05/2025 /// WWW.DIGITALBUSINESS-MAGAZIN.DE

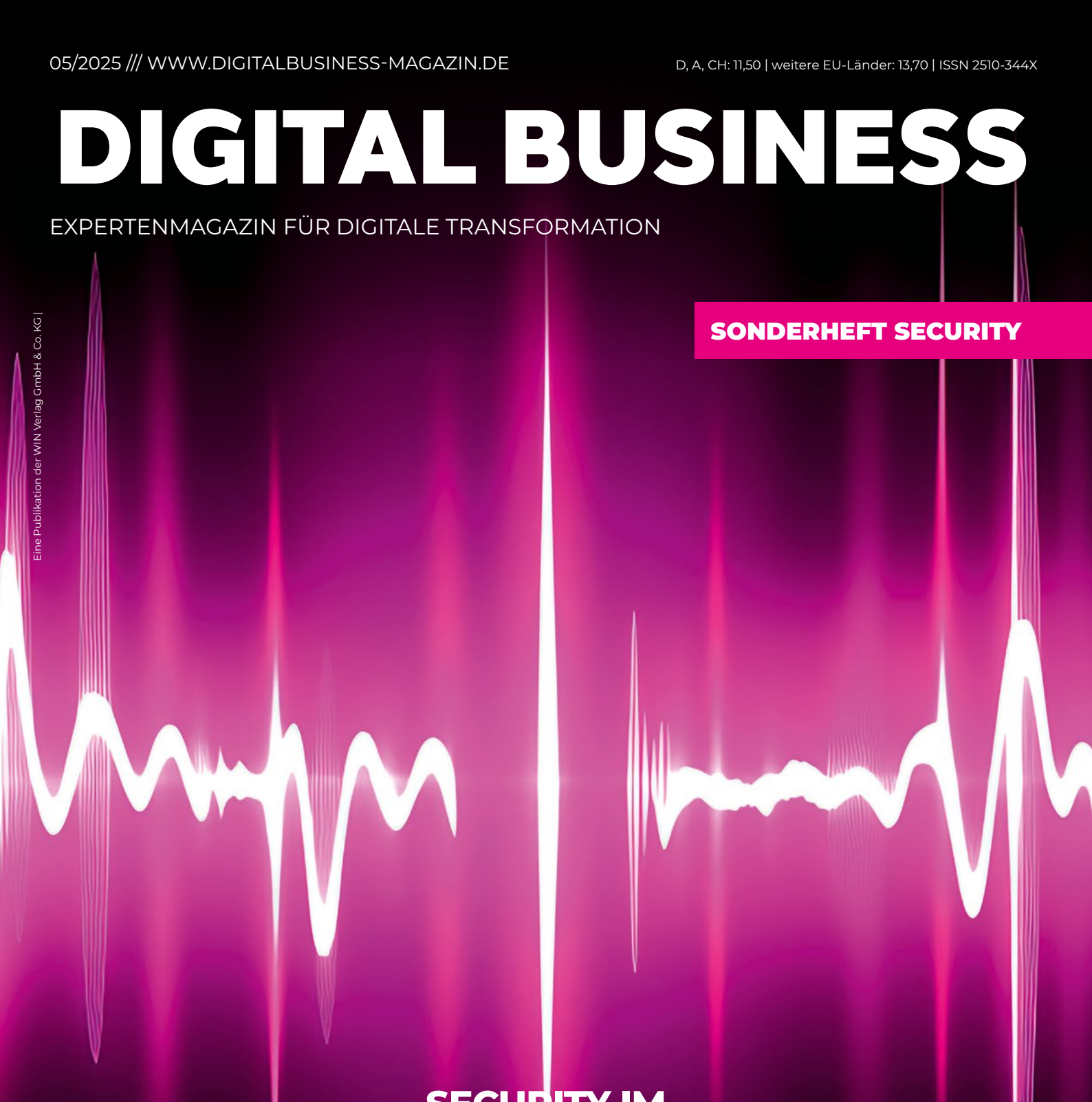
D, A, CH: 11,50 | weitere EU-Länder: 13,70 | ISSN 2510-344X

DIGITAL BUSINESS

EXPERTENMAGAZIN FÜR DIGITALE TRANSFORMATION

Eine Publikation der WIN Verlag GmbH & Co. KG |

SONDERHEFT SECURITY



SECURITY IM

DAUERSTRESS

TECHNOLOGISCHES WETTRENNEN UM DIE KI

KI IN DER IT-SECURITY

KI verändert die Bedrohungslage für Unternehmen massiv. Doch Schutz ist mit der richtigen Strategie möglich.

EXPERTEN-TALK

KI wird künftig entscheidend sein, um mit der nächsten Generation von Cyberbedrohungen Schritt zu halten.

IT-SECURITY-MESSE IT-SA

Interview mit dem Exhibition Director der it-sa über aktuelle Sicherheitstrends und die Vernetzung von KMU mit Konzernen.

WatchGuard

b.o.c. IT-SECURITY
Platinum Partner

Real Security for the Real World

- Network Security
- Endpoint Security
- Identity Security
- Threat Detection and Response
- Managed Services for MSP
- Unified Security Platform

Besuchen Sie uns auf der it-sa 2025 in Halle 7 – Stand 230

WatchGuard Technologies | watchguard.de | vertrieb@watchguard.com | +49 700 92229333

BOC IT-Security GmbH | boc.de | info@boc.de | +49 208 8596440

EDITORIAL

Liebe Leserin, lieber Leser

• **im Zeitalter der digitalen Transformation ist die IT-Sicherheit unerlässlich geworden**, um Unternehmen vor den immer raffinierteren Bedrohungen der Cyberwelt zu schützen. Eine der spannendsten technologischen Entwicklungen in diesem Bereich ist die künstliche Intelligenz. Sie hat das Potenzial, die IT-Sicherheitslandschaft dramatisch zu verändern. Doch KI bringt eine Dualität mit sich: Während sie den Verteidigern mächtige Werkzeuge an die Hand gibt, nutzen Angreifer dieselbe Technologie für ihre Zwecke.

Die Gefahr, die von KI in den Händen von Cyberkriminellen ausgeht, spüren die Unternehmen auch in der Praxis: So sind laut einer aktuellen Studie des TÜV Verbands 51 Prozent der Betriebe in Deutschland, die im vergangenen Jahr Opfer eines Cyberangriffs wurden, davon überzeugt, dass die Angreifer bei ihren Attacken auf KI setzten. Bei großen Unternehmen ab 250 Mitarbeiter sind es sogar 81 Prozent. Umso erstaunlicher ist es, dass lediglich jedes zehnte Unternehmen bereits selbst künstliche Intelligenz zur Abwehr von Angriffen nutzt.

In dieser Ausgabe unseres „Sonderhefts Security“ beleuchten wir unter anderem die zweischneidige Rolle der künstlichen Intelligenz in der IT-Sicherheit. Wir bieten Einblicke, wie Unternehmen die Chancen von KI in der Cyberabwehr nutzen, während sie gleichzeitig die Risiken minimieren. •

Ihr
KONSTANTIN PFLIEGL, Leitender Redakteur
DIGITAL BUSINESS

konstantin.pfliegl@win-verlag.de

IMPRESSUM

DIGITAL BUSINESS Magazin
www.digitalbusiness-magazin.de

HERAUSGEBER UND GESCHÄFTSFÜHRER
Matthias Bauer, Günter Schürger

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:
Tim Berghoff, Martin Ennenbach, Carsten Ettmann, Bernd Forstner, Thimo Holst, Dr. Martin Krämer, Christoph Lipps, Dr. Jens-Uwe Meyer, Paul Moll, Frank Morgner, Alexander Opel, Hermann Ramacher, Kathrin Redlich, Mike Rennie, Dave Russel, Andre Schindler, Dr. Sebastian Schmerl, Frank Schwaak, Thomas Schumacher, Dr. Jens-Uwe Meyer, Stefan Tiefel, Richard Werner

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)

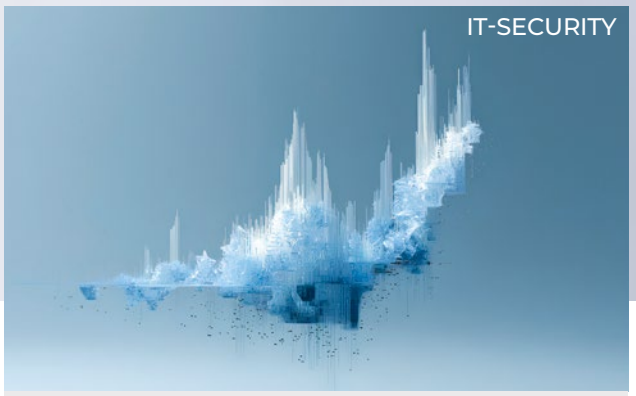
Bezugspreise
Einzelverkaufspreis: 11,50 Euro in D, A, CH und 13,70 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Jahresabonnement (6 Ausgaben): 69,00 Euro in D, A, CH und 82,20 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Vorzugspreis für Studenten, Schüler, Auszubildende und Wehrdienstleistende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

29. 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.

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



IT-SECURITY

DIGITAL BUSINESS

05 2025
Sonderheft Security

Steigende Cyberbedrohungen: Die Rolle von KI in der modernen IT-Security

Christoph Lipps vom Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) erklärt im Interview, wie sich die Bedrohungslage durch künstliche Intelligenz konkret verändert, wie fortschrittliche Sicherheitstechnologien von morgen aussehen und inwieweit KI schon in der Lage ist, komplexe Sicherheitsvorfälle eigenständig zu managen. /// von Konstantin Pfliegl

In Zeiten der steigenden Digitalisierung spielt IT-Security eine zentrale Rolle. Unternehmen weltweit stehen vor der Herausforderung, ihre digitalen Infrastrukturen vor immer raffinierteren Angriffen zu schützen. Künstliche Intelligenz (KI) hat sich hierbei als ein entscheidender Verbündeter erwiesen: Mit ihrer Fähigkeit, große Datenmengen in Echtzeit zu analysieren, Anomalien zu identifizieren und proaktive Schutzmaßnahmen vorzuschlagen, hat KI das Potenzial, die Sicherheitsarchitektur in Unternehmen grundlegend zu transformieren.

Doch wie hat sich Bedrohungslage durch künstliche Intelligenz konkret verändert? Wie sehen fortschrittliche KI-gestützte Sicherheitstechnologien von morgen aus? Und inwieweit ist KI schon in der Lage, komplexe Sicherheitsvorfälle eigenständig zu managen?

DIGITAL BUSINESS spricht darüber mit Christoph Lipps, Team Lead Cyber Resilience & Security beim Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI).

Herr Lipps, blicken wir zu Beginn auf den Status quo in der IT-Security: Wie hat sich die Bedrohungslage für Unternehmen in den letzten Jahren entwickelt, insbesondere im Hinblick auf KI-gestützte Angriffe?
Christoph Lipps | Zunächst kurz zur Einordnung, in welcher Umgebung wir uns aus meiner Sicht bewegen. Für die Unternehmen gilt, was auch wir in unserem täglichen Leben zunehmend spüren: Unsere Welt wird immer vernetzter. Das wird beispielsweise auch ganz aktuell vom Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) in der Leitinitiative Hyperkonnektivität aufgegriffen. Zudem wird davon ausgegangen, dass wir Ende 2025 weltweit fast 20 Milliarden vernetzte IoT-Geräte haben werden – Tendenz steigend. Diese Entwicklung ist natürlich nicht ganz neu und wurde, unter anderem vom DFKI, bereits im „Nationalen Referenzprojekt zur IT-Sicherheit in der Industrie 4.0“ erforscht.

Was sich aus meiner Sicht also verändert hat sind die Art und Wertigkeit der verarbeiteten und übertragenen Informationen, die Verfügbarkeit von Methoden der KI und die Leistungsfähigkeit dieser Methoden: Große Mengen von Daten automatisiert und strukturiert zu untersuchen und dabei auch Schwachstellen von Systemen zu finden und diese letztendlich zu benutzen.

Welche Rolle spielt KI bei der Erkennung und Abwehr von Cyberangriffen heutzutage? Geht es ohne KI überhaupt noch?
CL | Dabei bewegen wir uns natürlich auch in ethische oder philosophische Bereiche, vor allem mit der zweiten Frage. Ich beginne Mal mit dem zweiten Teil und hole dabei etwas aus. Für mich spielt das auch im Bereich der Industrie 4.0

DER GESPRÄCHSPARTNER
Christoph Lipps
ist Senior Researcher beim Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) in Kaiserslautern und leitet dort in der Forschungsgruppe Intelligente Netze das Team für Cyber Resilience & Security.
Bild: DFKI

„ Die Gefahr der **Manipulation von KI-Systemen ist eine sehr reale Bedrohung**, Stichwort Data Poisoning.“ *Christoph Lipps*

und der Frage, wird die Technologie den Menschen ablösen, eine Rolle. Etwa seit dem Jahr 1800 und der ersten sogenannten industriellen Revolution über Massenproduktion und Elektrifizierung um 1900, der Automatisierung und Elektronik in den 2000er bis hin zu den Cyber-physischen Systemen in den 2010er-Jahren gab es immer wieder die Frage, ob wir uns Menschen in dieser Kette noch brauchen. Hierzu habe ich eine klare Meinung: Ja, wir brauchen ihn.

Alle diese technologischen Entwicklungen haben immer dazu beigetragen das Leben und die Arbeitsbedingungen für uns Menschen einfacher zu machen. So sollten wir auch die Verwendung der Methoden der künstlichen Intelligenz sehen, als Werkzeug und als sinnvolle Ergänzung. Gemeinsam, als Kombination aus menschlichen Fähigkeiten und den Methoden der künstlichen Intelligenz können wir resiliente, sichere und zukunftsfähige Infrastrukturen erstellen.

Also ist künstliche Intelligenz heute fester Bestandteil der IT-Security?
CL | Die KI spielt natürlich eine zunehmend relevante Rolle. Wie bereits angesprochen, können die Methoden große Datenmengen sehr schnell analysieren und dabei auch komplexe Muster erkennen, welche für Menschen nur schwer bis gar nicht zu erkennen sind. Ich nehme immer sehr gerne Bezug auf den Cyber Resilience Lifecycle (Identify – Protect – Detect – Respond – Recover). In allen diesen Bereichen können die Methoden der künstlichen Intelligenz einen entsprechenden Beitrag leisten – neben der Erkennung beispielsweise vor allem auch bei der automatisierten Einleitung von Eindämmungs- und Gegenmaßnahmen.

Können Sie einige KI-gestützte Sicherheitstechnologien vorstellen, die derzeit im Einsatz sind?
CL | Diese liegen sicherlich im Bereich der Erkennung von Anomalien, insbesondere bei der Erkennung von sogenannten Zero-Day Angriffen. Aber auch bei den oben angesprochenen automatisierten Reaktionsdiensten gibt es aktuell relevante Werkzeuge, die auch kommerziell verfügbar sind.

Da ich nun aber eher aus der Forschung komme, sind für mich die Möglichkeiten der KI in der Sicherheitsforschung und -entwicklung etwas spannender. Neben dem aktuell viel diskutierten Ansätzen der Post-Quantum Cryptography (KI-Unterstützung bei der Seitenkanalanalyse, der Bewertung der Sicherheit und allgemein der Unterstützung und Optimierung der Algorithmik) ist ein spannender Ansatz sicherlich alles, was im Bereich von Zero-Trust -Modellen passiert, also dem „Vertraue niemandem – überprüfe alles“ -Gedanken.

Hier werden die Methoden der KI vor allem bei der kontinuierlichen Analyse von Gerätezustand, dem Verhalten von Nutzern und Standorten (also auch im Bereich der Detektion von Anomalien), aber auch bei der automatisierten Reaktion verwendet.

Inwieweit ist denn KI heutzutage schon in der Lage, komplexe Sicherheitsvorfälle eigenständig zu managen?
CL | Das passiert schon sehr gut. Es gibt viele Beispiele, in welchen die Methoden der künstlichen Intelligenz schon integriert sind, auch im kommerziellen Bereich. Aber vor allem im Bereich des (teil-)autonomen Network- und Traffic-Monitoring ist schon sehr viel im Einsatz.

Mit der KI in der Cybersecurity ist es wie ein Wettrennen: Sowohl Angreifer als auch Security-Tools setzen auf KI und versuchen, immer einen Schritt voraus zu sein. Was meinen Sie, besteht die Gefahr, dass KI-Systeme selbst von Cyberkriminellen manipuliert werden können?
CL | Absolut. Da ich selbst seit vielen Jahren Fußball spiele, verwende ich hier immer gerne das Bild der Stürmers und des Verteidigers. Der Stürmer (Angreifer) hat einen gewissen Vorteil in seinen Aktionen, er kann aktiv auf den Ball zugehen und hat wenige Sekundenbruchteile Vorsprung vor dem Verteidiger, der in der Regal auf die Aktionen reagieren muss.

Wieso enden dann aber nicht alle Spiele mit sehr hohen Ergebnissen? Naja, ein Verteidiger hat natürlich selbst auch unterschiedliche Fähigkeiten. Er konnte beispielsweise im Verlauf des Spieles oder in vorangegangenen Spielen das Verhalten des Angreifers beobachten und kann sich auf die Aktionen vorbereiten. Zudem hilft ihm seine Erfahrung, bestimmte Muster, die ein Angreifer eben immer macht, zu erkennen und zu antizipieren und dann eben vielleicht selbst den berühmten Schritt schneller zu sein.

Für beide Seiten gilt, vieles kommt durch das entsprechende Training, wie eben bei den KI-Modellen auch. Aber auch bei diesem Training können die Methoden der künstlichen Intelligenz unterstützen, beispielsweise in Form von Generative Adversarial Networks (GANs), welche zur Verbesserung – und eben als Trainingspartner – verwendet werden, also Generator versus Discriminator.

Das klingt nach einer realen Bedrohung…
CL | Die Gefahr der Manipulation von KI-Systemen ist eine sehr reale Bedrohung, Stichwort Data Poisoning. Es muss klar sein, auf welcher Basis welche Schlüsse gezogen wurden und in welchem Zustand die Daten waren und ob diese Trainingsdaten integer sind.

Hier werden wir in den kommenden Jahren noch einiges von „KI“ sehen, welche basierend auf fehlerhaften oder bewusst manipulierten Daten falsche Ergebnisse liefert.•

MEHR ERFAHREN
Lesen Sie das ausführliche Interview mit Christoph Lipps auf der Webseite von DIGITAL BUSINESS.

KI als Brandbeschleuniger: Wie Unternehmen resilient werden

Die Zahl der Cyberangriffe steigt rasant – und KI macht Täter schneller, präziser, gefährlicher. Accenture-Sicherheitschef Thomas Schumacher* erklärt, was deutsche Unternehmen jetzt tun müssen, um widerstandsfähig zu werden. /// von Heiner Sieger

Herr Schumacher, wie verändert KI die Bedrohungslage – speziell für deutsche Unternehmen?
Thomas Schumacher | Wir beobachten einen exponentiellen Anstieg von Cyberattacken: plus 75 Prozent im Jahresvergleich. Diese werden nicht nur häufiger, sondern auch wesentlich raffinierter ausgeführt. Der Einsatz vonKI macht die Angriffe schneller, präziser und vor allem individueller. So genannte Ransomware, also Schadsoftware, mit der sich Eindringende sich Zugriff auf Daten und IT-Landschaft verschaffen, bleibt zum Beispiel in der verarbeitenden Industrie besonders wirksam. Zusätzlich sehen wir verstärkten Druck auf Forschungseinrichtungen und Behörden. Mittels KI lassen sich regelrechte Fallen bauen. Personalisiert auf geschäftliche Rollen, Prozesse und Timing- vom Bewerbungsumfeld bis zur Finanzabteilung – was die Erfolgsquote nochmals erhöht. KI erleichtert zudem Deepfakes und Identitätsbetrug – bis hin zu erfundenen „Mitarbeitenden".

Welche Learnings lassen sich aus Ihrer Studie ableiten – global und für Deutschland?
TS | Die Datengrundlage des State of Cybersecurity Reports ist breit und international. Global zählen rund zehn Prozent der Unternehmen zur „Reinvention Ready Zone", in Deutschland sind es lediglich acht Prozent. Laut der Accenture Studie „Cyberresilienter CEO" unterschätzen viele CEOs Cybersicherheit noch immer. 44 Prozent sehen sie nur als punktuelle Maßnahme statt als dauerhafte Managementaufgabe. Und über die Hälfte glaubt, dass Prävention teurer ist als ein Angriff – dabei zeigen die Zahlen von Bitkom klar das Gegenteil: Neun Milliarden Euro Investitionen stehen 148 Milliarden Euro Schaden gegenüber.

Warum ist Deutschland diesbezüglich im Rückstand?
TS | Die Adoptionsgeschwindigkeit neuer Technologien ist häufig geringer. Das sah man bei Cloud, das wiederholt sich bei KI. US-Unternehmen investieren früher, schneller und breiter. Dieses Muster überträgt sich auf Security: Wer generell zügiger innoviert, verankert Security eher als Querschnittsaufgabe – inklusive Budget, Governance und Durchsetzungskraft auf Vorstandsebene.

Sie sprechen von der Reinvention Ready Zone. Was kennzeichnet die Vorreiter in diesem Bereich?
TS | Sie begreifen Sicherheit als Business-Enabler, nicht als Kostenstelle. Sicherheit ist von Beginn an mitgedacht, sowie in Produkte, Services und Prozesse integriert. Diese Unternehmen haben ihre Basisdisziplinen – Netzwerk-, Cloud- und Identitätssicherheit sowie Awareness – systematisch ausgebaut. Das ist wie im Fußball: Ein Weltklasse-Sturm nützt wenig, wenn die Abwehr offen ist. Auf einem starken Fundament lässt sich KI in der Abwehr wirkungsvoll einsetzen.

Wo hakt es in Deutschland am häufigsten?
TS | An konsequenten Basics. Wer elementare Schutzmaßnahmen nicht beherrscht, kann mit KI-gestützter Verteidigung keine Wunder erwarten. Hinzu kommt die Lieferkette: Sicherheit endet nicht an der Werkstür. Es braucht eine klare Governance über das eigene Unternehmen hinaus, sonst reißen Partner und Dienstleister Sicherheitslücken auf – mit unmittelbaren Geschäftsrisiken.

Welche strukturellen und technischen Schritte sind jetzt entscheidend?

DER GESPRÄCHSPARTNER
Thomas Schumacher
ist Managing Director und Leiter von Accenture Security in Deutschland, Österreich und der Schweiz. Er verantwortet den Ausbau der Cybersecurity-Services, unter anderem Managed Security bis hin zu SOC-Services.

TS | Zuerst das klare Commitment der Führung und eine verankerte Strategie: Security-by-Design, eindeutige Verantwortlichkeiten, durchgängige Policies. Technisch gilt „Fix the Basics“: Dazu zählen Hardening, Segmentierung, Patch- und Schwachstellenmanagement, starke Identitäten und nicht zuletzt kontinuierliches Monitoring. Darauf baut eine Reifegrad-Roadmap auf, die Erkennung, Reaktion und Wiederanlauf beschleunigt – zunehmend mit KI-Unterstützung.

Wie bewerten Sie den Einsatz US-amerikanischer oder chinesischer KI aus Sicherheitssicht?
TS | Unternehmen brauchen eine Souveränitätsstrategie: Welche Workloads laufen wo, mit welchen Daten, unter welchen Rechtsrahmen? US-Hyperscaler sind kaum zu umgehen, dennoch muss man „unter die Motorhaube“ schauen – auch bei souveränen Angeboten. Bei chinesischen Anbietern sind IP-Schutz, Datenzugriffe und Abhängigkeiten besonders kritisch zu prüfen.

Wie häufig ist Security-by-Design in KI-Projekten wirklich gelebte Praxis?
TS | Zu selten. Nur 23 Prozent beziehen Sicherheit von Anfang an in ihre Transformationsprozesse ein. Gleichzeitig driftet das Budget auseinander: Die KI-Ausgaben wachsen aktuell rund 2,6-mal schneller als die Security-Budgets. Das schafft blinde Flecken bei Datenschutz, IP-Schutz und Compliance. Wer KI skaliert, muss Security parallel skalieren – sonst steigt das Restrisiko unverhältnismäßig.

Kann man die Vielzahl interner KI-Anwendungen überhaupt noch überblicken?
TS | Ja – mit KI. Discovery- und Monitoring-Tools identifizieren eingesetzte KI-Modelle und -Dienste, ordnen Risiken zu und liefern Handlungsoptionen. In der Abwehr korreliert KI riesige Datenmengen, hebt Anomalien, priorisiert Vorfälle und schlägt Maßnahmen vor. Wichtig ist ein Zielbild aus Governance, Inventarisierung, Richtlinien, technischen Kontrollen und kontinuierlicher Überwachung. Der Wettlauf hat begonnen – und ohne Invest dreht sich die Spirale zugunsten der Angreifer.

Haben Sie ein Praxisbeispiel wie KI die Cybersecurity unterstützen kann?
TS | In unseren Accenture-Security Operations Centern finden KI-gestützte Systeme die sprichwörtliche Nadel im Heuhaufen. Sie verknüpfen Logs und Telemetriedaten, identifizieren Muster, priorisieren Alarme und unterbreiten Analysten konkrete Empfehlungen. Routinetätigkeiten laufen 24/7 automatisiert. Bei Deepfakes erkennen spezialisierte Verfahren synthetische Stimmen und Videos mit hoher Trefferquote – das ist nach realen Fällen bei Banken in Asien relevant. So werden Reaktionszeit und Qualität spürbar besser.

Ransomware, Social Engineering, Deepfakes – welche Bedeutung hat die „menschliche Schwäche“ im KI-Zeitalter?
TS | Angriffe sind heute auf Personen und Situationen zugeschnitten. Fingierte Bewerbungs-Mails treffen die Personalabteilung im richtigen Moment mit der richtigen Wortwahl. Lösegeldforderungen nach Ransomware-Angriffen werden anhand interner Daten kalkuliert. Deshalb bleiben Sensibilisierung, starke Identitäten und strikte Rechtevergabe unverzichtbar – ergänzt um technische Kontrollen, die KI-gestützte Täuschung erkennen und stoppen.

Welche Trends prägen die nächsten zwei bis drei Jahre?
TS | Erstens Agentic AI: eigenständig agierende KI-Agenten automatisieren komplette Sicherheitsabläufe – von Erkennung bis Remediation. Das entlastet knappe Fachkräfte und erhöht Geschwindigkeit und Qualität. Zweitens Identitäten: Digitale Identitäten von Menschen, Maschinen und künftig auch Agenten werden zum Schlüsselfaktor. Ohne verifizierte, vertrauenswürdige Identitäten bleiben Betrugserkennung und Zugriffssteuerung lückenhaft.

Welche Handlungsempfehlungen geben Sie Kunden?
TS | Security ist Grunddisziplin der digitalen Ökonomie. Sie gehört von Anfang an in jede Initiative – besonders in KI-Projekte. KI stärkt die Verteidigung, wenn das Fundament stimmt. Ignorieren ist keine Option. Wer Strategie, Governance, Basis-Schutz und KI-gestützte Abwehr vereint und die Lieferkette mitdenkt, wird resilienter und handlungsfähig bleiben. •

Multi-Cloud-Security: Komplexität beherrschen, Risiken minimieren

Hybrid- und Multi-Cloud-Architekturen sind längst fester Bestandteil moderner IT-Strategien. Laut dem von Fortinet gesponserten 2025 State of Cloud Security Report setzen 82 Prozent der Unternehmen auf hybride oder Multi-Cloud-Modelle – entweder durch die Kombination lokaler Server mit Public-Cloud-Diensten oder durch die parallele Nutzung mehrerer Anbieter. /// von Thorsten Henning

DIE VORTEILE DIESER STRATEGIEN LIEGEN AUF DER HAND: Flexibilität bei der Wahl des passenden Dienstes für jeden Workload, eine höhere Resilienz gegenüber Ausfällen sowie die Möglichkeit, schnell auf neue Marktanforderungen zu reagieren. Mit dieser Flexibilität steigt jedoch auch die Komplexität der Sicherheitsarchitektur, und damit auch die Angriffsfläche. Hinzu kommen steigende Anforderungen an Compliance und Governance, die Unternehmen zusätzlich belasten. Gerade in stark regulierten Branchen, wie dem Finanz- oder Gesundheitswesen, kann die fehlende Harmonisierung von Sicherheitsrichtlinien zu erheblichen Risiken und Verzögerungen bei Cloud-Projekten führen.

Damit wird deutlich: Wer die Vorteile von Multi-Cloud voll ausschöpfen will, muss Cybersecurity einen zentralen Stellenwert einräumen – von konsistenten Richtlinien über die Abwehr von Bedrohungen bis hin zum Schutz der Endnutzer.

Laut dem 2025 State of Cloud Security Report sehen 55 Prozent der Unternehmen den Verlust an Sichtbarkeit als weiteres Problem. Unterschiedliche Management-Tools, proprietäre Schnittstellen und fragmentierte Datenflüsse sorgen dafür, dass Security-Teams oft nur einen Teil des tatsächlichen Geschehens überblicken. Dies wird besonders heikel beim Schutz sensibler Daten: Durch die Verteilung über mehrere Plattformen erhöht sich die Gefahr von Fehlkonfigurationen und die Einhaltung regulatorischer Anforderungen wie der DSGVO wird erschwert. Fehlende Transparenz kann zudem dazu führen, dass Sicherheitslücken unbemerkt über längere Zeit bestehen bleiben.

Hinzu kommt die wachsende Dynamik von Cyberbedrohungen. 64 Prozent der befragten Unternehmen haben nur wenig Vertrauen in ihre Fähigkeit, moderne, ausgefeilte Angriffe in Echtzeit zu erkennen und zu stoppen. Die Korrelation sicherheitsrelevanter Ereignisse über verschiedene Plattformen hinweg bleibt eine

> „ Um die Vorteile der Multi-Cloud vollständig auszuschöpfen, muss Cybersecurity von Anfang an ein strategischer Kernbestandteil sein und darf nicht als nachgelagerter Kontrollmechanismus betrachtet werden.

Zentrale Herausforderungen in verteilten Cloud-Umgebungen

Die Heterogenität von Multi-Cloud-Umgebungen stellt eine der größten sicherheitstechnischen Herausforderungen dar. Unterschiedliche Anbieter, Services und Architekturen erschweren die zentrale Steuerung von Cybersecurity-Maßnahmen, und jedes zusätzliche System erweitert die Angriffsfläche. Potenzielle Einfallstore entstehen insbesondere durch Fehlkonfigurationen, unzureichende Zugriffskontrollen oder bislang unbekannte Schwachstellen.

Schwachstelle, wodurch gefährliche blinde Flecken entstehen können. Diese Problematik wird durch den Fachkräftemangel verstärkt: 76 Prozent der Unternehmen verfügen nicht über genügend Cybersecurity-Spezialisten. In der Praxis bedeutet dies, dass vorhandene Teams oft mit reaktiven Aufgaben ausgelastet sind und proaktive Cybersecurity-Maßnahmen zu kurz kommen.

Strategien für eine belastbare Multi-Cloud-Security

Effektive Multi-Cloud-Security setzt auf eine durchdachte Strategie und den Einsatz moderner Cyberse-

Bilder: @Fortinet

DER AUTOR
Thorsten Henning
Regional Director Pre-Sales and Business Development DACH bei Fortinet

curity-Tools. Zentrale Elemente sind die kontinuierliche Überwachung der gesamten Cloud-Infrastruktur sowie die automatisierte Behebung von Fehlkonfigurationen oder übermäßigen Berechtigungen. Moderne Cloud-Security-Posture-Management-(CSPM)- und Cloud-Native-Application-Protection-Platform-(CNAPP)-Lösungen erkennen Risiken in Echtzeit und ermöglichen eine sofortige Gegenmaßnahme. Ergänzend sorgt Data Security Posture Management (DSPM) für Transparenz bei der Übertragung sensibler Daten zwischen Cloud-Umgebungen, verhindert unbefugten Zugriff und unterstützt die Einhaltung regulatorischer Vorgaben.

Darüber hinaus sind einheitliche Mechanismen für Bedrohungserkennung und Zugriffskontrolle über alle Plattformen hinweg unverzichtbar. Plattformübergreifende Lösungen wie Cloud Detection and Response (CDR) oder Cloud Workload Protection Platforms (CWPP) verkürzen Reaktionszeiten und verbessern die Präzision der Abwehr. Ein zentrales Identitäts- und Berechtigungsmanagement (CIEM) ermöglicht gleichzeitig die konsistente Durchsetzung von Sicherheitsrichtlinien und reduziert Risiken durch unkontrollierte Zugriffsrechte. Skalierbare, cloudbasierte Security-Tools stellen sicher, dass Schutzmaßnahmen nahtlos in On-Premises- wie auch in Public-Cloud-Umgebungen greifen.

Gleichzeitig bleibt der Mensch ein kritischer Faktor: Investitionen in Schulungen zu DevSecOps, Container-Security oder cloudnativen Architekturen helfen, interne Teams zu stärken und Abhängigkeiten von externen Ressourcen zu reduzieren. In Kombination mit bewährten Cybersecurity-Maßnahmen wie Endpoint Detection and Response (EDR), Next-Generation Firewalls (NGFW), Intrusion Prevention Systemen (IPS), Multi-Faktor-Authentifizierung (MFA) und regelmäßigen Updates entsteht ein End-to-End-Schutz für komplexe Cloud-Umgebungen.

Zentralisierter Plattformansatz statt Tool-Wildwuchs

Die zunehmende Komplexität von Multi-Cloud-Umgebungen macht einen klaren Gegenentwurf zum Tool-Wildwuchs erforderlich. Anstatt zahlreiche isolierte Cybersecurity-Einzellösungen parallel zu betreiben, setzen immer mehr Unternehmen auf konsolidierte Plattformen, die zentrale Cybersecurity-Funktionen bündeln. Laut dem 2025 State of Cloud Security Report bevorzugen 97 Prozent der befragten Unternehmen eine einheitliche Cloud-Security-Plattform mit zentralem Dashboard, um die Komplexität zu reduzieren, konsistente Richtlinien umzusetzen und mehr Transparenz zu schaffen.

Ein Beispiel für einen solchen zentralisierten Ansatz ist die einheitliche, KI-gestützte Plattform Lacework FortiCNAPP. Sie vereint Funktionen wie Cloud Security Posture Management, Cloud-Native Application Protection und Data Security Posture Management in einer Oberfläche und sichert den gesamten Lebenszyklus cloud-nativer Anwendungen aus einer Hand. Darüber hinaus ermöglicht Lacework FortiCNAPP die automatische Erkennung und Behebung von Bedrohungen, KI-gestützte Anomalieerkennung sowie die Integration von Code-Security bereits in der Entwicklungsphase. So können Security-Teams schneller auf Runtime-Bedrohungen reagieren, Datenströme absichern und Berechtigungen konsistent verwalten, ohne die Vorteile einer Multi-Cloud-Architektur einzuschränken. •

FORTINET

Zukunft der Cybersecurity: KI-gestützte Lösungen für neue Herausforderungen

Auch die Cybersecurity kommt um das Thema künstliche Intelligenz nicht mehr herum. Wir haben Experten gefragt: „Was sind die nächsten Schritte in der Entwicklung von KI-gestützten Cybersicherheits-Lösungen, um den sich ständig ändernden Technologiefortschritten gerecht zu werden?“ /// von Konstantin Pfliegl

ALEXANDER OPEL

Product Technology & Education Manager
bei Eset Deutschland

• **KI-GESTÜTZTE CYBERSICHERHEIT** muss künftig mehr leisten als nur Anomalien zu erkennen. Die nächsten Entwicklungsschritte liegen in einer neuen Systemlogik: Lernfähige Modelle müssen aktiv im laufenden Betrieb den Kontext erfassen, sich dynamisch an unbekannte Angriffsmuster anpassen und komplexe Zusammenhänge zwischen technischen Signalen und Bedrohungszielen analysieren und interpretieren können.

Virtuelle Angriffsszenarien

Technologien wie Graph-Neuronale Netzwerke, die Beziehungen in Daten abbilden, reasoning-basierte Bedrohungsanalysen, die logische Schlussfolgerungen ziehen, oder simulationsgestützte Risiko-Projektionen (Digital Twins of Attack), die Angriffsszenarien virtuell durchspielen, werden die Grundlage dafür bilden. Ebenso wichtig ist Resilienz, sowohl gegenüber gezielten Täuschungen durch Angreifer, aber auch ungewollten Fehleinschätzungen durch die KI selbst. Systeme müssen Unsicherheiten offenlegen und Entscheidungen erklärbar machen.

Für Eset heißt das: Unsere KI-Architekturen sind so konzipiert, dass sie europäische Datenschutzstandards erfüllen, nachvollziehbar bleiben und sich in hybride Infrastrukturen integrieren lassen. Die Cloud ist dabei ein entscheidender Enabler, aber ohne dabei die Kontrolle über Daten oder Logik an Dritte abzugeben. Wir glauben: Die Zukunft gehört nicht der Superintelligenz, sondern der intelligenten Zusammenarbeit von Mensch und System. •

STEFAN TIEFEL

Senior Market Development Manager Security
& Network bei Noris Network

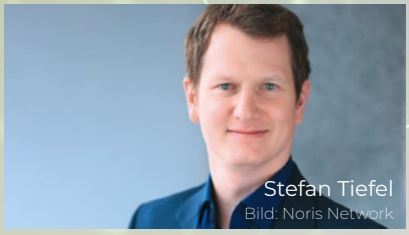
• **AUTONOME SYSTEME**, generative Bedrohungen und Regulierungen stellen die Cybersicherheit vor tiefgreifende Herausforderungen. Es braucht entschlossene Schritte, um künstliche Intelligenz für den Schutz digitaler Infrastrukturen aufzustellen. Googles „Big Sleep“ demonstriert, wie Machine-Learning-Modelle verdächtige Aktivitäten erkennen und unterbinden können – ohne menschliches Zutun. Der nächste Schritt sind vernetzte KI-Agenten, die domänenübergreifend operieren und in der Lage sind, schneller auf komplexe Bedrohungsszenarien zu reagieren.

Nachvollziehbare Entscheidungen

Gleichzeitig stoßen Black-Box-Modelle zunehmend an Grenzen. Deshalb rücken Explainable AI (XAI) und nachvollziehbare Entscheidungen in den Fokus. Nur transparente KI-Modelle lassen sich wirksam in Audits, Compliance-Anforderungen und operative Sicherheitsprozesse integrieren. Neben ihrer Schutzfunktion übernimmt KI zunehmend eine zentrale Rolle in der Orchestrierung und Automatisierung. Von der Analyse verteilter Telemetriedaten bis hin zur Generierung von Richtlinien (Policy-as-Code) reicht das Spektrum moderner Anwendung. In DevSecOps-Pipelines prüfen KI-Modelle Quellcode, APIs und Konfigurationen in Echtzeit und schließen Lücken, bevor sie produktiv werden. Mit der EU-Cyberresilienz-Verordnung und NIS-2 etabliert sich zudem ein verbindlicher Ordnungsrahmen, damit KI-basierte Sicherheitslösungen datenschutzkonform, überprüfbar und ethisch tragfähig werden. •


Alexander Opel
Bild: Eset


Mike Rennie
Bild: GoTo


Stefan Tiefel
Bild: Noris Network

MIKE RENNIE

Senior Manager Information Security
bei GoTo

• **DIE NÄCHSTEN SCHRITTE IN DER ENTWICKLUNG** von KI-gestützten Cybersicherheitslösungen müssen mit dem sich ständig wandelnden technologischen Umfeld – auch mit KI – Schritt halten. KI-basierte Lösungen revolutionieren bereits zentrale Bereiche wie Bedrohungserkennung, automatisierte Reaktion und Schwachstellenmanagement, indem sie Bedrohungen schneller und präziser identifizieren als manuelle oder herkömmliche Prozesse. Etablierte Anbieter im Bereich Cybersicherheit integrieren KI-Funktionen in rasantem Tempo, um „KI für das Gute" einzusetzen.

Evolution von Cyberangriffen

Dieser Fortschritt bringt jedoch neue Herausforderungen mit sich. KI treibt nicht nur die Entwicklung der Cybersicherheit selbst voran, sondern beschleunigt auch die Evolution von Cyberangriffen und den Einsatz „für das Schlechte" – Deepfakes, KI-generierte Schadsoftware und automatisierte Social-Engineering-Angriffe sind wachsende Risiken, selbst in Remote-Support-Szenarien.

Cybersicherheit als Glücksspiel

Die zentrale Herausforderung liegt in der nicht-deterministischen Natur der KI: Es wird immer schwieriger vorherzusagen, wie sich Hacker und ihre Taktiken verändern werden. Für CISOs wird Cybersicherheit dadurch zunehmend zu einem Glücksspiel. Rahmenwerke wie ISO und NIS bieten zwar eine gewisse Struktur für KI-Sicherheit und Risikomanagement, können aber keine genauen Prognosen liefern.

Dennoch stellen sie für IT-Sicherheitsverantwortliche derzeit die besten verfügbaren Werkzeuge dar, um Cyberangriffe innerhalb ihrer verwalteten IT-Umgebungen einzudämmen. KI wird entscheidend künftig sein, um mit der nächsten Generation von Cyberbedrohungen Schritt zu halten – und ihnen entgegenzuwirken. •

MARTIN ENNENBACH
IT-Security Consultant bei TÜV TRUST IT

FRANK SCHWAAK
Field CTO bei Rubrik

• **WÄHREND AKTUELL VIEL ÜBER DEN EINSATZ** von KI zur Verbesserung der Cybersicherheit gesprochen wird, sehen wir die eigentliche Herausforderung darin,kKünstliche Intelligenz selbst sicher, robust und verantwortungsvoll zu gestalten. Denn nur wenn KI-Systeme nicht selbst zur Schwachstelle werden, können sie ein verlässlicher Bestandteil einer modernen Cybersicherheitsstrategie sein.

Sicherheit und Transparenz

Die nächsten Schritte in der Entwicklung KI-gestützter Sicherheitslösungen müssen deshalb vor allem eines leisten: Sie müssen mit der rasanten technologischen Dynamik Schritt halten – ohne Sicherheit, Transparenz und Kontrolle zu verlieren. Genau hier setzt der Gedanke der KI-Governance an.

Bei TÜV Trust IT sehen wir in der Praxis: KI kann nur dann wirksam zur Abwehr von Cyberbedrohungen beitragen, wenn sie von Anfang an strategisch gesteuert wird. Dazu zählen etwa die Bewertung und Zulassung von KI-Modellen im Unternehmenskontext, die Sicherstellung regulatorischer Compliance (zum Beispiel AI Act, DSGVO, NIS-2), die Definition unzulässiger Anwendungen sowie der Aufbau interdisziplinärer Gremien, die IT-Sicherheit, Datenschutz und Fachbereiche zusammenbringen. Als TÜV TRUST IT unterstützen wir Unternehmen dabei gezielt – mit praxiserprobter Expertise in KI-Governance, regulatorischer Absicherung und sicherer Systemgestaltung.

Denn nur wenn KI selbst nicht zur Schwachstelle wird, kann sie ein verlässliches Werkzeug für moderne, adaptive Cyberabwehr sein – etwa in der Anomalieerkennung oder bei der automatisierten Reaktion auf Angriffe. Der nächste notwendige Schritt ist daher der gezielte Aufbau belastbarer KI-Governance-Strukturen, flankiert durch transparente Prozesse, klare Richtlinien und praxisnahe Schulungskonzepte. •

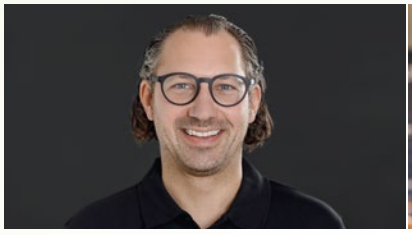
• **CYBER- UND RANSOMWARE-ANGRIFFE** werden professioneller, oft durch künstliche Intelligenz unterstützt. Das erhöht die Nachfrage nach ebenfalls KI-gestützten Cybersicherheits-Lösungen, die Anpassungsfähigkeit und proaktive Bedrohungserkennung verbessern. Algorithmen für maschinelles Lernen (ML) erlauben es, Bedrohungen nahezu in Echtzeit zu identifizieren und darauf zu reagieren. Im Gegensatz zu statischen Hash-Werten mutieren bösartige Codes, aber ML und KI können diese Verhaltensmuster analysieren und Bedrohungen frühzeitig erkennen.

IT-Teams für KI

Unerlässlich sind selbstlernende Systeme, die sich an neue Bedrohungen anpassen. Arbeiten KI-Entwickler und Cybersicherheitsexperten zusammen, bleiben Lösungen effektiv und flexibel. In Krisensituationen unterstützt KI IT-Teams bei der Suche nach dem letzten sauberen Backup, um die Geschäftskontinuität schnell wiederherzustellen. Generative KI automatisiert auch Routineaufgaben, etwa KI-Chat-Begleiter, die bei der Erkennung, Untersuchung, Behebung und Dokumentation von Vorfällen helfen. Das macht Sicherheit effizienter und senkt die Arbeitsbelastung. KI-Tools sind entscheidend, um die Cyber-Resilienz angesichts fehlender qualifizierter IT-Sicherheitsexperten aufrechtzuerhalten.

Transparenz und Kontrolle

Da KI-Agenten mit Zugriff auf Mitarbeiterebene, aber nur begrenzter Aufsicht immer autonomer werden, steigen die operativen Risiken. Unternehmen können schädliche Aktionen von Agenten oft nicht verfolgen oder rückgängig machen. Rubrik schließt diese Lücke mit Agent Rewind und bietet Transparenz und Kontrolle über KI-gesteuerte Aktivitäten. •



Martin Ennenbach
Bild: TÜV Trust IT

Frank Schwaak
Bild: Rubrik

Cyber Security meets Qualitätsmanagement

SCHLAGKRÄFTIGES DUO moderner Unternehmensführung

Cyber Security ist von der IT-Aufgabe zur gesamtunternehmerischen Herausforderung geworden und betrifft damit auch immer stärker das QM. Moderne Softwarelösungen wie die der ConSense GmbH machen Cyber Security zum strategisch eingebundenen Bestandteil eines intelligent vernetzten Managementsystems.

DIE BEDROHUNG DURCH CYBER-ANGRIFFE WÄCHST. Unternehmen erleiden durch erfolgreiche Attacken aus dem Netz neben hohen finanziellen Schäden auch einen Imageverlust. Angesichts der Zunahme der Vorfälle gewinnen Normen und Gesetze zur Stärkung der Informationssicherheit wie ISO 27001, NIS2 und CISIS12 an Bedeutung. Sie alle verfolgen das Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und Systemen zu gewährleisten. Neben technischen Schutzmaßnahmen verlangen sie ein ganzheitliches Sicherheitsverständnis.

QM als Cyber-Schutzfaktor

Das macht Cyber Security zu einer Aufgabe, die nicht nur die IT betrifft, sondern das gesamte Unternehmen einschließt – und damit auch das Qualitätsmanagement. Ein systematisches QM unterstützt dabei, Prozesse transparent zu gestalten, Risiken zu identifizieren und durch kontinuierliche Verbesserung widerstandsfähiger zu werden. Diese Grundprinzipien lassen sich auf den Bereich Cyber Security übertragen. Moderne Softwarelösungen schaffen Synergien zwischen QM und Cyber Security, um ein effizientes Management zu unterstützen. Die Aachener ConSense GmbH entwickelt solche Softwarelösungen zum Aufbau transparenter QMS und IMS. Sie helfen dabei, Prozesse nachvollziehbar zu dokumentieren, Risiken zu erkennen und zu minimieren, um die Resilienz eines Unternehmens zu stärken. Ein zentrales Tool ist das Modul ConSense GRC (Governance, Risk & Compliance).

Komplexität im Griff mit ConSense GRC

ConSense GRC versteht Cyber Security als integralen Bestandteil eines ganzheitlichen Compliance- und Risikomanagements. Das Modul ergänzt die **ConSense Softwarelösungen** und vereinfacht die Umsetzung von Anforderungen wie ISO 27001, NIS2, TISAX oder branchenspezifischen Standards, verbunden mit weiteren Regelwerken wie der DSGVO. Durch die zentrale Verwaltung von Richtlinien, Prozessen und Nachweisdokumenten entsteht ein transparentes, ganzheitliches Sicherheitskonzept. Zentrales Element ist das integrierte Asset-Management: Für jedes relevante Asset im Unternehmen wird der Schutzbedarf ermittelt und automatisch innerhalb der Struktur des Systems „vererbt". Es entsteht ein vollständiges Bild schutzwürdiger Werte im Unternehmen und eine fundierte Basis für die Risikobewertung. Automatisierte Prozesse erinnern an Prüfpflichten und Fristen, Risiken werden systematisch überwacht und Berichte per Knopfdruck erstellt. Damit werden Audits vereinfacht und die Rückverfolgbarkeit gesichert.

Ganzheitliche Sicherheitsstrategie:
Moderne Software wie die GRC Lösung von ConSense macht Cyber Security zum strategisch eingebundenen Bestandteil eines intelligent vernetzten Managementsystems

(Bildquelle: #452879076 Adobe Stock – by Gorodenkoff)

Cyber Security beginnt im QM

Ein gelebtes QM-System bildet die Basis für ganzheitliche Sicherheitsstrategien. Die **GRC Lösung der ConSense GmbH** integriert Cyber Security nahtlos in ConSense QMS und IMS. So entsteht ein Gesamtsystem, das Synergien nutzt, Insellösungen vermeidet und die Resilienz stärkt. Damit wird Cyber Security von der isolierten IT-Disziplin zum strategisch eingebundenen Bestandteil eines intelligent vernetzten Managementsystems. •

HINTERGRUND ConSense GmbH

Die ConSense GmbH aus Aachen zählt zu den technologisch führenden Anbietern von Softwarelösungen und Services für Qualitäts- und Integrierte Managementsysteme. Sie entwickelt seit 2003 skalierbare Lösungen für Unternehmen jeder Größe mit Fokus auf einem Softwarestandard für IMS. Dahinter steht der Anspruch, komplexe Herausforderungen effizient zu lösen – mit transparenten, verständlichen und anwendungsfreundlichen Managementsystemen.

ConSense setzt konsequent auf lebendige Systeme, die gezielt die Akzeptanz von Anwender:innen fördern und sie zur aktiven Nutzung einladen. Die flexiblen Lösungen unterstützen dabei, Normen und hochkomplexe regulatorische Anforderungen effizient und konform umzusetzen – von ISO-Normen über Themen wie Compliance, Cyber Security, NIS2, ISMS, Umweltmanagement und mehr. Über 1000 erfolgreich realisierte Projekte und Anwendungszahlen im sechsstelligen Bereich zeugen von der umfassenden Erfahrung und Expertise des ConSense Teams.

KI im Doppelspiel: Autonome Agenten definieren die Verteidigung neu

Künstliche Intelligenz ist zu einem prägenden Akteur geworden, der unseren Alltag, unsere Arbeitswelt und die Abwehr digitaler Bedrohungen grundlegend verändert. Während Unternehmen KI nutzen, um Abwehrstrategien zu stärken, setzen Cyberkriminelle sie ein, um Angriffe skalierbarer und raffinierter zu gestalten. /// von Dr. Martin Krämer

IM JAHR 2025 RÜCKEN KI-AGENTEN INS ZENTRUM: autonome Systeme, die mit minimalem Input komplexe Aufgaben planen, ausführen und anpassen. Dadurch werden sowohl Verteidigung als auch Angriffe transformiert. Generative KI und Large Language Models (LLMs) ermöglichen täuschend echte Phishing-Mails ohne typische Fehler, massenhaft personalisierte Betrugsversuche sowie automatisierte Fake-Websites oder Chatbot-Betrug. Deepfakes verstärken CEO- und Social-Engineering-Angriffe wie im Fall des britischen Ingenieurbüros Arup, das vergangenes Jahr 25 Millionen US-Dollar durch gefälschte Videoanrufe verlor. Zunehmend rücken solche kognitiven Angriffe in den Fokus: Sie zielen nicht nur auf technische Schwachstellen, sondern manipulieren gezielt Wahrnehmung und Verhalten, etwa durch Desinformationskampagnen, die Vertrauen untergraben oder Wahlergebnisse beeinflussen.

Risiken bei LLM-Einsatz

Unternehmen riskieren durch schlecht integrierte KI-Schnittstellen neue Angriffsvektoren wie Prompt Injection oder Content Evasion. Multimodale KI erhöht das Risiko, schädliche Befehle in Bild- oder Audiodaten einzubetten. RAG-Systeme, die externe Daten einbinden, sind anfällig für Data Poisoning und Fehlinformationen. Zusätzlich bergen Trainingsdaten Bias-Risiken, die zu diskriminierenden oder falschen Entscheidungen führen können.

Autonome KI-Agenten als Angriffsakteure

Forschende warnen vor abtrünnigen Systemen, die sich eigenständig reproduzieren oder gegen ihre Betreiber agieren könnten. In kriminellen Händen können KI-Agenten Schwachstellen aufspüren, Social-Media-Daten massenhaft abgreifen oder vollautomatisch personalisierte Betrugsoperationen durchführen. Das Potenzial zur vollständigen Automatisierung von Cybercrime ist erheblich.

Defensive Nutzung von KI

Unternehmen müssen proaktiv handeln:

- **Erkennung & Reaktion:** KI-gestützte Plattformen analysieren Netzwerkverhalten in Echtzeit, erkennen Anomalien und LOL-Techniken (Living off the land) schneller als Menschen.
- **Phishing-Prävention:** Analyse von Sprachmustern, Metadaten und Verhalten identifiziert KI-generierte Angriffe, Deepfake-Checks entlarven manipulierte Medien.
- **Schulung:** Simulierte KI-Angriffe sensibilisieren Mitarbeitende gezielt.
- **Täuschungstechnologien:** KI-Honeypots und kontinuierlich trainierte Abwehrmodelle erschweren Angreifern die Arbeit.
- **Bekämpfung von Desinformation:** KI-Tools erkennen synthetische Inhalte, verifizieren Quellen und können Angreifer mit Gegenbots wie „Daisy“ in nutzlose Gespräche verwickeln.

Fazit

In einer Zukunft, in der Angreifer und Verteidiger gleichermaßen KI einsetzen, ist Wissen über gegnerische Methoden entscheidend. Anstatt unüberlegt neue KI-Tools einzuführen, sollten Unternehmen strategisch prüfen, ob Lösungen der steigenden Raffinesse der Bedrohungen standhalten. Ein unkontrollierter KI-Einsatz ohne Risikobewertung könnte neue Schwachstellen schaffen – maßvolle, gut überwachte Implementierung ist daher essenziell. •

DER AUTOR
Dr. Martin Krämer
ist Cybersecurity Evangelist bei KnowBe4.

Bild: KnowBe4

Wenn aus E-Mails Einfallstore werden:

Cloud-Schutz mit System

ESET Cloud Office Security schützt Microsoft 365 und Google Workspace zuverlässig vor digitalen Angriffen. Die Lösung lässt sich einfach einsetzen und erfüllt höchste Datenschutzanforderungen.

OB KUNDEN-E-MAILS, INTERNE ABSPRACHEN ODER TEAMS-MEETINGS: In vielen Unternehmen läuft ein Großteil der Kommunikation heute über Microsoft 365 oder Google Workspace. E-Mails, Dokumente und Termine werden geteilt, Chats und Videokonferenzen sind Alltag. Doch genau dort, wo die Zusammenarbeit einfach funktioniert, entstehen neue Risiken. Phishing-Mails, verseuchte Anhänge oder Zugriffe auf freigegebene Dateien bleiben oft unentdeckt, wenn man sich nur auf den Standardschutz der Plattformen verlässt.

ESET Cloud Office Security (ECOS) sorgt genau hier für mehr Sicherheit. Die Lösung erweitert den Schutz für Microsoft 365 und Google Workspace mit klaren, praxisnahen Funktionen. Die Kombination aus Spam-Filter, Malware-Scanner, Anti-Phishing und Cloud Sandboxing sichert die Unternehmenskommunikation, Zusammenarbeit und den vorhandenen Cloud-Speicher nachhaltig ab.

Cloud-Schutz, der einfach funktioniert

Wie wichtig Cloud-Sicherheit ist, belegen diese Zahlen aus der ESET Telemetrie. Jeden Monat erkennt ECOS im Schnitt über 65.000 Phishing-Versuche, 75.000 E-Mail-Bedrohungen und rund 6,3 Millionen Spam-Nachrichten. Auch scannt die Software automatisch alle Dateien, die über OneDrive, SharePoint, Google Drive oder Microsoft Teams geteilt werden. Das senkt nicht nur das Risiko, sondern entlastet auch die IT-Abteilung im Alltag.

Die Einrichtung von ECOS dauert nur wenige Minuten. Neue Nutzer werden automatisch erkannt und gesichert, ohne dass Admins manuell nacharbeiten müssen. Die Lösung wächst mit, passt sich flexibel an und ist besonders für hybride Arbeitsmodelle geeignet. Eine zentrale Web-Konsole sorgt dafür, dass Verantwortliche den Überblick behalten und Einstellungen nach Bedarf anpassen können.

Security-Funktionen mit echtem Mehrwert

Wer ECOS im Alltag nutzt, merkt schnell: Es geht nicht nur um Schutz, sondern auch um Kontrolle und Effizienz. Beispielsweise erlaubt der automatische E-Mail-Rückruf, verschickte Nachrichten auch nach der Zustellung zu löschen, wenn sich herausstellen sollte, dass sie infiziert sind.

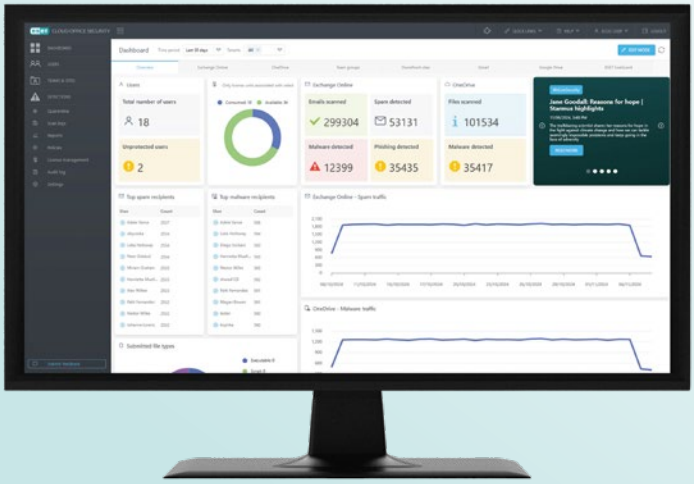
Mit dem sogenannten „Body-Banner" können eingehende E-Mails gut sichtbar klassifiziert werden. Warnungen wie „External" oder „Phishing-Versuch", Erklärungstexte und besondere Farben geben dem Empfänger wichtige Informationen. So kann er schneller und sicherer entscheiden, ob es sich vielleicht um eine gefährliche Nachricht handelt.

Zudem wurden der Anti-Spoofing- und Homoglyphen-Schutz zur Erkennung und Blockierung von Phishing-Versuchen durch gefälschte E-Mail-Absender und manipulierte URLs hinzugefügt. Dies hilft Angriffe zu erkennen, bei denen einzelne Buchstaben gegen ähnlich aussehende Zeichen ausgetauscht wurden.

ESET LiveGuard Advanced eliminiert Phishing, APTs und Zero-Days

Mit ESET LiveGuard Advanced bietet die Lösung einen wichtigen Schutzschild an. Die Analyse von potentiell gefährlichem und bisher unbekanntem Binärcode (Zero Days) in einer Cloud-Sandbox bietet zusätzlichen Schutz vor beispielsweise Advanced Persistent Threats (APT) und Ransomware. •

www.eset.de/itsa



Dashboard der Cloud-Konsole

Schutz ohne Grenzen: Sicherheit für verteilte Arbeitsplätze

Cyberangreifer werden von Tag zu Tag agiler und raffinierter. Entsprechend muss die Absicherung von Unternehmensnetzwerken weit über die Installation herkömmlicher Firewalls und Antivirensoftware hinausgehen. /// von Paul Moll

UNTERNEHMEN HABEN HEUTZUTAGE MIT HOCHENTWICKELTER MALWARE UND RANSOMWARE sowie mit hartnäckigen, gezielten Angriffen zu kämpfen. Und diese erfordern eine einheitliche Verteidigung. Ein robuster Schutz kann nur durch die Integration intelligenter, cloudfähiger Lösungen erreicht werden, die alle kritischen Ressourcen eines Unternehmens schützen. Vor diesem Hintergrund sind hier einige wichtige Tipps im Zuge der Auswahl einer Netzwerksicherheitslösung, die sowohl Mitarbeiter im Homeoffice und unterwegs als auch die Bürobelegschaft umfassend schützt:

Erster Schritt: Vollständige Bewertung der Infrastruktur
Bevor die Entscheidung für den richtigen Ansatz fallen kann, ist es wichtig, die aktuelle Infrastruktur gründlich zu bewerten. Dabei sind Faktoren wie die Anzahl der Endgeräte, der Umfang der Cloud-Nutzung und die vorhandenen Sicherheitstools zu berücksichtigen. Unternehmen mit verteilten Standorten oder solche, die mit sensiblen Daten umgehen, benötigen fortschrittliche KI-gestützte Funktionen zur Erkennung von Bedrohungen und zur Reaktion in Echtzeit.

KI-gestützter Zero-Day-Schutz
Im Zeitalter polymorpher Malware und Zero-Day-Exploits reicht herkömmlicher signaturbasierter Virenschutz nicht mehr aus. Es zählen Lösungen, die KI-gestützte Bedrohungserkennung und verhaltensbasierte Analysen nutzen. Um größtmögliche Sicherheit zu gewährleisten, müssen potenzielle Bedrohungen in Echtzeit identifiziert und neutralisiert werden. Nur so kann ein Netzwerk den sich ständig weiterentwickelnden Risiken immer einen Schritt voraus sein.

Einheitliches Bedrohungsmanagement
Fragmentierte Sicherheitssysteme führen allzu oft zu Lücken und Ineffizienzen, die Kriminelle ausnutzen können. Durch die Einführung einer einheitlichen Sicherheitsplattform, die moderne Firewall-Funktionen, Intrusion Prevention Systeme (IPS), sichere Web-Gateways und eine zentralisierte Verwaltung vereint, können Unternehmen ihre Sicherheitslage über eine einzige Oberfläche einsehen und administrieren. Dies ermöglicht eine schnellere Korrelation von Bedrohungen und beschleunigt die Reaktion auf Vorfälle im gesamten Netzwerk.

Cloudbasierte Skalierbarkeit und Echtzeit-Bedrohungsinformationen
Remote-Arbeit und cloudbasierte Infrastrukturen sind in den meisten Unternehmen gang und gäbe, was bedeutet, dass es in besonderem Maße auf Skalierbarkeit und Agilität ankommt. Cloudbasierte Lösungen bieten die Flexibilität

DER AUTOR
Paul Moll ist Senior Field Marketing Manager Central Europe bei Watchguard Technologies.
Bild: Watchguard

und Aktualität von Bedrohungsinformationen, die zur Abwehr neuer Schwachstellen erforderlich sind. Durch einen kontinuierlichen Fluss intelligenter Echtzeit-Informationen wird sichergestellt, dass Abwehrmaßnahmen mit der Bedrohungslage Schritt halten.

Einhaltung gesetzlicher Standards

DSGVO, BSI-Grundschutz und NIS-2 stellen strenge Compliance-Anforderungen, denen die Netzwerksicherheit gerecht werden muss. Es geht nicht nur darum, verlässlichen Schutz zu bieten, sondern auch alle relevanten, regulatorischen Aspekte zu berücksichtigen. Nur so lassen sich Strafgelder und/oder Reputationsschäden stichhaltig abwenden.

Kultur des Sicherheitsbewusstseins

Menschliches Versagen ist nach wie vor eine der häufigsten Ursachen für Cybersicherheitsverletzungen. Es gibt keine Technologie, die entsprechende Fehler vollständig ausgleichen kann. Regelmäßige, gezielte Schulungen zum Sicherheitsbewusstsein sind entscheidend, um den Technologieeinsatz auf ein solides Fundament zu stellen und sich vor Social-Engineering-Taktiken und Phishing-Betrug zu schützen.

Leistung ohne Kompromisse

Die in einem hybriden Netzwerkkonzept verfügbaren Sicherheitsmaßnahmen dürfen sich nicht negativ auf die Produktivität eines Unternehmens auswirken. Es sollte jederzeit gewährleistet sein, dass es nicht zu Beeinträchtigungen kommt. Damit die Belegschaft auch in den sichersten Umgebungen produktiv arbeiten kann, ist verlässliche Leistung beim Netzwerkschutz das A und O.

Durchführung von Pilotprojekten

Vor einer vollständigen Einführung können Pilotversuche mit der Lösung in einem kontrollierten Segment des Netzwerks wertvolle Erkenntnisse liefern. So lassen sich die Leistung und Integrationsfähigkeit bewerten und die Konfiguration optimieren, um Fehlalarme zu reduzieren. Es ist hilfreich, wichtige Stakeholder frühzeitig einzubeziehen, um sicherzustellen, dass die Lösung bei einer unternehmensweiten Einführung tatsächlich den Anforderungen und betrieblichen Bedürfnissen entspricht. Robuste IT-Sicherheit hängt von einer proaktiven, einheitlichen Verteidigungsstrategie ab, die alte Zöpfe in Form von isolierten Tools wie Antivirenprogrammen abschneidet.

Cybersicherheitslösungen für verteilte Unternehmen

Das Konzept des hybriden Arbeitens steht in der heutigen, sich schnell verändernden Geschäftswelt an vorderster Front. Da Unternehmen zunehmend auf flexible Arbeitsmodelle und Remote-Zusammenarbeit umstellen, ist die Gewährleistung eines sicheren Zugriffs auf Unternehmensnetzwerke, -geräte und -daten wichtiger denn je. Im Zuge des Übergangs zu hybriden Arbeitsmodellen bieten sich für Cyberkriminelle deutlich mehr Möglichkeiten. Sowohl Mitarbeitende als auch Arbeitsgeräte an Büro- und Remote-Standorten können ein Sicherheitsrisiko darstellen. Hybride Arbeitsmodelle ermöglichen es der Belegschaft, zwischen Remote- und Büroarbeit zu wählen und selbst zu entscheiden, wo bzw. wann sie arbeiten. Eine solch bedeutende Veränderung erfordert von Unternehmen, ihren hybriden Arbeitsplatz mit einem modernen Sicherheitsportfolio vor Cyberangriffen zu schützen.

Einheitliche Sicherheit ist der Schlüssel zu umfassendem Schutz. Ein solches Konzept berücksichtigt, dass kein einzelnes Sicherheitsprodukt oder keine einzelne Sicherheitslösung unfehlbar ist. Stattdessen werden verschiedene Sicherheitsmaßnahmen kombiniert, um Kundenumgebungen, Geräte und Benutzer zu schützen. Durch die Etablierung mehrerer Verteidigungsebenen reduzieren sich die Lücken und Schwachstellen zwischen den einzelnen Ebenen, so dass es für Cyberkriminelle deutlich schwieriger wird, Schwachstellen auszunutzen.•

Internationale Bühne für Sicherheitslösungen

Zwischen GenAI, Souveränität und Managed Security Services: Thimo Holst, Exhibition Director der it-sa, über die aktuellen Sicherheitstrends der Messe, die Vernetzung von KMU mit Konzernen und das neue Format CIO-Match. /// von Heiner Sieger

> „ Deutlich an Fahrt gewinnt KI – speziell GenAI. Sie verändert nicht das Grundmuster des Wettlaufs zwischen Angreifern und Verteidigern, beschleunigt ihn aber drastisch.
>
> *Thimo Holst*

Herr Holst, welche Rolle spielt die it-sa heute im internationalen Vergleich – und wie hat sich ihre Relevanz in den vergangenen Jahren verändert?
Thimo Holst | Die it-sa ist in Europa die größte Veranstaltung für IT-Sicherheit; je nach Kennzahl – etwa der Ausstellungsfläche – rangiert sie weltweit an der Spitze. Das Wachstum ist rasant: Wir legen seit Jahren um 10 bis 15 Prozent zu, 2025 kommt eine zusätzliche Messehalle hinzu, die bereits ausgebucht ist. Bei den Ausstellern ist das Feld sehr international – von europäischen bis zu zahlreichen US-Anbietern. Beim Publikum ist die Messe bislang überwiegend deutschsprachig. Das ändert nichts an der globalen Relevanz, zeigt aber, wo unsere Ausbaupotenziale liegen: vor allem mehr internationale Fachbesucher nach Nürnberg zu holen.

Welche Cybersecurity-Themen stehen 2025 ganz oben – und wie spiegeln sie sich in Programm und Ausstelleangeboten wider?
TH | Unser Programm entsteht bottom-up: Aussteller und Partner bringen die Inhalte ein, dadurch sehen wir unmittelbar, was Priorität hat. Ransomware, Supply-Chain-Angriffe und Zero Trust sind weiterhin stark vertreten. Deutlich an Fahrt gewinnt KI – speziell GenAI. Sie verändert nicht das Grundmuster des Wettlaufs zwischen Angreifern und Verteidigern, beschleunigt ihn aber drastisch: Angriffe werden raffinierter, Abwehrlösungen nutzen KI spiegelbildlich. Zunehmend wichtig werden außerdem nationale und europäische Sicherheit, hybride Kriegsführung und die Frage digitaler Souveränität: Wem kann ich – auch geopolitisch – vertrauen?

Das klingt nach einem Drahtseilakt zwischen globalen Anbietern und Vertrauensfragen: Wie gehen Sie mit dem Spannungsfeld um, wenn viele US- oder asiatische Firmen ausstellen und zugleich europäische Datenhoheit diskutiert wird?
TH | Wir sind Plattformanbieter. Unsere Aufgabe ist es nicht, Lösungen als „vertrauenswürdig" oder „nicht vertrauenswürdig" zu klassifizieren. Vielfalt ist gewollt – mit klaren politischen Leitplanken: Seit Beginn des russischen Angriffskriegs lassen wir keine russischen Aussteller zu. Ansonsten entscheiden der Markt und unsere Besucher, wem sie Vertrauen schenken. Wir beobachten geopolitische Entwicklungen, mögliche Handelsbarrieren und deren Auswirkungen aufmerksam. Diese Fragen gehören auf die Bühne – und werden auf der it-sa offen diskutiert.

NIS2, DORA, EU Cyber Resilience Act: Wie unterstützt die it-sa Entscheider und IT-Verantwortliche bei Verständnis und Umsetzung?
TH | Durch unsere enge Zusammenarbeit mit BSI, Bitkom und TeleTrusT sowie europäischen Partnern wie ECSO und ENISA bieten wir umfassende Orientierung. In sechs offenen Foren direkt in den Hallen präsentieren Aussteller und Institutionen Praxisvorträge und konkrete Lösungswege. Ergänzend vertiefen ganztägige Tracks im Congress-Programm regulatorische Anforderungen, Best Practices und Umsetzungsschritte. Der Zugang bleibt niederschwellig, damit sich Verantwortliche – vom IT-Leiter bis zum CISO – gezielt einen ganzen Tag lang in ein Thema einarbeiten können.

Welche Technologien oder Ansätze haben aus Ihrer Sicht das größte Potenzial – oder bergen die größten Risiken?
TH | Als Veranstalter kuratieren wir Schwerpunkte nicht inhaltlich, sondern orchestrieren ein starkes Netzwerk: Aussteller, Verbände und Weiterbildungspartner setzen die inhaltlichen Akzente. Firmen stellen in den Foren Lösungen vor; Trainingsanbieter bieten vertiefende Schulungen im Kongress; Verbände ergänzen mit strategischer Einordnung. Außerdem vernetzen wir gezielt Entscheider – etwa über unser neues Format CIO Match,

DER GESPRÄCHSPARTNER

Thimo Holst

ist Exhibition Director der it-sa Expo&Congress bei der NürnbergMesse. Mit seinem Team treibt er die Internationalisierung auf Besucherseite, den Ausbau des Kongresses und die inhaltliche Strukturierung der Messe voran. Die it-sa gilt als Europas größte Fachmesse für IT-Sicherheit in Nürnberg; die digitale Plattform it-sa 365 ergänzt das Angebot ganzjährig.

das Top-CIOs und CISOs mit Anbietern zusammenbringt. Die Bewertung, was das meiste Potenzial oder Risiko hat, überlassen wir bewusst den Fachexperten.

Viele KMU kämpfen mit knappen Ressourcen. Welchen konkreten Nutzen zieht der Mittelstand aus einem Besuch der it-sa?

TH | Zunächst schafft der Besuch Bewusstsein – und das ist essenziell. Das starke Wachstum zeigt: Die Relevanz ist im Mittelstand angekommen, doch es gibt weiterhin Lücken. Deshalb haben wir erstmals eine europaweite Studie beauftragt, die speziell KMU adressiert. Der Fragebogen vergleicht Selbsteinschätzung und tatsächlichen Reifegrad, angelehnt an BSI-Checklisten. So machen wir sichtbar, wo Handlungsbedarf besteht. Auf der Messe finden KMU auf kurzem Weg Anbieter, die zu ihrem Reifegrad passen – von Basismaßnahmen bis zu Managed Services – und erhalten konkrete, umsetzbare Fahrpläne.

Die it-sa gilt als starke Netzwerkplattform. Welche Formate bringen Start-ups, etablierte Anbieter, Anwender und Forschung gezielt zusammen?

TH | Am oberen Ende der Entscheiderkette adressiert CIO-Match bis zu 50 Top-CIOs und CISOs aus Konzernen und großen Mittelständlern – mit kuratierten Gesprächen auf Augenhöhe. Für Start-ups bieten wir Komplettpakete inklusive Messestand und Bühnenpräsenz; die Nachfrage ist so groß, dass es Wartelisten gibt. Gemeinsam mit dem ATHENE Center, dem IT-Sicherheitscluster und Sponsoren wie Infinigate, Telekom und Kaspersky verleihen wir jährlich den Start-up-Award. Unser Ziel: passgenaue Kontakte und Bühne für Innovationen.

Menschliche Fehler und Fachkräftemangel bleiben Dauerbrenner. Wie spielt die it-sa diese Themen?

TH | Unser Publikum ist überwiegend fachlich versiert – von IT-Security-Teams bis hin zu CISOs und CIOs. Entsprechend liegt der Schwerpunkt darauf, wie Verantwortliche Awareness im Unternehmen schaffen: Schulungsangebote, Phishing-Simulationen, Policies, Usability. Dazu kommt der Trend zu Managed Security Services, um Personalengpässe abzufedern. Beides zieht sich als Querschnittsthema durch Vorträge und Ausstellerlösungen – ohne in diesem Jahr die Überschrift zu bilden. Entscheidend ist: Wir liefern Tools, Wissen und Partner, damit Sicherheitskultur im Alltag entsteht.

Wohin entwickelt sich die it-sa: stärkere Internationalisierung, mehr digital – oder bleibt persönliches Netzwerken das Herzstück?

TH | Beides: Mit it-sa 365 haben wir längst eine ganzjährige digitale Plattform mit Vorträgen, Workshops und Matchmaking. Für die Präsenzmesse verfolgen wir drei klare Ziele: Erstens Europa – wir wollen die starke Aussteller-Internationalität auf die Besucherseite übertragen. Zweitens der Ausbau des Kongresses hin zu einem Forum, das auch Politik, Verbände und Top-Entscheider adressiert. Drittens Orientierung: In einem komplexen Markt mit rund 1.000 Ausstellern und etwa 30.000 Besuchern müssen sich die Richtigen effizient finden – durch kluge Struktur, klare Themenpfade und Formate.

Wie hat sich für Sie persönlich Rolle und Aufgaben in den vergangenen Jahren verändert?

TH | Ich bin seit mehr als 15 Jahren im Messegeschäft und habe die it-sa nach dem Ruhestand meines Vorgängers übernommen – als Exhibition Director. Seitdem halte ich mit dem Team die hohe Dynamik der Messe, entwickle aber gleichzeitig die drei strategischen Linien weiter: Internationalisierung in Europa, ein gestärkter Kongress und mehr Orientierung für Besucher und Aussteller. Die it-sa hat enormes Potenzial – und wir arbeiten daran, es systematisch zu heben. •

KI als Angriffswerkzeug: Unternehmen müssen wachsam sein

Phishing, Erpressung, Datendiebstahl: Die Zahl der Cyberangriffe auf Unternehmen nimmt stetig zu. Die Cyberganoven gehen dabei mithilfe von künstlicher Intelligenz immer raffinierter vor. Das stellt Unternehmen vor immer größere Herausforderungen.

/// von Konstantin Pfliegl

DIE BEDROHUNGSLAGE FÜR UNTERNEHMEN IN DEUTSCHLAND VERSCHÄRFT SICH: Vergangenes Jahr kam es in 15 Prozent der Betriebe zu IT-Sicherheitsvorfällen – 4 Prozentpunkte mehr zwei Jahre zuvor. Gut die Hälfte davon war sogar mehrfach betroffen. Die Zahlen gehen aus der aktuellen Studie „Cybersicherheit in deutschen Unternehmen: Neue Bedrohungslage – besserer Schutz" des TÜV Verbands hervor.

Organisierte Kriminalität und staatliche Akteure

Unternehmen fürchten vor allem kriminelle Banden und staatliche Hacker. Jeweils rund die Hälfte der vom TÜV Verband befragten Unternehmen sieht in der organisierten Kriminalität und in Cybergangstern, die im Auftrag von Staaten tätig sind, eine beträchtliche Bedrohung. Vor allem größere Unternehmen ab 250 Mitarbeiter sehen Angriffe auf die firmeneigene IT durch organisierte Kriminelle als realistisch. Fast drei Viertel von ihnen (73 Prozent) sehen dies als Bedrohung. Mit abnehmender Größe sinkt auch die Sorge, zum Opfer solcher Attacken zu werden.

Eigene Beschäftigte werden übrigens über alle Unternehmensgrößen hinweg nur von einer Minderheit als Gefahr betrachtet.

Angriffsmethode Nummer 1: Phishing

Die mit Abstand häufigsten Angriffsmethoden waren Phishing- und Spear-Phishing-Angriffe, 84 Prozent der betroffenen Unternehmen berichten von solchen Angriffen.

Je zwölf Prozent der von einem Sicherheitsvorfall betroffenen Betriebe nennen Passwort- und Ransomware-Angriffe als nächsthäufige Ursachen, gefolgt von Denial-of-Service-Angriffen (DoS) oder Distributed-Denial-of-Service-Attacken (DDoS) mit 6 Prozent.

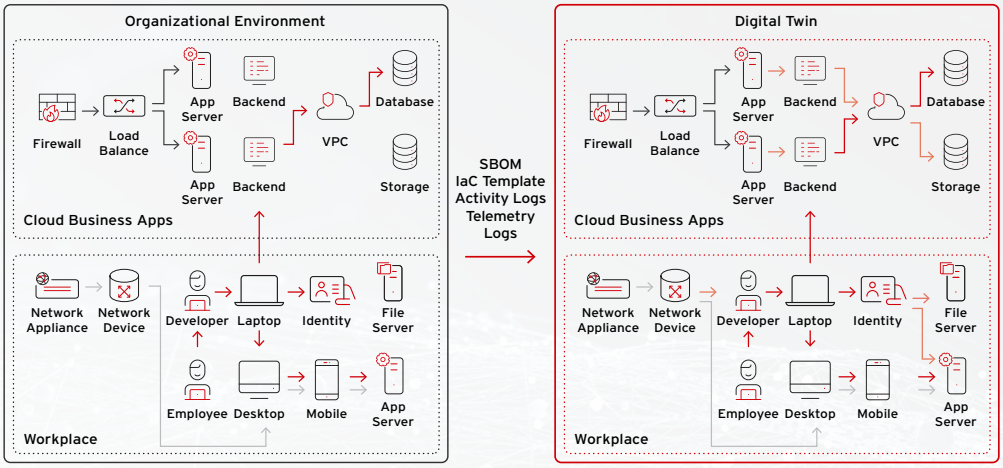
Spear-Phishing-Angriffe sind dabei eine besonders besorgniserregende Variante von Cyberkriminalität. Eine vermeintliche Mail vom Kunden oder dem Kreditinstitut, mit dem ein Unternehmen zusammenarbeitet – zum Beispiel mit der Bitte, über einen Link ein paar Daten zu auf zu überprüfen: Beim Spear-Phishing nutzen Cyberkriminelle ihr Wissen über Beschäftigte aus, um sie zu täuschen und gezielt Zugang zum Unternehmenskonto der Person zu erhalten. Der Erfolg von Phishing-Angriffen liegt laut dem TÜV Verband möglicherweise in den immer besser werden KI-basierten Textgeneratoren wie ChatGPT begründet: Sie tragen in den Händen von Kriminellen zu einem höheren Grad an Automatisierung, Professionalisierung und Individualisierung von Phishing-Angriffen bei.

Künstliche Intelligenz: Schutz und Gefahr

Viele betroffene Unternehmen sind davon überzeugt, dass die Angreifer bei ihren Attacken auf künstliche Intelligenz setzten (51 Prozent). Bei großen Unternehmen ab 250 Mitarbeiter sind es sogar 81 Prozent.

Doch auch wenn sich die Unternehmen häufig sicher sind, dass Cyberkriminelle auf KI setzen – viele Betriebe nutzen selbst keine künstliche Intelligenz zur Abwehr (73 Prozent). Lediglich 10 Prozent haben bereits eine KI zur Abwehr im Einsatz. Diese kommt vor allem zur Betrugserkennung (70 Prozent), Anomalie-Erkennung (59 Prozent) und bei der Schwachstellenanalyse (58 Prozent) zum Einsatz. •

Von reaktiver zu **proaktiver Cybersecurity**



Der Cybersecurity Digital Twin erstellt eine virtuelle Simulation der individuellen IT-Umgebung

CYBERKRIMINALITÄT IST HEUTE EIN GLOBALES GESCHÄFT und die Akteure in einer hochprofessionellen Schatten-Industrie organisiert. Gleichzeitig haben IT-Security-Teams mit einer wachsenden Angriffsfläche und einer Flut an Warnmeldungen zu kämpfen, die es erschwert, kritische Indikatoren zu erkennen. Dazu kommen neue regulatorische Anforderungen. Künstliche Intelligenz wird deshalb immer wichtiger, um die täglichen Security-Herausforderungen zu meistern. Gerade Agentenbasierte Künstliche Intelligenz (Agentic AI) bietet Unternehmen verschiedene Unterstützungs- und Automatisierungsmöglichkeiten, mit denen sie proaktiv werden können, um Angreifern einen Schritt voraus zu sein.

Spezialisierte Cybersecurity-Agenten

Ein Beispiel dafür sind sogenannte „Cybersecurity Digital Twins". Diese KI-Agenten erstellen eine virtuelle Simulation der individuellen IT-Umgebung, die kontinuierlich mit Daten des Originalobjekts oder -systems aktualisiert wird. In dieser können die Aktivitäten realer Angreifer imitiert und die Risikoexposition in Echtzeit berechnet werden. Dabei lernen die Agenten dynamisch dazu. Auf diese Weise können Sicherheitsverantwortliche ihre Verteidigungsstrategie durch eine unbegrenzte Anzahl von Tests an einer Simulation kontinuierlich validieren und optimieren – ganz ohne Ressourcen des aktiven Security-Systems zu verbrauchen oder Störungen zu verursachen. Dank der durch KI-Agenten gewonnenen Fähigkeit, Aktionen von Angreifern vorherzusehen, können Unternehmen mit einem proaktiven Security-Ansatz schneller sein als ein Angreifer.

Datenkorrelation und -analyse im großen Maßstab

Agentenbasierte KI-Technologie hat zudem das Potenzial, die bekannten Nachteile von SIEM-Lösungen (Security Information and Event Management) zu überwinden: Kosten, Komplexität und eine Flut von Warnmeldungen. Herkömmliche SIEM-Lösungen basieren auf manueller Konfiguration und vordefinierten Parsern, die jedoch mit der Geschwindigkeit und Vielfalt heutiger Datenquellen nicht mehr Schritt halten können. Ein Agentic SIEM kann dank KI-Unterstützung hingegen eigenständig die relevanten Warnmeldungen herausfiltern und reduziert so die Arbeitslast für Security-Analysten. Zudem lassen sich neue Datenquellen und Log-Typen innerhalb von wenigen Tagen oder sogar Stunden integrieren – im Vergleich zu mehreren Monaten bei klassischen SIEM-Lösungen.

Die Zukunft der Cybersicherheit ist proaktiv und KI-gestützt

Während sich Bedrohungslandschaften und IT-Infrastrukturen weiterentwickeln, muss auch die Security Schritt halten. Reaktive Cybersicherheit ist nicht mehr zeitgemäß. Mit einer proaktiven Security-Strategie, die das Potenzial von KI-Agenten ausschöpft, können Unternehmen dagegen Risiken vorausschauend mindern und auch künftige Herausforderungen meistern. Die technologische Basis schafft eine umfassende Cybersecurity-Plattform wie Trend Vision One. Diese führt Security-Daten, -Systeme und -KI-Modelle zusammen und ermöglicht zentrale Steuerung. Das reduziert die Komplexität und schafft umfassende Transparenz über Aktivitäten, Risiken und Bedrohungen in der gesamten IT-Umgebung. •

Cloud Security und Resilienz

in hybriden Unternehmensinfrastrukturen

Die IT-Sicherheitslage hat sich verschärft: Künstliche Intelligenz wird sowohl von Angreifern als auch Verteidigern genutzt. Die EU reagiert mit Gesetzen wie NIS-2 und dem Cyber Resilience Act und Unternehmen setzen zunehmend KI ein. Doch oft fehlt die strategische Einbettung. /// von Hermann Ramacher

DIE BEDROHUNGSLAGE IN DER IT-SECURITY hat sich in den letzten Jahren dramatisch verschärft. KI spielt dabei eine Doppelrolle: Sie wird von Angreifern genutzt, um Phishing-Mails zu perfektionieren oder Schadcode zu generieren – und gleichzeitig von Verteidigern, um Bedrohungen frühzeitig zu erkennen und abzuwehren. Die Europäische Union hat auf die Bedrohungslage mit einer ganzen Reihe von Gesetzen reagiert, darunter die NIS-2-Richtlinie (Network and Information Security Directive 2), die DORA-Verordnung (Digital Operational Resilience Act) und der Cyber Resilience Act (CRA).

Laut dem aktuellen Cisco Cybersecurity Readiness Index 2025 nutzen bereits 86 Prozent der deutschen Unternehmen KI zur Angriffserkennung, 65 Prozent auch für Reaktion und Wiederherstellung. In der Praxis zeigt sich dennoch ein fragmentiertes Bild: Viele Unternehmen setzen KI vorerst nur in Form einzelner Tools oder als Teil von Herstellersuiten, ohne strategische Einbettung ein. Die Integration in bestehende Prozesse, die Schulung der Mitarbeiter und die kontinuierliche Anpassung an neue Bedrohungsszenarien bleiben auf der Strecke, laut KPMG sind erst 44 Prozent der Unternehmen ausreichend aufgestellt.

Schutz in hybriden Welten

Die meisten Unternehmensinfrastrukturen sind heute hybrid oder basieren auf Multi-Cloud-Umgebungen. Das bringt einerseits Flexibilität, andererseits aber auch Komplexität. Besonders im Bereich Sicherheit und Governance stoßen viele IT-Abteilungen an ihre Grenzen, weil die Kombination aus On-Premises-Systemen, Private und Public Clouds die einheitliche Kontrolle und Überwachung erschwert. Unterschiedliche Sicherheitsstandards, fragmentierte Datenbestände und fehlende Schnittstellen erhöhen das Risiko für Sicherheitslücken. Ein umfassendes Schutzkonzept mit modernen Sicherheitsarchitekturen wie Extended Detection and Response (XDR) oder Zero Trust ist vonnöten.

Nach dem Grundsatz „Niemals vertrauen, immer überprüfen“ wird beim Zero Trust Modell jeder Zugriff authentifiziert und autorisiert, wodurch die Angriffsfläche erheblich reduziert wird. Zunehmend wird hier auf KI-gestützte Mechanismen gesetzt, die Nutzerverhalten analysieren, Anomalien erkennen und automatisiert auf verdächtige Aktivitäten reagieren. Zusätzliche Entlastung für Administratoren bringt die Auslagerung von Security-Aufgaben an Managed Service Provider.

Security braucht Technologie und Vertrauen

Die Einführung von KI-gestützten Sicherheitsarchitekturen im Channel ist kein technisches Projekt, sondern eine umfangreiche Transformation einhergehend mit einem kulturellen Wandel. Sie erfordert neue Denkweisen, neue Kompetenzen und neue Partnerschaften. Gerade im Mittelstand, wo Ressourcen knapp und Entscheidungswege oft pragmatisch sind, braucht es Partner, damit KI nicht als abstrakte Zukunftsvision wahrgenommen und Hybridarbeit nicht zur Sicherheitslücke wird. •

> „ Die Einführung von **KI-gestützten** Sicherheitsarchitekturen ist kein technisches Projekt.
>
> *Hermann Ramacher*

DER AUTOR
Hermann Ramacher
ist Geschäftsführer der ADN Distribution GmbH.
Bild: ADN Distribution

Generative KI im Unternehmen nutzen – kontrolliert und sicher!

MIT CLOUD-BASIERTEN GENERATIVEN KI-ANWENDUNGEN WIE CHATGPT KÖNNEN UNTERNEHMEN effizienter, intelligenter und kreativer agieren. Sie profitieren beispielsweise von automatisierter Text- und Code-Generierung, schneller Datenanalyse und intelligentem Wissensmanagement. Die Kehrseite: Prompt- und Nutzungsdaten werden in der Regel an Server in Drittländern übertragen. Das verstößt oft gegen Compliance-Vorgaben, DSGVO und branchenspezifische Sicherheitsstandards – und wirft die Frage auf: Wie lässt sich generative KI sicher, datenschutzkonform und kontrollierbar in der eigenen Organisation nutzen?

Ein praktikabler Ansatz ist ein Zero-Trust-Framework, das generative KI-Modelle lokal hostet, absichert und die kontrollierte Nutzung relevanter Programmierschnittstellen (API) ermöglicht. Der lokale LLM-Betrieb – z.B. als Kombination des Open-Source-Sprachmodells Llama mit dem Inferenz-Framework vLLM – wird dabei über eine mehrschichtige, streng kontrollierte Sicherheitsarchitektur geschützt. Diese Architektur ermöglicht:

- Selektives Bereitstellen von KI-Diensten wie API, Web-Oberfläche, Wissensportal nach außen,
- Authentifizierten, kontextsensitiven Zugriff mit granularen Policies (Device Trust, Identity Federation),
- Strikte Isolation der Anwendung von der Infrastruktur – es wird nur die Anwendungsebene vermittelt, nicht die darunter liegende Infrastruktur,
- Skalierbare, sichere und DSGVO-konforme Nutzung generativer KI über Standortgrenzen hinweg – ohne Kompromisse bei Netzwerk- oder Datensicherheit.

Realisierbar ist die Architektur mit Komponenten des deutschen IT-Security-Spezialisten genua, einem Unternehmen der Bundesdruckerei-Gruppe:

- Als Perimeterschutz agiert die Firewall- und VPN-Appliance genuscreen. Sie schützt vor externen Angriffen, kontrolliert auch verschlüsselte Verbindungen und erlaubt nur definierten Traffic.
- Im internen Netzwerk lässt die Application-Layer-Firewall genugate nur definierte Zugriffe auf Server zu, die vLLM und das Sprachmodell hosten.
- Die Zero-Trust-Application-Access-Lösung genusphere ermöglicht einen kontrollierten Zugriff von außen auf Applikationen. Zugriffsrechte werden kontext-, rollen- und gerätespezifisch vergeben.

Fazit

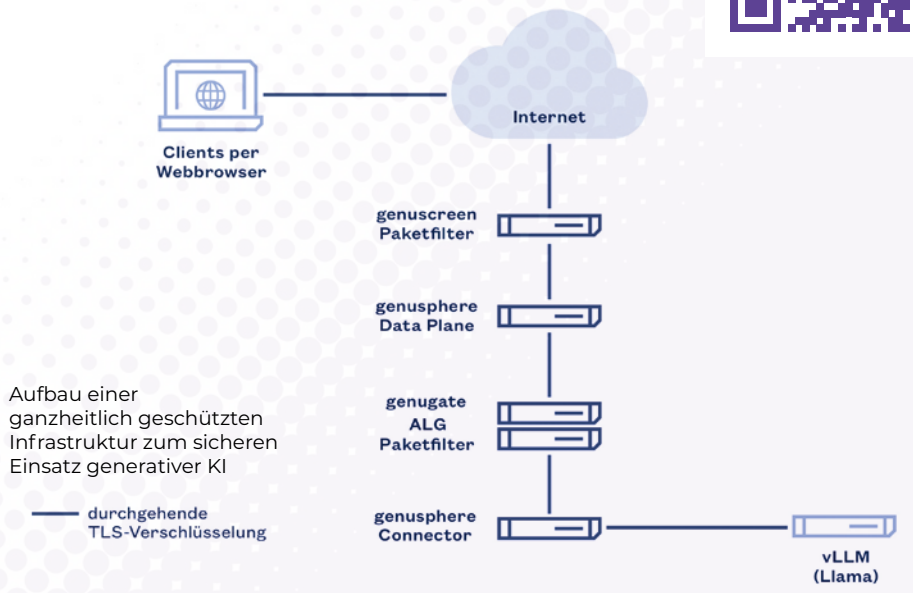
Die Kombination aus lokalem LLM, effizienter Inferenz und mehrschichtigem Zero-Trust-Framework erlaubt es Organisationen, die Chancen moderner KI zu nutzen und zugleich volle Kontrolle über ihre Daten und digitale Zukunft zu behalten.

Sie wollen mehr über Chancen und Risiken moderner KI erfahren?

Im neuen Open-Access-Fachbuch „Künstliche Intelligenz und Wir“ haben Experten von genua, der Bundesdruckerei und zahlreiche weitere namhafte Autorinnen und Autoren aus Wissenschaft und Wirtschaft ihre Fachkompetenz zu einem umfassenden Überblick über den aktuellen Stand und die Zukunft von KI gebündelt. genua sponsert Zugang zum E-Book.

Wie das genau funktioniert, erläutern genuas Experten vom 7. bis 9. Oktober 2025 auf der it-sa

Halle 9, Stand 424



Aufbau einer ganzheitlich geschützten Infrastruktur zum sicheren Einsatz generativer KI

genua.

KI als Angriffswerkzeug: Unternehmen müssen wachsam sein

Die Integration von künstlicher Intelligenz in die Cyberwelt markiert einen fundamentalen Wandel in der Bedrohungslandschaft, der von vielen Beteiligten – insbesondere auf Seite der Unternehmen – immer noch viel zu wenig beachtet wird. KI wird zunehmend von Cyberkriminellen eingesetzt, um Angriffe zu automatisieren, zu skalieren und raffinierter zu gestalten. Zeit zu handeln. /// von Bernd Forstner

BESONDERS BESORGNISERREGEND IST DIE SOGENANNTE „Demokratisierung" hochentwickelter Angriffsmethoden. Was früher spezialisiertes Fachwissen erforderte, wird durch KI-Tools für ein breiteres Spektrum von Akteuren zugänglich. Ein unzufriedener Mitarbeiter aus beispielsweise der Finanzabteilung könnte mithilfe eines Large Language Models (LLM) einfach zu befolgende Anleitungen erhalten, wie man Ransomware im Netzwerk platziert – ohne tiefgreifendes technisches Wissen zu besitzen.

Phishing auf neuem Niveau

Auch die Phishing-Angriffe haben durch KI eine dramatische Entwicklung erfahren. Eine aktuelle Studie zeigt, dass vollautomatisierte Spear-Phishing-Kampagnen, die von LLMs generiert wurden, eine Klickrate von 54 bis 56 Prozent erreichen – vergleichbar mit oder sogar besser als die Ergebnisse menschlicher Experten. Der Phishing Threat Trends Report 2025 prognostiziert, dass 82,6 Prozent aller Phishing-E-Mails in diesem Jahr künstliche Intelligenz nutzen werden. Dabei sind die Zeiten vorbei, in denen man Phishing-E-Mails an Rechtschreib- oder Grammatikfehlern erkennen konnte. KI-generierte Texte sind oft fehlerfrei und sprachlich nuanciert, was die Erkennung durch herkömmliche Spamfilter und sogar durch menschliche Augen extrem erschwert.

Technische Angriffe werden automatisiert

Aber es geht noch weiter: Forschungsprojekte wie HackingBuddyGPT zeigen, dass LLMs in der Lage sind, Unternehmensnetzwerke zu hacken. In simulierten Umgebungen konnten LLMs Schwachstellen ausnutzen, um Accounts zu kompromittieren – und das zu extrem niedrigen Kosten. Die Kosten pro kompromittiertem Domänenkonto liegen bei nur 17,56 US-Dollar in der teuersten Variante.

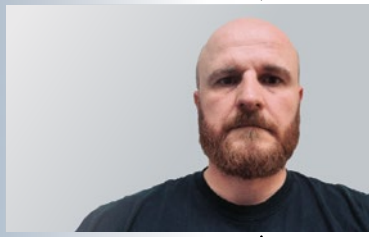
Besonders beunruhigend ist die Fähigkeit der LLMs zur Selbstkorrektur. Wenn ein initialer Exploit fehlschlägt, analysiert das LLM den Fehler, passt seine Strategie an und versucht es erneut. Diese iterative Verbesserung übertrifft die Fähigkeiten vieler automatisierter Scanner.

Handlungsempfehlungen für Unternehmen

Angesichts dieser Entwicklungen müssen Unternehmen ihre Cybersicherheitsstrategien grundlegend verbessern. Dazu gehört:

1. **Verbessertes Security Awareness Training:** Mitarbeiter müssen im Erkennen von KI-generierten Phishing-E-Mails geschult werden. Kritisches Denken und Verifikation ungewöhnlicher Anfragen sind essenziell.
2. **Stärkung technischer Abwehrmechanismen:** Ein robustes Patch- und Schwachstellenmanagement ist wichtiger denn je. Multi-Faktor-Authentifizierung sollte flächendeckend implementiert werden.
3. **Vorbereitung der Incident Response:** Regelmäßige Übungen mit KI-gesteuerten Angriffsszenarien helfen Teams, effektive Reaktionspläne zu entwickeln.

Die Prognose, dass sich die Cybersicherheit bis Anfang 2028 fundamental gewandelt haben wird, ist keine Warnung vor einer fernen Zukunft, sondern beschreibt eine bereits begonnene Transformation, die wahrscheinlich keine drei Jahre brauchen wird. Nur wer heute handelt, kann morgen resilient sein. Es eilt! •



DER AUTOR
Berd Forstner
ist Security Architect bei A1 Digital. Bild: A1 Digital

Künstliche Intelligenz

Darum sind AI Gateways zum Schutz nötig

KI-Agenten benötigen Zugang zu Diensten, Tools und Daten. Aber dieser Zugriff darf nicht unbegrenzt sein. Zur Kontrolle sind API-basierte AI Gateways nötig.

Stephan Schulz, Senior Principal Solutions Engineer bei F5

GESCHÄFTSANWENDUNGEN STELLEN IHRE FUNKTIONEN ÜBER APIS BEREIT. Dabei konsolidieren Gateways API-übergreifende Funktionen wie Benutzerzugriff, Autorisierung und Service-Erkennung. Auch für KI-Agenten sind APIs entscheidend. Denn sie benötigen eine klare Abgrenzung, auf welche Ressourcen sie zugreifen dürfen und welchen Sicherheitskontext sie für jede ihrer Aktionen verwenden sollen.

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

Der KI-Torwächter

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

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

Einfache Einrichtung

Als Bestandteil der F5 Application Delivery and Security Platform ist AI Gateway einfach einzurichten und zu optimieren. Teams können mit minimalem Aufwand Richtlinien erstellen und Erkennungsparameter für verschiedene Umgebungen verfeinern. Erweiterte Erkennungsfunktionen lassen sich mit eingesetzten Sicherheitstools verbinden. So können Analysten schnell Vorfälle korrelieren und automatisierte Reaktionen auslösen.

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

- Kontinuierliche Prüfung und Überwachung des Datenzugriffs und der Datenübertragung in jeder Bereitstellungsumgebung
- Starke Authentifizierung und Autorisierung sowie Berechtigungsverwaltung und rollenbasierte Zugriffskontrolle (RBAC)
- Inline-Bewertung jeder Eingabe und Antwort, die Inhalte sofort blockiert oder redigiert, ohne auf externe Proxys oder Endpunkt-Agenten angewiesen zu sein

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

Besuchen Sie uns gerne auf der it-sa

Halle 7A-531

Sanktionsscreening wird zur Chefsache

Die anstehende Novelle des Außenwirtschafts-Gesetzes (AWG) 2025 bringt neue Anforderungen an die Sanktions-Compliance mit sich. Unternehmen sind künftig stärker gefordert, ihre Prüfprozesse ganzheitlich aufzustellen – insbesondere mit Blick auf Transparenz und Datenqualität. /// von Carsten Ettmann

Neue Vorgaben für die Sanktionsprüfung

Mit der AWG-Novelle 2025 wird die EU-Richtlinie 2024/1226 in deutsches Recht überführt. Ziel ist es, die Umsetzung bestehender Sanktionen wirksamer zu gestalten. Dabei rücken Unternehmen, die geschäftlich mit internationalen Partnern verbunden sind oder Zahlungen ins Ausland tätigen, noch stärker in den Fokus.

Die geplanten Änderungen betreffen nicht nur regulierte Branchen, sondern grundsätzlich jede Organisation, die Geschäftsbeziehungen pflegt. Künftig sollen bestimmte Verstöße gegen Sanktionsvorgaben nicht nur als Ordnungswidrigkeit, sondern als Straftat eingestuft werden. Gleichzeitig wird die mögliche Höhe von Bußgeldern angepasst: Je nach Fall können bis zu 40 Millionen Euro anfallen. Auch juristische Personen, also Unternehmen selbst, können direkt zur Verantwortung gezogen werden.

Beachtenswert ist zudem, dass Unternehmen mit Tochterunternehmen in Embargoländern besonders vorsichtig sein müssen. Verstößt die Tochtergesellschaft gegen eine (für sie nicht geltende) EU-Sanktion, kann dies der europäischen Muttergesellschaft zugerechnet werden. Wenn dabei der Verdacht entsteht, dass die Tochtergesellschaft lediglich genutzt wird, um Sanktionen zu umgehen oder zu verschleiern, besteht die Möglichkeit, dass dies als ein besonders schwerer Fall angenommen wird, für welchen Freiheitsstrafen von bis zu zehn Jahren drohen.

Hinzu kommen neue Ermittlungsinstrumente, etwa durch das Einfrieren von Geldern oder von wirtschaftlichen Ressourcen. Ermittlungen und Vollstreckungen unterliegen künftig verlängerten Fristen. Auf EU-Ebene ist zudem bis zum Jahr 2030 eine umfassende Bewertung der Wirksamkeit dieser Maßnahmen vorgesehen. All dies zeigt: Unternehmen tun gut daran, ihre internen Abläufe zur Sanktionsprüfung sorgfältig zu überprüfen und gegebenenfalls anzupassen.

Sorgfalt bei der Auswahl der Prüfobjekte

Eine häufig unterschätzte Herausforderung besteht darin, zu definieren, wer überhaupt in die Sanktionsprüfung einbezogen werden sollte. In vielen Fällen wird lediglich der direkte Vertragspartner geprüft. Dabei kann es entscheidend sein, auch wirtschaftlich Berechtigte (UBOs), Geschäftsführende, Treuhänder oder sonstige verbundene Personen mit einzubeziehen. Gerade bei komplexen Eigentümerstrukturen oder Konzernverflechtungen kann es vorkommen, dass eine sanktionierte Person mittelbar an einem Unternehmen beteiligt ist. Die sogenannte OFAC 50 Prozent-Regel aus den USA ist ein Beispiel dafür, dass die Prüfung der unmittelbaren Geschäftspartner nicht ausreicht: Hält eine sanktionierte Person mehr als die Hälfte an einem Unternehmen – auch indirekt –, gilt auch dieses als betroffen. Zu beachten ist diesbezüglich, dass die EU eine vergleichbare Regelung kennt – das sogenannte erweiterte Bereitstellungsverbot. Danach gelten ebenfalls solche Unternehmen als sanktioniert, die direkt oder indirekt zu mehr als 50 Prozent im Eigentum gelisteter Personen oder Organisationen stehen.

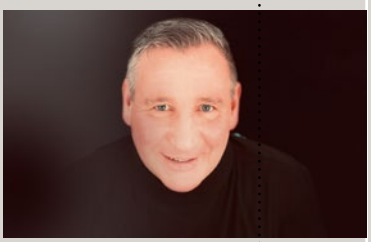
Solche Eigentumsverhältnisse lassen sich ohne verlässliche Datenbasis oft nicht auf den ersten Blick erkennen. Umso wichtiger ist es, über vollständige Informationen zu Beteiligungsverhältnissen und Unternehmensnetzwerken zu verfügen, um die regulatorischen Anforderungen sinnvoll und effektiv umsetzen zu können.

Mehr Klarheit durch EU-weite Harmonisierung

Ein Ziel der Richtlinie 2024/1226 ist es auch, die Umsetzung und Durchsetzung von Sanktionen innerhalb der EU stärker zu vereinheitlichen. Bisher waren die nationalen Systeme sehr unterschiedlich ausgestaltet sowohl in Bezug auf Zuständigkeiten als auch auf Sanktionierungsmaßnahmen und die technische Umsetzung der Prüfungspflichten.

Mit der geplanten Harmonisierung soll nicht nur die Effektivität bestehender Maßnahmen erhöht, sondern auch der Wettbewerb fairer gestaltet werden. Unternehmen profitieren langfristig von mehr Rechtssicherheit, müssen sich allerdings darauf einstellen, dass Prüfpflichten enger gefasst und Kontrollen intensiver werden. Gleichzeitig wird ein grö-

DER AUTOR
Carsten Ettmann
ist Senior Consultant bei Dun & Bradstreet.



ßerer Fokus auf Transparenz gelegt – etwa durch die Forderung, wirtschaftlich Berechtigte eindeutig zu identifizieren und alle Geschäftspartner kontinuierlich zu überwachen.

Insbesondere international tätige Unternehmen sind gut beraten, ihre Prozesse grenzüberschreitend auszurichten. Denn auch außerhalb der EU, etwa in den USA oder im Vereinigten Königreich, gelten teilweise strengere Anforderungen. Wer verschiedene Regelwerke und Listen gleichzeitig im Blick behalten muss, steht schnell vor einer komplexen Herausforderung.

Prozesse auf den Prüfstand stellen

Vor diesem Hintergrund empfiehlt es sich, die bestehenden Prozesse zur Sanktionsprüfung regelmäßig zu hinterfragen. Dabei geht es nicht nur um die technische Umsetzung, sondern auch um organisatorische Fragen: Ist das Screening automatisiert und aktuell? Wird dokumentiert, wann und wen man geprüft hat? Sind auch indirekte Beteiligungen, Gruppenstrukturen oder begünstigte Personen berücksichtigt?

Die Antworten auf diese Fragen entscheiden darüber, wie gut ein Unternehmen auf mögliche Prüfungen durch Aufsichtsbehörden vorbereitet ist und ob es bei Bedarf belastbare Nachweise liefern kann.

Fazit: Strategisch vorsorgen, statt reagieren

Die AWG-Novelle 2025 wird neue Anforderungen bringen – aber auch die Möglichkeit, Compliance-Prozesse zukunftssicher aufzustellen. Sanktionsscreening wird damit zu einem strategischen Thema, das nicht nur rechtliche Vorgaben erfüllt, sondern auch zur Stärkung der eigenen Geschäftsbeziehungen beiträgt.

Wer frühzeitig handelt, schafft nicht nur Sicherheit, sondern kann Prüfungen und Audits gelassen entgegensehen. Eine gute Datenbasis und verlässliche Screening-Prozesse sind dabei der Schlüssel – und eine Investition in nachhaltige Compliance. •

Datenresilienz: Warum das Prinzip den Realitätscheck braucht

In Zeiten zunehmender KI-Einführung und immer neuer gesetzlicher Regularien wissen viele Unternehmen nicht, wie es um die Widerstandsfähigkeit ihrer Daten steht. Wie Unternehmen ihre Datenresilienz durch Selbstkritik und Stresstests mit aktuellen Standards in Einklang bringen können. /// von Dave Russell

JAHRELANG HABEN VIELE UNTERNEHMEN DAS THEMA DATENRESILIENZ auf die lange Bank geschoben. Im Laufe der Zeit hat die Zunahme an Bedrohungen, Vorschriften und Best Practices jedoch die Spielregeln verändert. Datenresilienz steht mittlerweile auf der To-Do-Liste vieler Unternehmen – und das ist auch dringend notwendig. Jetzt, da sich branchenweite Standards verbessert und Unternehmen eine genauere Vorstellung davon haben, worauf sie achten müssen, werden viele von ihnen mit einer unangenehmen Tatsache konfrontiert: Sie sind nicht so gut vorbereitet, wie sie es sein sollten. Der von Veeam gemeinsam mit McKinsey erstellte Bericht über die Datenresilienz in größeren Unternehmen zeigt, dass selbst altbekannte Grundlagen wie „Menschen und Prozesse" regelmäßig als unzureichend eingestuft wurden.

DER AUTOR
Dave Russell
ist Senior Vice President, Head of Strategy bei Veeam Software.
Bild: Veeam Software

> „ Der erste Schritt für jedes Unternehmen mit **einer unterdurchschnittlichen Datenresilienz** sollte darin bestehen, sich ein **genaues Bild vom eigenem Datenprofil** zu machen.
>
> *Dave Russell*

Gleichsetzung von Datenresilienz mit Cybersicherheit

Wie konnte es dazu kommen? Und wie können Unternehmen diese Defizite beheben? Für Entscheidungsträger in den Führungsetagen ist Resilienz vielleicht nicht das spannendste Thema. Obendrein wurde Datenresilienz bisher oft mit der allgemeinen Cybersicherheit gleichgesetzt. Waren Maßnahmen für die IT-Sicherheit implementiert, nahm man einfach an, dass die Daten auch widerstandsfähig gegenüber äußeren (oder inneren) Einflüssen sind. Wie bei den meisten Eventualitäten lässt sich der wahre Wert von Datenresilienz leider erst erkennen, wenn etwas schiefgeht. Abgesehen vom CISO behandeln Geschäftsführer Backup- und Wiederherstellungsprozesse oft wie einen Airbag. Man vergisst, dass er vorhanden ist, bis man in einen Zwischenfall verwickelt wird – und ist dann umso dankbarer, dass er da ist.

Nachdem die Strafverfolgungsbehörden gegen einige der bekanntesten Hacker-Gruppen vorgegangen sind, könnte man annehmen, dass Cyberangriffe insgesamt rückläufig seien. Doch die Realität könnte nicht weiter von dieser Annahme entfernt sein: Im letzten Jahr waren 69 Prozent der befragten Unternehmen mit einem Angriff konfrontiert, wobei 74 Prozent immer noch nicht die Best Practices für die Datenresilienz einhielten. Die Bedrohungslage entwickelt sich ständig weiter: Kleinere Gruppen und neue Akteure füllen schnell Lücken durch aufgedeckte Hacker. Zugleich sind schnellere Angriffsmethoden zur Datenexfiltration auf dem Vormarsch.

Gefordert ist ein kritischer Blick auf die eigene Datenresilienz

Der gleiche Bericht von Veeam in Zusammenarbeit mit McKinsey ergab, dass 74 Prozent der teilnehmenden Unternehmen nicht in der Lage wären, sich schnell und sicher von einer Störung zu erholen. Während Lücken in der Cyberresilienz oft erst bemerkt werden, wenn es bereits zu spät ist, wurden in diesem Fall viele dieser Mängel von den Unternehmen selbst gemeldet. Das wirft die Frage auf: Wenn Unternehmen sich der Probleme bewusst sind, warum schließen sie ihre Lücken dann nicht?

In einigen Fällen könnte es schlicht an der Tatsache liegen, dass sie gerade erst zu dieser Erkenntnis gelangt sind. Neue EU-Vorschriften wie NIS2 und DORA haben das Problem ins Rampenlicht gerückt. Denn sie verlangen von den Unternehmen, ihre Widerstandsfähigkeit in allen Bereichen zu verbessern. Im letzten Jahr mussten diese ihre gesamte Datenresilienz kritisch bewerten, viele zum ersten Mal. Dabei haben sie eine Reihe von unbekannten Schwachstellen aufgedeckt.

Standards für die Datenresilienz bei Einführung neuer Technologien

Unabhängig davon, wie die Unternehmen ihre Lücken erkannt haben, sind sie nicht über Nacht in Rückstand geraten. In vielen Fällen geschah dies schrittweise, da ihre Standards für die Datenresilienz mit der Einführung neuer Technologien und Anwendungen nicht Schritt hielten. Da die meisten Unternehmen KI implementieren, um der Konkurrenz voraus zu sein und ihre Geschäftsprozesse zu optimieren, sind die Auswirkungen auf ihre Datenprofile weitgehend unbemerkt geblieben. Die schiere Menge an Daten, die von diesen Anwendungen benötigt und generiert wird, hat zu ausufernden Datenprofilen geführt. Diese gehen weit über die bestehenden Maßnahmen zur Datenresilienz hinaus.

In Kombination mit einem unzureichenden Verständnis für Datenresilienz ist dies ein Rezept für ein Desaster. Infolgedessen haben sich viele Unternehmen an den falschen Maßstäben gemessen. Standard-Tabletop-Übungen sind ein guter Start, aber Datenresilienz lässt sich nicht auf dem Papier messen. Theoretisch mögen Prozesse funktionieren, im Ernstfall kann es jedoch ganz anders aussehen.

Cyberkriminelle warten nicht auf den Zugriff

Was kommt als Nächstes? Anstatt auf einen Vorfall zu warten, der das Sicherheitskonzept auf die Probe stellt, sollten sich Unternehmen daran gewöhnen, in dauerhafter Bereitschaft auf einen Vorfall zu sein. Das bedeutet, dass Lücken proaktiv aufgedeckt und behoben werden müssen – egal, wie umständlich das sein mag.

Der erste Schritt für jedes Unternehmen mit einer unterdurchschnittlichen Datenresilienz sollte darin bestehen, sich ein genaues Bild vom eigenem Datenprofil zu machen. Sie sollten sich darüber klar werden, über welche Daten sie verfügen, wo sie gespeichert sind und warum sie diese benötigen oder nicht benötigen. Auf diese Weise können sie zumindest einen Teil Ihrer Datenflut reduzieren: indem sie veraltete, redundante oder triviale Daten herausfiltern und sich auf die Sicherung der tatsächlich benötigten Daten konzentrieren.

Doch damit ist die Arbeit noch nicht getan. Sobald neue Maßnahmen zur Datenresilienz eingeführt sind, ist es an der Zeit, sie einem Stresstest zu unterziehen – und das nicht nur einmal. Diese Maßnahmen müssen umfassend getestet werden, um sie bis an ihre Grenzen zu bringen – ganz so wie im echten Leben: Cyberangreifer hören nicht einfach auf, wenn die Systeme ein wenig zu knirschen beginnen und sie werden auch nicht auf den perfekten Zeitpunkt für eine Attacke warten.

Lücken in bestehenden Maßnahmen aufdecken

Deswegen sollte man verschiedene Szenarien durchgehen, in denen wichtige Beteiligte im Urlaub oder die Sicherheitsteams mit anderen Aufgaben beschäftigt sind. So deckt man alle potenziellen Lücken in den bestehenden Maßnahmen auf. Das mag übertrieben erscheinen, doch identifiziert man diese Schwachstellen nicht vorher, erfahren Sicherheitsverantwortliche erst während oder nach einem echten Angriff davon. Es handelt sich zwar um einen erheblichen Arbeitsaufwand, doch Datenresilienz zu erlangen ist es wert. Laut dem Bericht von Veeam verzeichnen Unternehmen mit fortschrittlichen Datenresilienz-Funktionen ein um zehn Prozent höheres jährliches Umsatzwachstum als Mitbewerber, die in diesem Bereich hinterherhinken.

Das bedeutet nicht, dass eine verbesserte Datenresilienz diese Zahlen auf wundersame Weise in die Höhe treibt, aber die Optimierung wird sich zwangsläufig auf die Prozesse im gesamten Unternehmen auswirken. Eins sollten sich CISOs bewusst machen: Cyber-Bedrohungen werden immer komplexer werden und der Daten-Fußabdruck in absehbarer Zeit nicht kleiner. Dies ist ein Problem, mit dem sich jedes Unternehmen auseinandersetzen muss. Deshalb sollte man lieber jetzt ins kalte Wasser springen, bevor man durch einen Cyberangriff von Bord gestoßen wird. •

Cyberangriff?

Keine Panik! – Die neuen Wege im Schutz vor digitalen Risiken

Tim Berghoff, Security Evangelist bei G DATA CyberDefense, erklärt, warum IT-Sicherheit heute vor allem Kontext braucht – und wie Unternehmen mit professioneller Beratung und smarten Lösungen Angreifern immer einen Schritt voraus bleiben. /// von Heiner Sieger

Herr Berghoff, Sie tragen den außergewöhnlichen Titel „Security Evangelist". Was genau sind Ihre Aufgaben und was macht diesen Job für Sie so besonders – und gelegentlich auch herausfordernd beziehungsweise knifflig?
Tim Berghoff | Als Security Evangelist bei G DATA CyberDefense sehe ich meine Hauptaufgabe darin, Kontexte herzustellen und gute Nachrichten zu vermitteln – und das ist in der IT-Security keineswegs selbstverständlich. Ich möchte Zusammenhänge verständlich machen und zeigen, dass viele Schlagzeilen dramatischer klingen, als die Fakten es oft hergeben. Es ist meine Rolle, Orientierung zu bieten und komplexe Entwicklungen einzuordnen, egal ob gegenüber Kunden, der Öffentlichkeit oder auf Konferenzen. Natürlich gibt es Situationen, in denen die Sachlage ernst ist. Trotzdem versuche ich, mit einer gewissen Portion Humor und Gelassenheit an die Thematik heranzugehen.

G DATA kann auf vier Jahrzehnte IT-Sicherheit zurückblicken. Welche Meilensteine in der Entwicklung des Unternehmens waren für Sie besonders prägend und haben auch das Unternehmen geprägt?
TB | G DATA ist seit 40 Jahren ein fester Bestandteil der Branche. Wir haben damals mit dem ersten Virenscanner für den Atari ST begonnen. Seit 2006 konzentrieren wir uns ausschließlich auf IT-Sicherheit. Besonders prägend war für mich die Gründung unserer Tochterfirma G DATA Advanced Analytics, die den Bereich Forensik und Incident Response fokussiert. Unsere Transformation vom produktgetriebenen Anbieter zur Dienstleistungs- und Beratungsexpertise war ein weiterer großer Schritt. Heute bieten wir neben Schutzsoftware auch umfangreiche Beratung, Analysen und Notfallhilfe nach Angriffen an.

Wie hat sich die Bedrohungslage seit den 1980er Jahren verändert? Gibt es Angriffsarten, die heute besonders relevant sind?
TB | Im Kern sind einige Angriffe – wie Ransomware, also die Verschlüsselung von Daten gegen Lösegeld – seit Jahrzehnten bekannt. Bereits in den 1980ern gab es den AIDS-Trojaner, der Lösegeld forderte. Heute aber ist die Bedrohung deutlich professioneller und wirtschaftlich getrieben. Cybercrime ist zu einem professionellen Geschäftszweig geworden, mit Arbeitsteilung und spezialisierten Dienstleistern. Die Szene ist hochgradig spezialisiert; Angriffe erfolgen arbeitsteilig und sind auf maximale Gewinnmaximierung ausgelegt. Die Techniken haben sich weiterentwickelt, das Grundprinzip bleibt aber oft gleich.

Wie gelingt es Ihnen als Security Evangelist, mit der zunehmenden Professionalität der Angreifer Schritt zu halten und welchen Stellenwert hat dabei Beratung?
TB | Wir beobachten tatsächlich ein regelrechtes Wettrüsten. Mal sind wir vorne, mal die Angreifer. Schlaflose Nächte bereitet mir das aber selten, da wir konsequent daran arbeiten, unsere Schutzmaßnahmen zu verbessern und Unternehmen aufzuklären. Beratung ist heute wichtiger denn je: Neben Software bieten wir gezielte Dienstleistungen und Unterstützung an, etwa bei der forensischen Analyse oder im Krisenmanagement nach Angriffen. Für viele kleine und mittelständische Unternehmen wäre es wirtschaftlich kaum möglich, das nötige Spezialwissen intern vorzuhalten. Hier springen wir ein und helfen, tragfähige Sicherheitskonzepte zu entwickeln.

Welche technologischen Innovationen und Dienstleistungen sind bei G DATA entscheidend, um Unternehmen gegen aktuelle Bedrohungen zu schützen?
TB | IT-Abteilungen sehen sich heute mit einer enormen Aufgabenvielfalt konfrontiert: Sie müssen nicht nur für aktuelle Software sorgen, sondern auch eine immer komplexer werdende Sicherheitsarchitektur betreiben. Dieses Spezialwissen ist auf dem Arbeitsmarkt rar. Deshalb bieten wir neben klassischen Schutzlösungen auch „Managed Services" an, wie Incident Response, Forensik und Sicherheitsberatung. Besonders gefragt sind Lösungen, die Unternehmen ohne eigene größere Security-Teams nutzen können. Unser Ziel ist es, Unternehmen handlungsfähig zu halten – auch im Notfall.

In der Cybersecurity werden aktuell viele neue Abkürzungen und Begriffe diskutiert. Welche Rolle spielen moderne Ansätze wie Managed Extended Detection and Response (MXDR)?

DER GESPRÄCHSPARTNER

Tim Berghoff ist seit 2009 bei G DATA CyberDefense und als Security Evangelist ein gefragter Redner, Fachautor und Ansprechpartner für Medien und Unternehmen. Mit Wurzeln im IT-Support und der Produktberatung steht er heute für die strategische Einordnung und Aufklärung komplexer Sicherheitsthemen – mit lebendiger Sprache und stets aktuellem Bezug.

> „ IT-Abteilungen sehen sich heute mit einer enormen Aufgabenvielfalt konfrontiert: Sie müssen nicht nur für aktuelle Software sorgen, sondern auch eine **immer komplexer werdende Sicherheitsarchitektur** betreiben.
>
> *Tim Berghoff*

TB | Klassische Sicherheitslösungen laufen häufig on-premise, das heißt auf eigenen Servern. Sie bieten Schutz, erfordern aber, dass Unternehmen selbst das nötige Know-how zur Auswertung und Reaktion besitzen. Moderne MXDR-Lösungen hingegen werden von spezialisierten Dienstleistern wie unserem Unternehmen gemanagt. Sie analysieren kontinuierlich Protokolle und Angriffsindikatoren. Im Ernstfall greifen Experten ein und leiten Gegenmaßnahmen ein. Gerade für kleinere Unternehmen, die nicht über eigene Sicherheitsanalysten verfügen, ist das ein enormer Vorteil.

Oft heißt es, die größte Schwachstelle bei Cyberangriffen auf Unternehmen seien die Mitarbeiterinnen und Mitarbeiter. Wie schätzen Sie den Faktor Mensch in der IT-Sicherheit ein und welche Rolle spielen Awareness-Trainings?

TB | Der Mensch ist tatsächlich ein entscheidender Faktor. Zwar versuchen Unternehmen, Risiken durch Automatisierung zu minimieren, doch viele Angriffe setzen gezielt auf menschliches Fehlverhalten. Daher ist es wichtig, Mitarbeitende laufend zu schulen und zu sensibilisieren. Einmalige Schulungen reichen nicht aus; wir setzen auf kontinuierliche, interaktive und praxisnahe Awareness-Programme. Nur so kann das Sicherheitsniveau nachhaltig angehoben werden. Die Rückmeldungen, die wir daraus gewinnen, fließen in die ständige Verbesserung unserer Trainings ein.

Werfen wir noch einen Blick in die Zukunft: Die Cybersecurity-Branche steht vor einem ständigen Wandel. Welche Trends und Herausforderungen sehen Sie für die nächsten Jahre? Wie wird sich G DATA weiterentwickeln?

TB | KI ist sicherlich eines der wichtigsten Themen der nächsten Jahre. Sie eröffnet beeindruckende neue Möglichkeiten, stellt uns aber auch vor völlig neue Herausforderungen. Wir entwickeln zum Beispiel Trainings, die gezielt auf Angriffsszenarien mit KI eingehen. Hinzu kommen gesetzliche Vorgaben wie die NIS2-Richtlinie der EU, die die Anforderungen an Unternehmen weiter verschärfen wird. G DATA wird sich weiter anpassen, um seinen Kunden schnell und effizient helfen zu können. Konkrete Zukunftsprognosen sind aber schwer zu treffen, da sich die Bedrohungslage ständig und teils völlig überraschend verändert. Flexibilität und schnelle Reaktion werden deshalb noch wichtiger.

Herr Berghoff, was geben Sie Unternehmen abschließend mit auf den Weg?

TB | Ganz viel im Bereich IT Sicherheit braucht Kontext und den Kontext zu finden, das ist halt nicht immer leicht. Dazu gibt es ein sehr schönes Zitat von dem von mir sehr geschätzten Bochumer Kabarettisten Jochen Malmsheimer, der mal gesagt hat: „Hören Sie neben das Laute: Lassen Sie sich nicht vom Geklingel und Geschepper aus der ersten Reihe ablenken und schauen Sie auch mal in die zweite Reihe."

Mein Tipp: Vertrauen Sie auf professionelle Unterstützung und stellen Sie Ihr Sicherheitskonzept regelmäßig auf den Prüfstand. •

Vorstand, übernehmen Sie!

Kathrin Redlich, Vice President DACH & CEE bei Rubrik, erklärt, warum IT-Sicherheit Chefsache sein muss, wie Unternehmen widerstandsfähig gegen Cyberangriffe werden und nur schnelles Handeln das Schlimmste verhindert. /// von Heiner Sieger

Für Viren und Cyberangriffe waren viele Jahre meist die „Haus-Tekkies“ zuständig. Wie verändert die aktuelle Flut und Raffinesse der Attacken die Rolle der IT-Sicherheit auf der Managementebene?

Kathrin Redlich | Die Unternehmen müssen sich heute stärker denn je darauf einstellen, angegriffen zu werden. 94 Prozent der deutschen IT- und Sicherheitsverantwortlichen hatten im vergangenen Jahr mit Cyberangriffen zu kämpfen – das ist mehr als der weltweite Durchschnitt (90,7 Prozent). Erschreckenderweise meldete 1 von 5 Unternehmen in Deutschland mehr als 100 Angriffe, die höchste Rate weltweit.

Entscheidend ist, vorbereitet zu sein, um Schäden möglichst gering zu halten und den Geschäftsbetrieb schnellstmöglich wiederherzustellen. Dies setzt einen „assumed-breach“-Denkansatz voraus: Demnach sind Angriffe keine Frage des Ob, sondern des Wann und Wie. Unternehmen, die das verstanden haben, sehen IT als einen zentralen Business Enabler, der jetzt fest in der obersten Führungsebene angesiedelt ist. Cybersecurity betrifft das gesamte Unternehmen und ist damit zum Vorstandsthema geworden. Der CEO muss wissen, wie sicher das Unternehmen ist, welches Risiko besteht und welche Folgen ein Angriff haben könnte. Ebenso muss er verstehen, welche Maßnahmen im Ernstfall zu ergreifen sind, und entsprechende Szenarien vorbereiten. Hier ist er auf die Expertise des CIO oder CISOs angewiesen.

Rubrik hat den Fokus von klassischem Backup auf Cyber-Resilienz verschoben. Was waren die Auslöser für diesen Strategiewechsel und wie reagieren Ihre Kunden darauf?

KR | Schon unser Mitbegründer und heutige CEO Bipul Sinha hat immer betont, dass es nicht nur um Backup geht. So war Cyberresilienz von Anfang an Teil der Rubrik-DNA. Heute ist die Bedrohungslage mit zunehmenden Ransomware-Attacken nun völlig anders. Da kommen die integrierten Security- und Resilience-Lösungen noch mehr zum Tragen, damit Unternehmen nach einem Vorfall handlungsfähig bleiben.

Der CIO muss beispielsweise wissen, welche Daten verschlüsselt wurden und wann der letzte Zeitpunkt war, an dem die Daten noch sauber waren. Unsere Lösung Turbo Threat Hunting kann das rasch herausfinden. Ein wichtiger Aspekt ist auch, welche sensiblen Daten betroffen sind und ob sie exfiltriert wurden. Dies macht das Opfer im Zweifel erpressbar und kann sogar zu Strafen führen.

DIE GESPRÄCHSPARTNERIN

Kathrin Redlich

ist seit Februar 2024 Vice President DACH & CEE (Deutschland, Österreich, Schweiz und Zentral-/Osteuropa) beim Cybersecurity- und Backup-Spezialisten Rubrik. In dieser Führungsposition verantwortet sie das Wachstum und die strategische Weiterentwicklung des Unternehmens in der Region.

> „ Der CEO muss wissen, wie sicher das Unternehmen ist, welches Risiko besteht und **welche Folgen ein Angriff haben könnte.** Ebenso muss er verstehen, welche Maßnahmen im Ernstfall zu ergreifen sind, und entsprechende Szenarien vorbereiten.
>
> *Kathrin Redlich*

Sie betonen, dass Cyber-Resilienz nicht nur ein IT-Thema, sondern Aufgabe des gesamten Unternehmens ist. Wie gelingt es Ihnen, die Security Cloud in allen Unternehmensbereichen Ihrer Kunden zu verankern?
KR | In der Regel starten wir über die IT-Infrastruktur, machen aber sehr früh deutlich, dass auch der Sicherheitsverantwortliche am Tisch sitzen sollte. Gerade heute, wenn hybride Multi-Cloud-Umgebungen Standard sind, müssen Infrastruktur und Security zusammengedacht werden.

Wann holen Sie dann den CISO oder sogar den CEO mit an Bord?
KR | Im ersten Schritt versuchen wir, ein Verständnis für die Situation zu bekommen; wir evaluieren gemeinsam die Anforderungen und Herausforderungen. Mit diesem konsolidierten Blick gehen wir dann ins Gespräch mit der Geschäftsleitung und gleichen unsere Perspektiven ab. Dies ist meist nach dem vierten bis fünften Meeting der Fall. Hier steht dann vor allem die Sicherstellung des fortlaufenden Geschäftsbetriebs im Fokus.

Welche aktuellen Cybersecurity-Trends beobachten Sie im DACH-Raum und wie begegnet Rubrik den steigenden Bedrohungen durch Cyberangriffe?
KR | Der aktuelle Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Deutschland belegt: Die Zahl der Angriffe steigt rasant. Ein Indikator dafür ist die Polizeiliche Kriminalstatistik (PKS), die 131.391 in Deutschland verübte Cybercrime-Fälle für das Jahr 2024 ausweist. Bei weiteren 201.877 Straftaten handelt es sich um Auslandstaten, die vom Ausland oder einem unbekannten Ort aus verübt wurden. In Deutschland werden die Schäden von Bitkom mittlerweile auf rund 178,8 Milliarden Euro geschätzt – das sind 30 Milliarden mehr als im Vorjahr, und es handelt sich dabei nur um die gemeldeten Fälle.

Die fortschreitende digitale Vernetzung verstärkt dieses Problem, darüber hinaus sind die Angriffe zunehmend organisiert und teils politisch motiviert. Crime-as-a-Service ist eine immer größere Herausforderung. Besonders im Fokus stehen Ransomware und Phishing. Unser Ansatz ist, eine Balance zwischen Prävention und effizienter Wiederherstellung zu schaffen. Mit unseren interaktiven „Save-the-Data"-Workshops und Drehbüchern simulieren wir realistische Angriffsszenarien gemeinsam mit den Kundenverantwortlichen.

Viele Unternehmen fürchten Datenverlust und lange Ausfallzeiten nach einem Angriff. Welche Lösungen können eine schnelle Wiederherstellung und Geschäftskontinuität gewährleisten?
KR | Die Rubrik Security Cloud bietet ein besonders sicheres Backup, das nicht manipulierbar, nicht löschbar und nicht auffindbar ist – alles basiert auf Zero-Trust-Prinzipien. Ergänzend bieten wir Funktionen wie Ransomware-Investigation, Threat-Hunting, Erkennung sensibler Daten und orchestrierte Wiederherstellung. Das Ziel ist immer, Kunden schnellstmöglich wieder handlungsfähig zu machen, indem wir den saubersten Wiederherstellungspunkt identifizieren und nutzen. Letztlich geht es um zwei Fragen: Welche Daten und Applikationen sind betroffen, und wo liegt der letzte sichere und saubere Speicherpunkt?

Wie nutzen Ihre Lösungen künstliche Intelligenz oder Automatisierung, um Cyberangriffe frühzeitig zu erkennen und abzuwehren?
KR | Wir erforschen kontinuierlich Möglichkeiten, KI zu nutzen, um innovativ zu sein und beste Ergebnisse für unsere Kunden zu liefern. Künstliche Intelligenz und Machine Learning sind daher seit längerem in unsere Lösungen integriert. Im Ernstfall unterstützt KI die IT-Security-Teams bei der schnellen Suche nach dem letzten sauberen Backup und bei der Bedrohungserkennung.

Der generative KI-Chat-Begleiter „Ruby" etwas ist in der schon erwähnten Security Cloud integriert. Ruby nutzt generative KI, basierend auf Microsoft Azure OpenAI, sowie eine Data Threat Engine, die Maschinelles Lernen verwendet, um Cybervorfälle zu entdecken, zu untersuchen, zu beheben und zu dokumentieren. In der „Rubrik AI-Powered Cyber Recovery" kann generative KI eingesetzt werden, um nach einem Cyberangriff die richtigen Entscheidungen für eine schnelle und sichere Wiederherstellung zu treffen. Die Lösung bietet geführte Workflows und Aufgabenlisten, um Datenverluste zu minimieren und Ausfallzeiten zu reduzieren. Besonders für virtuelle Maschinen werden so effiziente und resiliente Wiederherstellungsprozesse ermöglicht, die Unternehmen helfen, auch bei komplexen Angriffen schnell wieder arbeitsfähig zu sein.

An welchen Innovationen oder neuen Lösungen arbeitet Rubrik, um die Cyber-Resilienz der Kunden weiter zu stärken?
KR | Ein aktueller Schwerpunkt ist das Thema Identity: Wenn das Active Directory, also die zentrale Nutzerverwaltung, kompromittiert wird, steht das Unternehmen still. Wir sorgen dafür, dass Unternehmen auch in diesem Szenario schnell wieder arbeitsfähig sind. Und zwar über unsere neue Sicherheitslösung Identity Resilience. Diese Lösung wurde entwickelt, um die gesamte Identitätslandschaft umfassend zu schützen. Identity Resilience sichert gezielt die häufigsten Angriffsvektoren ab, darunter sowohl menschliche als auch nicht-menschliche Identitäten, und unterstützt Unternehmen dabei, ihren Geschäftsbetrieb mit minimalen Ausfallzeiten aufrechtzuerhalten. Das Besondere daran: Identity Resilience adressiert einen kritischen blinden Fleck in der Sicherheitsarchitektur moderner Unternehmen. Die Nutzer-Authentifizierung ist ein zentraler Bestandteil der IT-Infrastruktur. Sie wird von der großen Mehrheit der Unternehmen genutzt – und bleibt ein konstant attraktives Ziel für Angreifer. Wird ein Identitätssystem kompromittiert, erhalten Angreifer Zugang zu kritischen Daten und Anmeldeinformationen – dadurch kann sogar eine Wiederherstellung nach einem Cyberangriff verhindert werden. •

KI ist mehr als nur ein NICE-TO-HAVE

Schwachstellen- und Patch-Management sind essenziell für die Cybersicherheit von Unternehmen. Allerdings sind beide mit einem hohen Aufwand für IT-Verantwortliche verbunden. Künstliche Intelligenz kann hier Abhilfe schaffen. /// von Andre Schindler

IN EINER AKTUELLEN STUDIE DES PONEMON INSTITUTE WURDEN UNTERNEHMEN BEFRAGT, die Datenverletzungen im Zusammenhang mit Cyberangriffen zu verzeichnen hatten: 60 Prozemt gaben an, dass sie diese auf eine bekannte, nicht gepatchte Schwachstelle zurückführen konnten. Ein solides Patch-Management kann dazu beitragen, viele Cyberangriffe abzuwehren. Für viele Unternehmen bleibt diese mühsame und zeitaufwändige Aufgabe jedoch eine Herausforderung.

Künstliche Intelligenz kann zur Lösung dieser Herausforderung beitragen, indem sie IT-Teams dabei unterstützt, den Patch-Prozess zu automatisieren und zu vereinfachen. Dennoch sollten Unternehmen ein Gleichgewicht finden, wenn es darum geht, sich auf die Fähigkeiten KI-basierter Tools zu verlassen. Der Einsatz von KI ist nicht immer vorteilhafter als der Einsatz traditioneller Methoden, sondern sollte vielmehr als Ergänzung betrachtet werden. Menschen sollten bei allen Entscheidungen immer das letzte Wort haben.

Intelligentes Patching für mehr Effizienz und Sicherheit

Um ihre Erfolgsquote zu verbessern, sind IT-Teams darauf bedacht, den manuellen Recherche- und Interventionsaufwand zu reduzieren, der bei herkömmlichen Patches erforderlich ist. KI-gestützte Lösungen übernehmen Routineaufgaben, priorisieren Risiken auf der Grundlage von Daten und reagieren auf die wachsende Zahl von Bedrohungen. Dadurch verringert sich der manuelle Zeitaufwand für Patches erheblich. Diese automatisierten Lösungen können einen echten Wettbewerbsvorteil darstellen, insbesondere für Unternehmen, die ein hohes

DER AUTOR
Andre Schindler
ist GM EMEA and SVP Global Sales bei NinjaOne.
Bild: NinjaOne

> „ KI-gestützte Lösungen übernehmen Routineaufgaben, priorisieren Risiken auf der Grundlage von Daten und reagieren auf die wachsende Zahl von Bedrohungen.
>
> *Andre Schindler*

Maß an Flexibilität und Skalierbarkeit benötigen. Mit dem Aufkommen und der Verbesserung dieser neuen Technologien wird das Patchen einfacher und effektiver.

Ein Beispiel hierfür ist die Datenanalyse in modernen KI-basierten Anwendungen. Diese priorisiert Patches nach ihrem Risikograd und empfiehlt geeignete Sicherheitsverbesserungen. Damit müssen IT-Abteilungen nicht mehr jedes Update manuell recherchieren oder testen, was den Zeitaufwand für diese Aufgabe drastisch senkt. KI-Tools, die Patches anhand von Stimmungen analysieren, können noch einen Schritt weiter gehen und enorme Datenmengen im Zusammenhang mit Software-Updates verarbeiten. Dies schließt auch historische Patch-Performance, bekannte Kompatibilitätsprobleme, Auswirkungen auf das System sowie Meinungen und Feedback von Benutzern ein. Anhand dieser Daten können die Tools optimale Patch-Strategien empfehlen. Mit diesen Strategien können Unternehmen nicht nur hochriskante Bedrohungen mit potenziell sehr negativen Folgen bekämpfen, sondern auch Ausfallzeiten und durch fehlerhafte und gefährliche Patches verursachte Produktivitätsprobleme vermeiden. Der Einsatz von KI-basierten Patching-Tools unterstützt IT-Abteilungen dabei, Situationen sicherer einzuschätzen und fundiertere Entscheidungen zu treffen.

Proaktive Sicherheitsstrategien

Zur Ergänzung einer optimalen Patch-Verwaltung können Unternehmen auch auf geeignete, effizientere KI-Lösungen für das Schwachstellenmanagement zurückgreifen. Ein KI-Tool für das Schwachstellenmanagement kann Systeme und Endpunkte kontinuierlich auf Bedrohungen scannen, potenzielle Angriffsvektoren vorhersagen und Sicherheitsverbesserungen empfehlen.

KI-gestützte Systeme erkennen nicht nur fehlende Updates, sondern können auch veraltete Softwareversionen identifizieren, unnötige Anwendungen entfernen und Konfigurationen automatisch optimieren.

Darüber hinaus kann KI aus riesigen Datenmengen Muster und Trends erkennen und subtile Anomalien aufspüren, die auf eine zukünftige Sicherheitsverletzung hindeuten könnten. Die Technologie verbessert auch die Erkennung von Bedrohungen, indem sie globale Bedrohungsdaten analysiert und Echtzeitdaten austauscht. Diese kollektive Intelligenz hilft Unternehmen, einen besseren Schutz vor neuen und sich weiterentwickelnden Bedrohungen aufzubauen.

Insgesamt kann künstliche Intelligenz dazu beitragen, die Angriffsfläche eines Unternehmens zu verringern. Dieses Maß an Cybersicherheit lässt sich mit herkömmlichen Sicherheitsmethoden allein nur schwer erreichen.

Die Vorteile nutzen

Durch die frühzeitige Integration von KI in eine Cybersicherheitsstrategie können Unternehmen die Vorteile der KI optimal nutzen. Es handelt sich zwar nicht um eine Wunderwaffe, aber durch die sorgfältige Auswahl der Technologie für relevante Anwendungsfälle wie risikobasiertes Patching oder Schwachstellenscans lassen sich der Zeitaufwand für manuelle Aufgaben senken, Entscheidungen besser fundieren und insgesamt die Arbeit von IT- und Sicherheitsteams erheblich erleichtern. Dennoch ist es wichtig, diese Verbesserungen mit menschlichem Instinkt und Fachwissen in Einklang zu bringen. KI sollte als Partner fungieren, der hilft, Lücken zu schließen und Effizienzsteigerungen zu erzielen, aber sie ist nicht dazu gedacht, IT- und Sicherheitsexperten bei der Entscheidungsfindung und der Umsetzung dieser Entscheidungen zu ersetzen.

Mit der Weiterentwicklung der Technologie werden Unternehmen von mühsamen und manuellen Aufgaben entlastet, aber die IT-Mitarbeiter werden nicht verschwinden. Sie werden lediglich mehr Zeit haben, sich strategischer und zielgerichteter mit dem Ausbau der allgemeinen Cybersicherheit und Resilienz zu befassen. •

PATCH-MANAGEMENT IN UNTERNEHMEN

Patch Management ist ein strukturierte Prozess, bei dem Software-Updates, Sicherheits-Patches und Firmware-Updates systematisch verwaltet und angewendet werden.

In der Praxis geht es beim Patch-Management darum, die Cybersicherheit mit den betrieblichen Anforderungen des Unternehmens in Einklang zu bringen. Hacker können Schwachstellen in der IT-Umgebung eines Unternehmens ausnutzen, um Cyberangriffe zu starten und Malware zu verbreiten. Anbieter veröffentlichen Updates, sogenannte Patches, um diese Schwachstellen zu beheben.

Cybervorfälle:
Fünf Schritte zu einer wirksamen Incident Response

Ein neuer Report von Arctic Wolf deckt eine gefährliche Schieflage auf: Viele Unternehmen verfügen zwar über einen Incident-Response-Retainer, aber nicht über einen passenden IR-Plan für die nötige Reaktionsfähigkeit im Ernstfall. Fünf Schritte zu einem effizienten Incident-Response-Plan. /// von Stefan Girschner

LAUT DEM „TRENDS REPORT 2025" VON ARCTIC WOLF und Sapio Research haben 88 Prozent der befragten Unternehmen einen Incident-Response-Retainer abgeschlossen. Allerdings verfügen nur 35 Prozent über einen getesteten Incident-Response-Plan. Die Mehrzahl investiert also in Ressourcen, ohne die organisatorische Grundlage dafür geschaffen zu haben. Ein Risiko, das im Ernstfall nicht nur Zeit kostet, sondern auch Kontrolle. Die Lücke zwischen Retainer und Readiness bei Incident Response ist dabei nicht nur eine Formalität, denn 81 Prozent der Unternehmen mit Retainer mussten diesen im vergangenen Jahr aktivieren. Fehlt die nötige Vorbereitung, verlaufen gerade die ersten Stunden und Tage oft unstrukturiert.

Zudem kann der externe Security-Dienstleister nicht sofort eingreifen, sondern ist zunächst auf Zuarbeit durch das angegriffene Unternehmen angewiesen. Dabei sind Cybervorfälle längst kein Ausnahmefall mehr, sondern Teil des operativen Alltags. Umso wichtiger ist es, dass Prozesse, Verantwortlichkeiten und Entscheidungswege im Vorfeld definiert und geprobt sind. Folgende fünf Schritte führen zu einem wirksamen Incident-Response-Plan:

1. **Ein Plan ist kein „PDF", sondern ein Prozess**
   Ein IR-Plan ist mehr als ein Dokument auf dem Server. Er definiert konkrete Rollen, Eskalationspfade und Entscheidungsbefugnisse. Er berücksichtigt externe Partner wie forensische Dienstleister, Versicherer oder Behörden, interne Schnittstellen sowie Kommunikationskanäle – auch für den Fall eines Ausfalls der Infrastruktur.

2. **Aktualität ist entscheidend**
   Laut dem Report wurde nur bei 59 Prozent der vorhandenen IR-Pläne im letzten Jahr ein Review durchgeführt – ein deutlicher Rückgang gegenüber dem Vorjahr (83 Prozent). Doch Personalstrukturen, Verantwortlichkeiten und IT-Architekturen verändern sich kontinuierlich. Ein nicht geprüfter IR-Plan birgt das Risiko, im Ernstfall an falsche Zuständigkeiten, alte Kontaktlisten oder irrelevante Systeme anzuknüpfen.

3. **Technologie ist Mittel und nicht Mittelpunkt**
   Maßnahmen wie EDR, SIEM oder Forensik sind wichtige Bausteine in der IR. Doch sie ersetzen keine vordefinierten Abläufe. Ein Beispiel: Laut dem Report hatten über die Hälfte der Unternehmen, die 2024 von einem signifikanten Angriff betroffen waren, kein funktionierendes Multi-Faktor-Authentifizierungsverfahren implementiert. Fehlende Grundschutzmaßnahmen verzögern die Erkennung und erschweren auch die Eindämmung.

4. **Übungen offenbaren die Realität**
   Ein effektiver Weg, die Einsatzfähigkeit eines IR-Plans zu bewerten, sind realistische Übungen. Tabletop-Szenarien oder simulierte Phishing-Angriffe zeigen schnell, wo Prozesse abbrechen, Schnittstellen fehlen oder Verantwortlichkeiten unklar sind. Unternehmen, die solche Tests regelmäßig durchführen, sind nicht nur schneller – sie erkennen auch besser, wann externe Hilfe tatsächlich notwendig ist.

5. **Integration ist der Schlüssel zur effektiven Incident Response**
   Ein IR-Plan darf kein Fremdkörper im Unternehmen sein. Er muss zu bestehenden Business-Continuity-Plänen, Sicherheitsarchitekturen und Versicherungsverträgen passen. Wer Incident Response isoliert betrachtet, läuft sonst Gefahr, Entscheidungen auf unsicherem Fundament zu treffen. •

„Ein Incident-Response-Plan ist kein Notnagel für den Ernstfall, sondern **Teil des normalen Betriebsrisikomanagements.** Organisationen, die sich allein auf einen Retainer verlassen, verlieren wertvolle Zeit – und im Zweifel ihre Handlungsfähigkeit. Deshalb unterstützen wir Unternehmen bei der **Entwicklung einsatzfähiger Response-Pläne.**"

Dr. Sebastian Schmerl, VP Security Services EMEA bei Arctic Wolf

Bild: Arctic Wolf

Von Check zu Schutz – mit System:

IT-Sicherheit, die wirklich wirkt

Cyberangriffe sind Alltag. Phishing, Ransomware, Identitätsdiebstahl und unsichere Cloud-Konfigurationen bedrohen Unternehmen jeder Größe – und die Angreifer werden immer raffinierter. Die Digitalisierung bringt enorme Chancen, aber auch neue Risiken: Wer heute für die Sicherheit seiner Daten und Systeme verantwortlich ist, steht vor der Herausforderung, die richtigen Maßnahmen zu wählen und dabei weder Zeit noch Budget zu verschwenden.

Die Realität: Eine Sicherheitsillusion.
Oft werden Schwachstellen übersehen, weil die IT-Landschaft komplex ist und die Ressourcen knapp sind. Die Folge: Angreifer finden Einfallstore, die im Tagesgeschäft untergehen – und der Schaden ist schnell enorm.

ADLONs Antwort: Security-Checks mit System.
Statt auf Einzelmaßnahmen oder teure Dauerprojekte zu setzen, bietet ADLON fünf modulare Security-Checks, die gezielt die größten Risiken adressieren – von E-Mail über Berechtigungen bis hin zu Phishing-Simulationen. Das System ist einfach: Jeder Check liefert einen klaren, unabhängigen Statusbericht und konkrete, verständliche Handlungsempfehlungen. Unternehmen profitieren von sofortigem Überblick, klaren To-Dos und Audit-Readiness – ohne Fachchinesisch.

Die fünf Security-Checks im Überblick:

E-Mail Security Check:
Schützt vor Phishing, Spoofing und unsicheren Konfigurationen.
Entra ID Permission Check:
Minimiert Risiken durch überflüssige oder veraltete Berechtigungen.
M365 Security Check:
Prüft die Microsoft-Umgebung auf Schwachstellen und Compliance.
Tenant Basis Check:
Sichert die Grundkonfiguration gegen gefährliche Defaults ab.
Phishing Simulation:
Testet realistisch, wie gut Mitarbeitende auf Angriffe vorbereitet sind.

Warum ist das für Entscheider relevant?
- Sofort Klarheit über die tatsächliche Sicherheitslage
- Gezieltes und effizientes Handeln ohne lange Projekte
- Erfüllung von Compliance-Anforderungen und Audit-Readiness
- Stärkung der Security-Kultur und Sensibilisierung der Mitarbeitenden

Das Besondere:
Jeder Check ist einzeln buchbar – oder als Kombi-Check. Die Umsetzung der Empfehlungen kann intern erfolgen oder mit ADLON als Partner. So bleibt die Kontrolle im Unternehmen und die Investition planbar.

Stets gut informiert: Security Webinare und Newsletter

IT-Sicherheit erfordert kontinuierliche Awareness! Mit dem ADLON Security Newsletter und den kostenlosen Security Webinaren bleiben Sie und Ihr Team immer auf dem neuesten Stand:
- Aktuelle Bedrohungen und Trends
- Praxisnahe Tipps und Handlungsempfehlungen
- Direkter Austausch mit Experten

Rechtzeitig zu den Webinaren anmelden:
adlon.de/events

Jetzt abonnieren:
adlon.de/newsletter

ADLON – Ihr Partner für Security am digitalen Arbeitsplatz

ADLON Intelligent Solutions GmbH ist der führende Anbieter für Security am digitalen Arbeitsplatz und spezialisiert auf Microsoft-Technologien.

- Über 35 Jahre Erfahrung in IT, Digital Workplace und IT-Security
- Zertifizierte Experten, BSI-Standards, zahlreiche Referenzen
- Lösungen für Mittelstand und Großunternehmen
- Fokus: Microsoft 365, Cloud, Identitäten, Awareness und Managed Security Services

Sie möchten **mehr** wissen?

Autor/Ansprechpartner:
ADLON Intelligent Solutions GmbH
Tizian Kohler, Head of Security
Albersfelder Straße 30
88213 Ravensburg
Tizian.Kohler@adlon.de
www.adlon.de

adlon
Empowering Business with IT

Das Hase- und Igel-Spiel

Egal, ob es noch fünf oder zehn Jahre bis zum sogenannten „Q-Day“ sind, klar ist: Der Wettlauf zwischen Angriff und Verteidigung, zwischen Hase und Igel, hat längst begonnen. Quantentechnologien sind keine Science-Fiction – sie bedrohen gängige aktuelle kryptografische Verfahren und damit die Sicherheit von IT-Systemen und Daten. Klarer Vorsprung für den Hasen. Noch. /// von Frank Morgner

DERZEIT SCHON DREHEN IT-SICHERHEITSFACHLEUTE IN UNTERNEHMEN und Organisationen sprichwörtlich jeden Stein um: Sie sind auf der Suche, wo und wie sie kryptographische Verfahren einsetzen und welche Systeme besonders anfällig für einen quantenbasierten Angriff wären, etwa bei Datenverschlüsselung, bei digitalen Zertifikaten, digitale Signaturen, Authentifizierungsverfahren und geschützten Kommunikationskanälen.

Auch das Gegenmittel für den Q-Day, die quantensichere Verschlüsselung, klingt für viele Menschen noch immer nach ferner Zukunft, dabei arbeiten Kryptografen schon seit mehr als 20 Jahren an solchen quantenresistenten Alternativen. Mittlerweile werden diese von etlichen Usern bereits täglich genutzt – meist unbewusst: Wer mit Messenger-Diensten wie WhatsApp oder Signal kommuniziert, tut dies quantensicher; gleiches gilt für Webbrowser wie Chrome oder Firefox. Laut dem Internetdienstleister Cloudflare ist bereits über ein Drittel des weltweiten User-generierten Internet-Contents quantenkryptografisch abgesichert. Mit anderen Worten: Die „Post-Quantum-Kryptografie“ (PQC) ist längst im Alltag angekommen, der Igel holt auf.

Sicherheitsanforderungen für die Ära des Quantencomputing

Die Bundesdruckerei-Gruppe beschäftigt sich seit vielen Jahren in verschiedenen Forschungsprojekten mit PQC, um digitale Identitäten und sensible Daten auch in einer Zukunft mit Quantencomputern zu schützen. In der Innovationabteilung konzentrieren sich über ein Dutzend Mitarbeitende ganz auf Quantentechnologien und schlagen die Brücke zwischen Forschung und Anwendungen für die Praxis. Als Technologieunternehmen des Bundes schaffen wir die nötige Infrastruktur für die Migration auf PQC, ohne dass User den Umstieg merken: im Finanzsektor oder Gesundheitssektor, bei elektronischen Zertifikaten und Signaturen, bei der Absicherung von Netzwerken oder bei digitalen Identitäten im Reisepass.

Mit der Infineon Technologies AG und dem Fraunhofer-Institut für Angewandte und integrierte Sicherheit hat die Bundesdruckerei bereits vor einigen Jahren den weltweit ersten Demonstrator für einen elektronischen Pass entwickelt, der auch die hohen Sicherheitsanforderungen für die Ära des Quantencomputing erfüllt. Auch eine Quantencomputer-sichere Public-Key-Infrastruktur (PKI), die als Prototyp im Testbetrieb läuft, wurde bereits entwickelt. PKI sind die Grundlage jeglicher digitalen Kommunikation. Wenn den Usern beim Surfen auf einer Website in der Adresszeilen ein Schloss angezeigt wird, wissen sie: Diese Webseite ist vertrauenswürdig. Die mithilfe dieser PKI ausgestellten und geprüften digitalen Zertifikate könnten zukünftig als Grundstein dienen für die sichere Identifikation von Organisationen und Personen im Quantenzeitalter sowie für quantensichere Kommunikationsverschlüsselung und -authentisierung.

DER AUTOR
Frank Morgner
ist Senior Innovation Developer bei der Bundesdruckerei GmbH.

> „ Wichtig beim Migrationsprozess auf quantenresistente Kryptografie: Angesichts des hohen Aufwands sollte neu integrierte Kryptografie gleich so angelegt werden, dass spätere Anpassungen einfacher sind. Das **Zauberwort** lautet: **Kryptoagilität**.
>
> *Frank Morgner*

Erste standardisierte quantenresistente Algorithmen liegen vor

Da das Feld der Quanten- und Post-Quanten-Technologien sehr dynamisch ist, wird die Standardisierung dieser neuen Verfahren umso wichtiger: auf nationaler wie internationaler Ebene. Zwar herrscht weiterhin viel Bewegung bei der Standardisierung und den regulatorischen Vorgaben; seit Ende 2024 liegen immerhin erste standardisierte quantenresistente Algorithmen vor. Diese gilt es, möglichst schnell weiträumig einzusetzen. Hase und Igel gleichauf?

Wichtig beim Migrationsprozess auf quantenresistente Kryptografie: Angesichts des hohen Aufwands sollte neu integrierte Kryptografie gleich so angelegt werden, dass spätere Anpassungen einfacher sind. Das Zauberwort lautet: Kryptoagilität – also die Möglichkeit, auch zukünftig Verschlüsselungen im System leicht tauschen zu können. Denn Methoden, die für morgen als sicher gelten, könnten übermorgen schon wieder gefährdet sein. Wenn wir jetzt so viel austauschen müssen, machen wir es am besten gleich so, dass es in Zukunft leichter geht.

Neue Verteidigungsansätze im Hase- und Igel-Spiel machen sich die Quantenmechanik selbst zunutze, um Kryptografie abzusichern. Vereinfacht gesagt: Der Verteidiger schlägt den Angreifer mit seinen eigenen Waffen. Diese neuen Verschlüsselungsverfahren basieren nicht auf mathematischen Problemen, sondern auf physikalischen Eigenschaften der Quantenmechanik.

Die nächste Generation der digitalen Sicherheit schaffen

Ein Beispiel ist die Technologie hinter dem sogenannten Quanten-Schlüsselaustausch: Bei der quantenbasierten Verteilung von Schlüsseln an Kommunikationsparteien (englisch: „Quantum Key Distribution“, QKD) bricht die Verbindung ab, sobald bemerkt wird, dass ein Dritter die Schlüssel abzugreifen versucht. Durch quantenmechanische Effekte wird also eine abhörsichere Kommunikation ermöglicht. Angriffe könnten so nicht nur entdeckt, sondern auch charakterisiert und letztlich bekämpft werden.

Auch bei QKD gilt: Die vermeintlich ferne Zukunft ist schon recht nah. Ende 2024 fand das zweite Schlüsselexperiment des QuNET-Projekts statt: Fraunhofer Heinrich-Hertz-Institut, Deutsche Telekom und Bundesdruckerei GmbH testeten quantensichere Kommunikation erstmals über ein breites Netzwerk mit mehreren Parteien. Dabei zeigten sie, wie dank einer durch Quantenschlüsselaustausch abgesicherten Verbindung sensible Daten – etwa Ausweisdaten – sicher ausgetauscht werden können.

In Kombination mit Post-Quanten-Kryptographie könnte die Quantenkommunikation langfristig als zusätzliche Sicherheitsschicht eingesetzt werden. So kann die nächste Generation der digitalen Sicherheit geschaffen werden. Der Igel hat gute Chancen, am Ende zu gewinnen – wie im Märchen. •

Im Visier der Unsichtbaren

Wie KI die Cybersicherheit verändert

Die nächste Welle der Cyberangriffe ist KI-gestützt – und die Abwehr auch. Doch mit der richtigen KI-Strategie bleiben Unternehmen immer einen Schritt voraus. IT-Security-Profi Richard Werner* von TrendMicro erklärt, mit welchen Maßnahmen sie das schaffen.

/// von Heiner Sieger

Herr Werner, Sie sind seit einem Vierteljahrhundert im Bereich Cybersecurity tätig. Welche Rolle spielt künstliche Intelligenz (KI) in der heutigen IT-Sicherheit und wie hat sie sich entwickelt?

Richard Werner | Künstliche Intelligenz ist längst ein fester Bestandteil der Cybersecurity. Kaum ein Produkt kommt heute noch ohne KI aus. Besonders spannend ist der Wandel durch Technologien wie ChatGPT oder Large Language Models (LLMs). Sie ermöglichen es, riesige Datenmengen, etwa aus Bedrohungsinformationen, effizienter zu analysieren und die Ergebnisse in verständliche Handlungsempfehlungen für Unternehmen zu übersetzen. Diese Automatisierung und Kontextualisierung machen unsere Abwehrmaßnahmen präziser und menschennaher denn je.

DER GESPRÄCHSPARTNER
Richard Werner
ist Cybersecurity Platform Lead für Europa bei Trend Micro und bringt über 25 Jahre Erfahrung in der IT-Sicherheitsbranche mit. Er berät Unternehmen im Aufbau zukunftsfähiger Cybersecurity-Strategien und ist als Experte regelmäßig in Fachmedien präsent.

> „Noch schöpfen die Cyberkriminellen die technischen Potenziale von KI nicht voll aus, weil sie mit bestehenden Methoden bereits erfolgreich sind. Doch sobald klassische Angriffe weniger gewinnbringend werden, **ist zu erwarten, dass KI-gestützte Methoden stark zunehmen** – dann wird die Bedrohungslage noch komplexer.
>
> *Richard Werner*

Inzwischen gibt es KI-Agenten, die nicht nur Bedrohungen erkennen, sondern auch eigenständig Maßnahmen einleiten können. Wie funktionieren diese Systeme konkret und wie zuverlässig sind sie im Vergleich zum Menschen?

RW | KI-Agenten sind spezialisierte, selbstlernende Systeme. Sie werden für definierte Aufgabenfelder trainiert und agieren eigenständig innerhalb festgelegter Grenzen. Ihre Stärke liegt in der Schnelligkeit: Sie analysieren Datenströme, erkennen Muster und können – sofern erlaubt – direkt Gegenmaßnahmen einleiten, um einen Angriff abzuwehren. Im Vergleich zum Menschen punkten sie mit Reaktionsgeschwindigkeit und der Fähigkeit, emotionale Faktoren auszublenden. In vergleichbaren Situationen treffen sie in etwa 99 Prozent der Fälle bessere und schnellere Entscheidungen als menschliche Analysten, auch wenn sie – wie beim autonomen Fahren – nie unfehlbar sind. Es bleibt stets ein kleiner Restbereich, in dem menschliches Urteilsvermögen überlegen ist.

Wo sehen Sie aktuell die größten Risiken im Zusammenhang mit KI, insbesondere was Manipulierbarkeit und Transparenz betrifft? Wie begegnen Sie bei TrendMicro diesen Herausforderungen?

RW | Die Manipulierbarkeit von KI ist ein zentraler Punkt. Ein Beispiel ist das sogenannte Prompt Engineering: Mit

gezielten Eingaben kann man eine KI zu falschen Ergebnissen verleiten. Auch die Manipulation von Trainingsdaten stellt ein Risiko dar. Um dem zu begegnen, legen wir bei Trend Micro großen Wert auf Transparenz. Zugänge werden klar geregelt, Berechtigungen genau definiert und die Herkunft der Daten überprüft. Wir setzen zudem auf Open-Source-Ansätze, damit die Community Schwachstellen schneller erkennt und Gegenmaßnahmen entwickelt werden können. So kann beispielsweise schnell nachvollzogen werden, welche Eingaben eine KI beeinflussen und ob sie vertrauenswürdig sind. Letztlich ist keine KI perfekt; sie muss lernen, auch eigene Fehleinschätzungen zu erkennen und zu korrigieren.

Einige Studien warnen, dass KI selbst zur Gefahr werden kann, etwa wenn sie von Angreifern manipuliert wird. Wie schützt TrendMicro sich und seine Kunden davor, dass eigene KI-Systeme nicht selbst zum Risiko werden?
RW | Sicherheit für die KI ist genauso wichtig wie Sicherheit durch KI. Das beginnt bei der Entwicklung: Nur klar autorisierte Personen dürfen Trainingsdaten einspielen oder Änderungen am System vornehmen. Wir steuern sehr genau, wer auf welche Teile der KI zugreifen kann. Der Schutz vor Manipulation steht dabei im Fokus. Selbstlernende Systeme, die sich autonom weiterentwickeln, sind aktuell noch selten – werden aber intensiv erforscht. Bis dahin bleibt die Kontrolle über Trainingsdaten und Entwicklungsprozesse der Schlüssel, um Missbrauch zu verhindern.

KI ist aber nicht nur ein Verteidigungswerkzeug. Wie nutzen Cyberkriminelle diese Technologie inzwischen – und was bedeutet das für die Unternehmen?
RW | KI ist längst auch ein Werkzeug der Angreifer. Rund 90 bis 95 Prozent aller Attacken auf deutsche Unternehmen werden von Kriminellen durchgeführt. Die meisten nutzen KI bisher vor allem, um ihre Methoden zu optimieren: Phishing-Mails werden glaubhafter, Social-Engineering-Attacken zielsicherer. Entscheidend ist die Fähigkeit von KI, große Datenmengen auszuwerten – etwa gehackte E-Mail-Postfächer oder Social-Media-Profile. Damit lassen sich Angriffe deutlich gezielter und effektiver durchführen. Noch schöpfen die Cyberkriminellen die technischen Potenziale von KI nicht voll aus, weil sie mit bestehenden Methoden bereits erfolgreich sind. Doch sobald klassische Angriffe weniger gewinnbringend werden, ist zu erwarten, dass KI-gestützte Methoden stark zunehmen – dann wird die Bedrohungslage noch komplexer.

Spitzt sich das Wettrennen zwischen Angreifern und Verteidigern durch den Einsatz von KI weiter zu? Wer ist da Ihrer Einschätzung nach im Vorteil?
RW | Das ist ein klassisches Katz-und-Maus-Spiel. Verteidigungsmaßnahmen werden von Angreifern sofort auf Schwachstellen getestet. Ein Beispiel: Schulungen gegen Phishing sind heute Standard, bieten gegen KI-optimierte Angriffe aber bald keinen ausreichenden Schutz mehr, insbesondere bei gezielten Attacken. Unternehmen müssen deshalb immer wieder neue Strategien entwickeln und Backup-Maßnahmen vorhalten, falls eine Verteidigung versagt. Angesichts des Mangels an IT-Fachkräften wird KI für die Verteidigungsseite unverzichtbar, um mit dem Tempo und der Vielfalt der Bedrohungen Schritt zu halten.

Was raten Sie Unternehmen: Benötigt jedes Unternehmen eine eigene KI-Cybersecurity-Strategie? Und worauf sollten sie achten, wenn KI-Anwendungen selbst entwickelt und eingesetzt werden?
RW | Jedes Unternehmen, das auf IT angewiesen ist, braucht eine durchdachte Cybersecurity-Strategie – Großunternehmen haben solche Konzepte längst, aber auch Mittelständler ziehen nach. Entscheidend ist, den Wert der eigenen Daten und Systeme zu erkennen und entsprechende Schutzmechanismen zu etablieren – vergleichbar mit einem Werkschutz in der physischen Welt. Im Falle von KI bedeutet das auch, die gesetzlichen Rahmenbedingungen wie den EU AI Act zu beachten: Welche Daten werden verarbeitet? Dürfen personenbezogene Daten in die KI eingespeist werden? Wer hat intern Zugriff auf die Systeme und kann Eingaben machen?

Für kleinere Unternehmen empfiehlt sich die Zusammenarbeit mit spezialisierten Servicepartnern, da das erforderliche Know-how und Personal oft fehlen. Auch wenn Unternehmen KI-Anwendungen wie ChatGPT nutzen, müssen sie regeln, welche Daten dort verarbeitet werden dürfen – etwa keine sensiblen Mitarbeiter- oder Kundendaten auf offenen Plattformen preisgeben.

Wie lässt sich verhindern, dass Interna oder sensible Daten bei der Entwicklung oder Nutzung von KI unbeabsichtigt abfließen oder missbraucht werden?
RW | Hier kommt es auf klare Zugriffsregelungen und technische Schutzmechanismen an. Es muss genau definiert werden, wer auf die KI-Systeme zugreifen darf und welche Daten verarbeitet werden. Bei offenen Plattformen besteht die Gefahr, dass Angreifer versuchen, sensible Daten herauszuziehen. Unternehmen sollten daher ausschließlich nicht-sensible Informationen dort einsetzen und zusätzliche Sicherheitsmaßnahmen wie Verschlüsselung oder Zugriffsbeschränkungen implementieren.

Haben Sie zum Abschluss noch eine Botschaft, die Sie jenen Unternehmen mit auf den Weg geben möchten, die über den Einsatz von KI in der IT-Sicherheit nachdenken?
RW | Mein Appell: Denken Sie Security von Anfang an mit. Bei früheren Technologietrends wie der Cloud wurde die Sicherheit oft nachträglich eingebaut – mit hohen Kosten und Problemen. Beim Thema KI sollten Sie aus diesen Fehlern lernen: Berücksichtigen Sie Risiken, holen Sie sich Expertenrat und bauen Sie Sicherheit bereits in die ersten Schritte Ihrer KI-Projekte ein. Das erspart Ihnen später massive Aufwände und schützt Ihr Unternehmen effektiver vor Angriffen. •

Sicherheit als Türöffner

Die NIS-2-Richtlinie bringt einen Paradigmenwechsel. Großunternehmen müssen ihre Lieferkette digital prüfen – und erwarten klare Nachweise. Für kleine IT-Dienstleister bedeutet das: Informationssicherheit wird zum entscheidenden Wettbewerbsfaktor für Wachstum und Kundenzugang. /// von Dr. Jens-Uwe Meyer

VORAUSSICHTLICH ENDE 2025 WIRD DAS GESETZ zur Umsetzung der europäischen NIS-2-Richtlinie verabschiedet – und unmittelbar in Kraft treten. Damit beginnt für die deutsche Wirtschaft ein neues Kapitel der Informationssicherheit. Während viele Schlagzeilen sich auf Konzerne und große kritische Infrastrukturen konzentrieren, zeigt sich schnell: Besonders betroffen sind kleine IT-Dienstleister und Softwareunternehmen. Sie geraten in den Fokus, weil ihre Leistungen ein entscheidender Bestandteil der digitalen Lieferkette sind.

Für sie bedeutet NIS-2 ein neues Zeitalter: Kunden werden Nachweise verlangen, Risiken in Verträgen absichern und Audits durchführen. Wer als Dienstleister darauf nicht vorbereitet ist, riskiert nicht nur einzelne Aufträge, sondern den dauerhaften Zugang zu wichtigen Kunden.

NIS-2: Was haben kleine IT-Dienstleister und Softwareunternehmen damit zu tun?

Die NIS-2-Richtlinie richtet sich in erster Linie an größere Unternehmen. Betroffen sind Branchen wie Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Lebensmittelproduktion, Gesundheit, Wasser- und Abfallwirtschaft sowie digitale Infrastruktur. Maßgeblich ist dabei die Unternehmensgröße: Bereits ab 50 Mitarbeitenden oder 10 Millionen Euro Jahresumsatz greift die volle Verantwortung.

Doch die wenigsten dieser Unternehmen erbringen ihre IT-Leistungen vollständig selbst. Rechenzentren, IT-Administration, Support, Softwareentwicklung oder sogar die Pflege von Webseiten sind fast immer an externe Dienstleister ausgelagert. Auch Standard- und Individualsoftware wird überwiegend eingekauft. Damit verlagert sich ein Teil der Verantwortung entlang der Lieferkette – und betrifft indirekt kleine und mittelständische IT-Dienstleister.

Die Geschäftsführung dieser größeren Kunden haftet künftig persönlich dafür, dass Risiken in der digitalen Lieferkette überwacht und kontrolliert werden. Entsprechend verlangen sie Nachweise von ihren Zulieferern. Genau deshalb bezeichnen viele Experten NIS-2 bereits als das „Lieferkettengesetz der Digitalbranche".

Was kommt auf kleine IT-Unternehmen jetzt zu?

Mit Inkrafttreten der nationalen Umsetzung werden die Pflichten klar umrissen sein. Kleine IT-Dienstleister müssen künftig:

- Vertragliche Zusicherungen abgeben, dass sie Informationssicherheitsmaßnahmen eingeführt haben.
- Eigene Risiken systematisch überwachen, dokumentieren und regelmäßig bewerten.
- Nachweise erbringen, dass definierte Sicherheitsprozesse auch tatsächlich eingehalten werden.
- Kontrollen durch Kunden akzeptieren, etwa in Form von Lieferantenaudits oder Fragebögen.

DER AUTOR
Dr. Jens-Uwe Meyer
ist Vorstand des Zertifizierungsinstituts DICIS.

Das bedeutet: Informationssicherheit wird vom Randthema zum festen Bestandteil von Vertragsverhandlungen, Projekten und Kundenbeziehungen.

Wie können sich kleine IT-Dienstleistungsunternehmen darauf vorbereiten?

Die Ausgangssituation ist eindeutig: Kunden sind verpflichtet, ihre digitale Lieferkette zu überprüfen. Viele Auftraggeber werden in den kommenden Monaten systematische Prüfprozesse aufbauen – und dabei nach klaren Standards fragen. Ein praxiserprobter Handlungsleitfaden ist die internationale Norm ISO 27001. Sie beschreibt, wie Informationssicherheit strukturiert und nachvollziehbar im Unternehmen umgesetzt werden kann. Entscheidend ist: ISO 27001 ist zertifizierbar. Unternehmen, die sich nach diesem Standard auditieren lassen, können gegenüber Kunden einen objektiven Nachweis erbringen, dass sie NIS-2-konform arbeiten.

Die zentralen Anforderungen sind:

- Einführung eines systematischen Risikomanagements, das Bedrohungen identifiziert und bewertet.
- Erstellung von Notfallplänen, um auf Sicherheitsvorfälle vorbereitet zu sein.
- Sensibilisierung und Schulung der Mitarbeitenden, damit Informationssicherheit gelebt wird.
- Regelmäßige interne Kontrollen (Audits), um die Wirksamkeit zu überprüfen.

Der Aufwand ist flexibel skalierbar: Von schlanken, digitalen Lösungen, die in wenigen Tagen implementiert werden können, bis hin zu komplexen Projekten über mehrere Monate. Gerade kleine Unternehmen profitieren von pragmatischen, digitalen Ansätzen. Moderne KI-Tools helfen dabei, den Dokumentationsaufwand massiv zu reduzieren und die Prozesse effizient zu gestalten.

> „ Für kleine IT-Dienstleister und Softwareunternehmen bedeutet NIS-2 ein neues Zeitalter: Kunden werden **Nachweise verlangen, Risiken in Verträgen absichern und Audits durchführen**. Wer als Dienstleister darauf nicht vorbereitet ist, riskiert nicht nur einzelne Aufträge, sondern den dauerhaften Zugang zu wichtigen Kunden.
>
> *Dr. Jens-Uwe Meyer*

Eine Zertifizierung ist zwar nicht gesetzlich vorgeschrieben, sie wird aber schnell zu einem starken Wettbewerbsvorteil. Denn Großunternehmen werden sich auf Dienstleister konzentrieren, die die neue Regulierung ernst nehmen. Kleine IT-Unternehmen, die diesen Schritt nicht gehen, laufen Gefahr, bei größeren Ausschreibungen systematisch ausgeschlossen zu werden.

Wie groß ist der Aufwand für eine Zertifizierung nach ISO 27001?

Viele Geschäftsführer kleiner Unternehmen fragen sich: „Wie sollen wir das stemmen?“ Die gute Nachricht: Eine ISO-27001-Zertifizierung ist weniger bürokratisch, als oft angenommen wird. Zunächst bedeutet die Norm, bestehende Maßnahmen zu systematisieren und zu dokumentieren. Viele kleine IT-Dienstleister haben längst gute Sicherheitsroutinen – etwa Backups, Passwortregeln oder Notfallpläne. Diese müssen jedoch nachvollziehbar verschriftlicht und in ein Gesamtsystem eingebettet werden.

NIS-2: Für kleine Dienstleistungsunternehmen mehr Chance als Risiko

Auf den ersten Blick wirkt NIS-2 wie eine zusätzliche Belastung. Tatsächlich eröffnet es kleinen IT-Dienstleistern und Softwareunternehmen aber große Chancen:

- Stärkere Kundenbindung: Wer seine Informationssicherheit nachweislich im Griff hat, wird zum verlässlichen Partner.
- Besserer Marktzugang: Viele Großkunden werden künftig nur noch zertifizierte Partner berücksichtigen.
- Wettbewerbsvorteile: Während unvorbereitete Wettbewerber unter Druck geraten, können proaktive Unternehmen wachsen.

NIS-2 verändert die Spielregeln in der Digitalbranche grundlegend. Kleine IT-Dienstleister, die sich frühzeitig vorbereiten, verwandeln regulatorischen Druck in einen klaren Marktvorteil. Informationssicherheit ist damit nicht nur Pflicht, sondern ein Schlüssel zu Wachstum und Stabilität. •

Cybersicherheit ist eine Frage der Haltung – nicht nur der Technik

Cybersicherheit wird in vielen Unternehmen noch immer als rein technisches Problem behandelt – ein Fehler, ist Jana-Irina Luley von Dell Technologies überzeugt. IT-Sicherheit ist vielmehr der strategische Hebel für Resilienz und Wettbewerbsfähigkeit von Unternehmen. /// von Jana-Irina Luley

DIE AUTORIN
Jana-Irina Luley
ist Senior Director & General Manager Enterprise Private bei Dell Technologies Deutschland.
Bild: Dell

IN VIELEN UNTERNEHMEN WIRD CYBERSICHERHEIT noch immer wie ein klassisches IT-Problem behandelt – operativ, technisch und punktuell. Doch diese Sichtweise greift zu kurz, denn in einer zunehmend vernetzten, KI-beschleunigten Wirtschaft ist IT-Sicherheit längst nicht mehr nur ein dringend notwendiger Schutzmechanismus.

Cybersicherheit ist vielmehr der strategische Hebel für wirtschaftliche Resilienz, für eine vertrauensvolle Beziehung mit den Stakeholdern und letztlich auch für mehr Wettbewerbsfähigkeit. Trotzdem fehlt ihr in vielen Organisationen genau das, was sie bräuchte: ein klares Mandat, eine strukturelle Verankerung im Top-Management und damit eine Entscheidungsgewalt.

Im Spannungsfeld zwischen widersprüchlichen Interessen

Oft sieht die Realität jedoch anders aus. Wer Verantwortung für Cybersicherheit trägt, steht im Spannungsfeld zwischen widersprüchlichen Interessen. Ein zusätzlicher Sicherheitstest? Zu teuer, sagt das Controlling. Granulare Rechtevergabe? Zu umständlich, meint die IT. Netzwerkrestriktionen für sensible Bereiche? Ein Affront gegenüber der Belegschaft und damit ein Risiko fürs Betriebsklima, findet das Management.

Kurzum:
Businessziele werden gegen Sicherheitsanforderungen, Benutzerkomfort gegen Risikominimierung und Innovationsdrang gegen Kontrollbedarf abgewogen. Studien wie die Digital Trust Insights 2025 von PwC zeigen: Nur 44 Prozent der deutschen Befragten trauen ihrer eigenen Führungsriege beim Thema Cybersecurity echte Durchschlagskraft zu. Und gerade einmal 35 Prozent der CISOs in deutschen Unternehmen sind aktiv an Infrastruktur- und Technologieentscheidungen beteiligt.

Cybersicherheit muss Bestandteil der Wertschöpfung werden

Die unbequeme Wahrheit ist, dass es in vielen Unternehmen den Posten des CISO nicht einmal gibt. Und wenn doch, dann ist dieser mehr Mahner als Entscheider. Damit bleibt seine Schlagkraft begrenzt, wie die PwC-Studie belegt. Häufig hat er nicht einmal ein eigenes Budget, keine direkte Berichtslinie ans Top-Management und kaum Einfluss auf Projektentscheidungen oder Geschäftsstrategien. Der „Security-Verantwortliche" darf zwar Hinweise geben, aber er darf nichts stoppen – schon gar nicht, wenn ein Geschäftsbereich ein neues Tool schnell live bringen will. Damit bleibt Cybersicherheit ein Parallelprozess statt integraler Bestandteil der unternehmerischen Wertschöpfung.

Diese Entkopplung ist gefährlich, denn die Bedrohungslage ist längst nicht mehr nur hypothetisch. Im Gegenteil: Künstliche Intelligenz eröffnet Angriffsflächen, die bis vor Kurzem unvorstellbar waren – von perfekt gemachten Phishing-Mails über täuschend echte Deepfakes bis hin zu komplett automatisierten Penetrationstools. Gleichzeitig geraten Lieferketten, Produktionssysteme und kritische Infrastrukturen zunehmend ins Visier professioneller Angreifer. Die Gefahr ist real und betrifft jedes Unternehmen unabhängig von der Größe.

Wer heute eine Firma führt, muss Sicherheit strategisch denken. Das bedeutet: klare Verantwortlichkeiten, echte Entscheidungskompetenz und ein Platz auf Augenhöhe mit anderen C-Level-Funktionen. Nicht jeder Betrieb braucht einen formellen CISO. Aber jeder Betrieb braucht jemanden, der die Gefahren nicht nur kennt, sondern auch stoppen darf – und zwar rechtzeitig, bevor aus technischen Risiken ein wirtschaftlicher Schaden entsteht. •

Abonnieren Sie den
WIN-verlagsübergreifenden

KI Newsletter!

Bleiben Sie auf dem Laufenden mit den neuesten Entwicklungen und Trends aus der Welt der Künstlichen Intelligenz. Unser kostenfreier Newsletter vom WIN-Verlag wird monatlich versendet und bietet Ihnen spannende Einblicke, exklusive Inhalte und Expertenmeinungen der verschiedenen Branchen.

Melden Sie sich jetzt an und verpassen Sie keine Ausgabe!

Bild: ipopba/AdobeStock

win-verlag.de

WIN VERLAG

TAROX

FOKUS IST KEIN TREND. SONDERN STRATEGIE.

Wir sind dabei – live in Halle 6 / 6-441.

Besuchen Sie uns auf der it-sa 2025 in Nürnberg. Wir freuen uns auf spannende Gespräche und frische Impulse.

#TAROXITSA2025

it sa
HOME OF IT SECURITY

tarox.de