
Bild: JFrog


TRUST
THE T
Souveräne Cloud, AI
und Security-Lösungen
für jedes Business.
Für mehr Infos
hier scannen.
AI

SECURITY AGENDA 2027

Der Strategie-Check für das neue Geschäftsjahr:
Von den Lehren des KI-Wettlaufs zur resilienten Budgetplanung – was jetzt auf die Prioritätenliste für den Vorstand gehört. /// von Heiner Sieger

EIN JAHR VOLLER UNTERNEHMENSKRITISCHER WETTLÄUFE LIEGT SCHON BALD WIEDER HINTER UNS – UND DIESE AUSGABE ZEIGT: Der permanente Kampf zwischen „Hase" (Angreifer) und „Igel" (Verteidiger) entscheidet sich nicht mehr an einer einzelnen Firewall, sondern an der Summe vieler kluger Einzelentscheidungen. Für die Budgetplanung 2027 bedeutet das: Wer als Unternehmen nur nachrüstet, verliert. Wer priorisiert, gewinnt. Diese Themen gehören auf die Sicherheitsagenda:

Vom Compliance-Zwang zum Wettbewerbsvorteil
NIS2 und der EU AI Act sind 2026 endgültig in der Unternehmensrealität angekommen. Wie die Titelstrecke gezeigt hat, wird ein integriertes Managementsystem zum Rückgrat der Resilienz – nicht als Pflichtübung, sondern als Steuerungsinstrument, das Audit-Sicherheit und operative Exzellenz miteinander verbindet. Externe Zertifizierungen fungieren dabei zunehmend als Vertrauensanker gegenüber Kunden, Partnern und Aufsichtsbehörden gleichermaßen.

Vom Werkzeugkasten zur Plattform
Die Analysen zu XDR, Managed SOC und autonomer Abwehr haben deutlich gemacht: Einzellösungen erzeugen mehr Alarmflut als Sicherheit. Der Effizienzgewinn entsteht nicht durch mehr Tools, sondern durch deren intelligente Korrelation – ergänzt durch ein externes SOC dort, wo eigenes Personal rund um die Uhr schlicht nicht verfügbar ist. 2027 entscheidet sich, welche Unternehmen den Sprung von der Tool-Sammlung zur konsolidierten Plattform schaffen, und welche im Datenrauschen untergehen.

Der Fachkräftemangel bleibt der stille Verstärker jedes Angriffs
Es reicht nicht, mehr Budget in Werkzeuge zu stecken, wenn niemand da ist, der die Ergebnisse interpretiert. Automatisierung und externe Security-Teams schließen diese Lücke nicht als Notlösung, sondern als strukturelle Antwort auf einen Arbeitsmarkt, der sich kurzfristig nicht ändern wird.

Von der Identität zur Vertrauensarchitektur
Deepfakes und KI-gestütztes Social Engineering definieren die Angriffsfläche Mensch neu. Verhaltensbiometrie und Zero-Trust-Prinzipien sind keine Kür mehr, sondern Grundvoraussetzung, um Identitäten in einer Welt synthetischer Stimmen und Gesichter zu schützen. Der Weg dorthin verläuft schrittweise – von Legacy-Systemen zu einer lückenlosen „Never Trust, Always Verify"-Architektur, ohne den laufenden Betrieb zu gefährden.

Von der Abhängigkeit zur Souveränität
Ob Cloud-Infrastruktur, Rechenzentrum oder Sprachmodell – der Wunsch nach Kontrolle über die eigenen Daten wurde 2026 zum handfesten Wirtschaftsfaktor. Die Diskussion um Exit-Fähigkeit, Kill-Switch-Risiken und private KI-Architekturen zeigt: Wer 2027 noch blind auf externe Blackboxes vertraut, geht ein Risiko ein, das sich kaum noch versichern lässt. Souveränität entsteht dabei nicht über Nacht, sondern über einen strukturierten Einstieg, etwa beginnend bei einer unabhängigen Disaster-Recovery-Umgebung.

Von der Blackbox zur erklärbaren KI
Agentic AI hält rasant Einzug in den Unternehmensalltag – und mit ihr die Frage, welche Zugriffsrechte ein Agent

tatsächlich benötigt. Read-only-Architekturen und eine konsequente Trennung von Analyse- und Änderungsfunktionen zeigen, dass sich produktive Anwendungsfälle auch ohne umfassende Systemrechte realisieren lassen.

Von der Lieferkette zum Gesamtrisiko

Die Sicherheit eines Unternehmens endet nicht an der eigenen Firewall, sondern reicht bis in jede eingebundene Softwarekomponente und jeden Zulieferer hinein.

Von der Reaktion zur Prävention

Unsere Vision 2030 hat es mit Zahlen belegt: Mehr als 50 Prozent der globalen Sicherheitsbudgets fließen bis zum Ende des Jahrzehnts in präventive statt reaktive Maßnahmen, während Unternehmen mit selbstheilenden Architekturen bereits heute bis zu 70 Prozent weniger Ransomware-Vorfälle verzeichnen.

Keines dieser Themen lässt sich isoliert lösen. Sie greifen ineinander, wie es der Wettlauf zwischen Hase und Igel in diesem Heft immer wieder gezeigt hat: Wer nur einzelne Punkte abarbeitet, verschiebt das Risiko lediglich an eine andere Stelle der Angriffsfläche, statt es tatsächlich zu verringern.

Sicherheit wird damit endgültig zur Vorstandsaufgabe, nicht zur Detailfrage der IT-Abteilung. Wer Budgets für 2027 verantwortet, muss nachvollziehen können, welches Risiko mit welcher Investition tatsächlich reduziert wird – nicht auf Basis von Bauchgefühl, sondern anhand nachvollziehbarer Kennzahlen wie Reaktionszeit, Wiederherstellungsdauer und Auditfähigkeit.

Die begleitende Checkliste verdichtet die zentralen Lehren aus allen Kapiteln dieser Ausgabe zu einer konkreten Agenda. •

WAS 2027 AUF DIE SECURITY-AGENDA GEHÖRT

Zehn Prioritäten für die Budgetplanung im neuen Geschäftsjahr

1
NIS2-Reifegrad prüfen – Ist die Compliance dokumentiert oder nur behauptet?

2
IMS als Steuerungstool etablieren – Governance und operative Sicherheit zusammenführen statt trennen.

3
Tool-Konsolidierung vorantreiben – XDR-Plattformen statt Einzellösungen gegen die Alarmflut.

4
Managed Detection einkalkulieren – 24/7-Abdeckung einplanen, wo eigenes Personal fehlt.

5
Identitätsschutz modernisieren – Verhaltensbiometrie gegen Deepfake-Betrug einplanen.

6
Zero-Trust-Reife erhöhen – Legacy-Systeme schrittweise in „Never Trust"-Architekturen überführen.

7
Exit-Fähigkeit testen – Cloud- und Anbieterwechsel im Ernstfall realistisch durchspielen.

8
KI-Agenten-Rechte begrenzen – Read-only-Prinzipien für Agentic AI konsequent umsetzen.

9
Lieferkette transparent machen – SBOM-Prozesse für Software-Komponenten einführen.

10
Cyber-Risiko finanziell absichern – Versicherung als Teil des Incident-Response-Plans verstehen.

Vision 2023: Das autonome Immunsystem

Der digitale Schutzwall von heute wird zum lebenden Organismus von morgen. Während Angreifer KI nutzen, um Schwachstellen in Rekordzeit zu finden, entwickelt sich die Abwehr zu einem selbstheilenden System, das Bedrohungen erkennt, bevor sie Schaden anrichten. Ein Blick auf die Zahlen, die diesen Wandel bereits heute belegen.

/// von Heiner Sieger

DIE IT-SICHERHEIT STEHT VOR IHRER GRÖSSTEN TRANSFORMATION SEIT DER ERFINDUNG DER FIREWALL. Was noch vor wenigen Jahren als Zukunftsmusik galt, wird bis 2030 zur betriebswirtschaftlichen Realität: der Wandel von der reaktiven Verteidigung zum autonomen, selbstheilenden Immunsystem.

Der Paradigmenwechsel ist bereits eingeleitet. Noch 2024 flossen über 95 Prozent der globalen IT-Security-Budgets in reaktive Maßnahmen – Systeme, die erst nach einem Angriff reagieren. Bis 2030 kehrt sich dieses Verhältnis um: Mehr als die Hälfte der Investitionen fließt dann in präventive Technologien, die Bedrohungen erkennen, bevor sie überhaupt wirksam werden.

Der Markt folgt dieser Logik in atemberaubendem Tempo. Die Ausgaben für KI-gestützte Sicherheitslösungen wachsen von 10 Milliarden US-Dollar (2024) auf über 204 Milliarden US-Dollar im Jahr 2030. Parallel entsteht ein völlig neues Segment: die Absicherung der KI-Systeme selbst, die bis 2030 einen Markt von 16,4 Milliarden US-Dollar erreicht – ein Beleg dafür, dass künstliche Intelligenz nicht nur Werkzeug, sondern auch Schutzobjekt wird.

Die Rolle des Menschen verändert sich grundlegend. Während 2026 noch weniger als ein Prozent der Unternehmen autonome Security-Agenten ganz ohne menschliche Aufsicht betreiben, wächst dieser Anteil bis 2029 auf zehn Prozent. Der CISO wird dabei nicht überflüssig – er wird zum Kurator, der die ethischen und strategischen Leitplanken für ein System definiert, das operativ längst eigenständig agiert.

Der Beweis liegt in den Ergebnissen. Unternehmen, die auf sogenannte „immutable workspaces" setzen – unveränderliche, KI-geschützte Arbeitsumgebungen – verzeichnen bis zu 70 Prozent weniger Ransomware-Vorfälle. Angesichts von über einer Million erwarteter Sicherheitslücken bis 2030 ist das mehr als ein Detail: Es ist der entscheidende Hebel im Wettlauf gegen automatisierte Angriffe. •

Der KI-Wettlauf, der sich durch dieses gesamte Heft zieht, findet hier sein vorläufiges Fazit.

Während der „Hase" auf Geschwindigkeit und Automatisierung setzt, gewinnt der „Igel" die Oberhand – nicht durch schnelleres Reagieren, sondern durch die Fähigkeit, sich selbst zu heilen, bevor der Schaden entsteht.

Der Beitrag wurde mit Unterstützung unseres KI-Assistenten erstellt

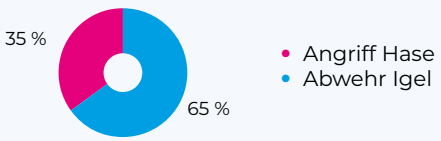
KI-WETTLAUF-CHECK

Autonome Angriffs-Bots durchsuchen Netzwerke – über 1 Mio. CVEs bis 2030 erwartet.

Selbstheilende Systeme senken Ransomware-Vorfälle um bis zu 70 Prozent.

Der Wettlauf 2030: Wer gewinnt?

KI-Wettlauf 2030 – Klarer Vorsprung Igel

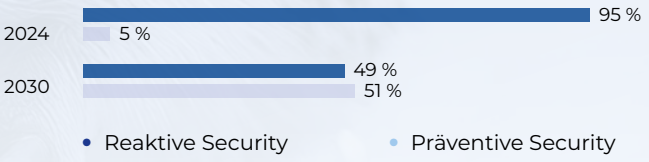


Angriff (Hase): Vollständig autonome Angriffs-Bots durchsuchen globale Netzwerke eigenständig nach neuen Schwachstellen – befeuert durch über 1 Million erwarteter Sicherheitslücken bis 2030.

Abwehr (Igel): Selbstheilende Systeme und autonome Security-Agenten schließen Lücken, bevor sie ausgenutzt werden können, und senken Ransomware-Vorfälle um bis zu 70 %.

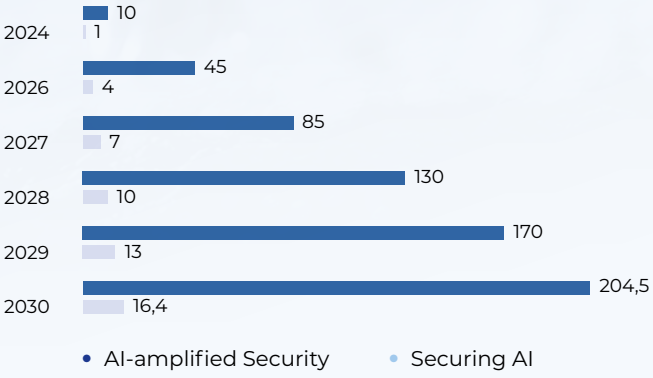
Der Paradigmenwechsel: Von Reaktion zu Prävention

Anteil an globalen IT-Security-Budgets (%)



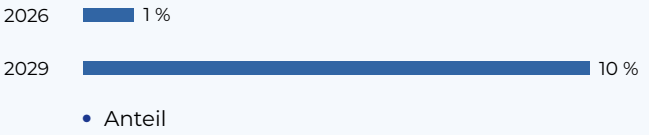
Der Markt: KI wird Waffe und Schutzgut zugleich

Marktwachstum bis 2030 (in Mrd. US-Dollar)



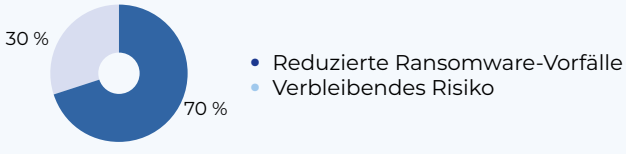
Die Autonomie: Der Mensch als Kurator

Unternehmen mit vollautonomen Security-Agenten ohne menschliche Aufsicht



Der Beweis: Weniger Schaden durch Resilienz

Wirkung von „Immutable Workspaces“ (2030)



IMPRESSUM

DIGITAL BUSINESS Magazin
www.digitalbusiness-magazin.de

HERAUSGEBER UND GESCHÄFTSFÜHRER
Matthias Bauer, Dennis Hirthammer

So erreichen Sie die Redaktion
Chefredaktion:
Heiner Sieger (v. i. S. d. P.), heiner.sieger@win-verlag.de
Tel.: +49 (89) 3866617-14
Redaktion:
Konstantin Pfliegl, konstantin.pfliegl@win-verlag.de
Tel. +49 (89) 3866617-18
Stefan Girschner, stefan.girschner@win-verlag.de
Tel.: +49 (89) 3866617-16

Mitarbeiter dieser Ausgabe:
Kathrin Beckert-Plewka, Dr. Yvonne Bernard, Matt Berzinski, Gerald Eid, Kay Ernst, Rijesh Haridas, Thomas Heinz, Marco Hoffmann, Dr. Stefan Killich, Michael Klatte, Aris Koios, Dr. Beverly McCann, Michael Locher-Tjoa, Reto Scagnetti, Roger Scheer, Peter Schill, Dr. Sebastian Schmerl, Moritz Schmidt, Andy Schneider, Christoph Schuhwerk, Stefan Tiefel, Leon Weise, Richard Werner, Tal Zarfati

Stellvertretende Gesamtanzeigenleitung
Bettina Prim, bettina.prim@win-verlag.de, Tel.: +49 (89) 3866617-23

Anzeigendisposition
Auftragsmanagement@win-verlag.de
Chris Kerler (089/3866617-32, Chris.Kerler@win-verlag.de)

Abonnentenservice und Vertrieb
Tel: +49 89 3866617 46
www.digitalbusiness-magazin.de/hilfe
oder eMail an
abovertrieb@win-verlag.de mit Betreff „www.digitalbusiness“
Gerne mit Angabe Ihrer Kundennummer vom Adressetikett

Artdirection/Titelgestaltung: DesignConcept Dagmar Friedrich-Heidbrink
Bildnachweis/Fotos: stock.adobe.com, Werkfotos

Druck:
Vogel Druck und Medienservice GmbH
Leibnizstraße 5
97204 Höchberg

Produktion und Herstellung
Jens Einloft, jens.einloft@vogel.de, Tel.: +49 (89) 3866617-36

Anschrift Anzeigen, Vertrieb und alle Verantwortlichen
WIN-Verlag GmbH & Co. KG
Chiemgaustr. 148, 81549 München
Telefon +49 (89) 3866617-0

Verlags- und Objektleitung
Martina Summer, martina.summer@win-verlag.de,
Tel.: +49 (89) 3866617-31, (anzeigenverantwortlich)

Zentrale Anlaufstelle für Fragen zur Produktsicherheit
Martina Summer (martina.summer@win-verlag.de, Tel.:089/3866617-31)

Bezugspreise
Einzelverkaufspreis: 11,50 Euro in D, A, CH und 13,70 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Jahresabonnement (6 Ausgaben): 69,00 Euro in D, A, CH und 82,20 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Vorzugspreis für Studenten, Schüler, Auszubildende und Wehrdienstleistende gegen Vorlage eines Nachweises auf Anfrage. Bezugspreise außerhalb der EU auf Anfrage.

30. Jahrgang; Erscheinungsweise: 6-mal jährlich

Einsendungen: Redaktionelle Beiträge werden gerne von der Redaktion entgegen genommen. Die Zustimmung zum Abdruck und zur Vervielfältigung wird vorausgesetzt. Gleichzeitig versichert der Verfasser, dass die Einsendungen frei von Rechten Dritter sind und nicht bereits an anderer Stelle zur Veröffentlichung oder gewerblicher Nutzung angeboten wurden. Honorare nach Vereinbarung. Mit der Erfüllung der Honorarvereinbarung ist die gesamte, technisch mögliche Verwertung der umfassenden Nutzungsrechte durch den Verlag – auch wiederholt und in Zusammenfassungen – abgegolten. Eine Haftung für die Richtigkeit der Veröffentlichung kann trotz Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden.

Sonderheft Security 2026
ISSN 2510-344X
Unsere Papiere sind PEFC zertifiziert
Wir drucken mit mineralölfreien Druckfarben

Außerdem erscheinen beim Verlag:
AUTOCAD Magazin, BAUEN AKTUELL, r.energy, DIGITAL ENGINEERING Magazin, DIGITAL MANUFACTURING, e-commerce Magazin, KGK Rubberpoint, PLASTVERARBEITER, PlastXnow

22. – 25. September 2026

SECURE YOUR BUSINESS

Die Leitmesse für Sicherheit

JETZT TICKET SICHERN!

SAVE THE DATE:
security essen 2028
19. – 22. September

security essen 26
the number one

www.security-essen.de

MESSE ESSEN