Verlagsbeilage Oktober 2025

‹kes›

Die Zeitschrift für Informations-Sicherheit

Special

Special mit Leseprobe aus dem ‹kes› Hauptheft

it-sa 2025

Trends, Produkte, Lösungen

DATAKONTEXT

MYRA

Die Welt ist unsicher genug.

Ihre IT-Infrastruktur muss es nicht sein.

Vertrauen Sie auf über 10 Jahre Erfahrung im professionellen Schutz von Behörden: Die hochzertifizierten Lösungen von Myra verteidigen kritische Dienste effizient und DSGVO-konform gegen bösartigen Webtraffic, Datendiebstahl und Manipulation.

Unsere Standards für Ihre Sicherheit:

ISO 27001 BSI zertifiziert
auf der Basis von IT-Grundschutz
Zertifikat Nr.: BSI-IGZ-0667-2024

PCI DSS Certified

BSIG
KRITIS-qualifiziert

BSI C5
TESTAT TYP 2

Trusted Cloud
SERVICE

CERTIFIED
IDW PS 951
ISAE 3402

KRITIS
Nachweis gemäß
§ 8a. Abs. 3 BSIG

CERTIFIED
ISO
9001:2015
COMPANY

www.myrasecurity.com

Inhalt

Bild: Pete/stock.adobe.com

Verzahnte Security-Strategien

Wie integrierte Führungs- und Technikstrukturen Cybersicherheit nachhaltig stärken

Fehlende Abstimmung zwischen Sicherheitstechnik und Governance-Strukturen schwächt die Cybersicherheit vieler Organisationen. Besonders die Schnittstellen zwischen Technologie, Management und Unternehmensprozessen weisen kritische Lücken auf, die Angreifer ausnutzen können.

Von Tim Cappelmann, AirITSystems GmbH

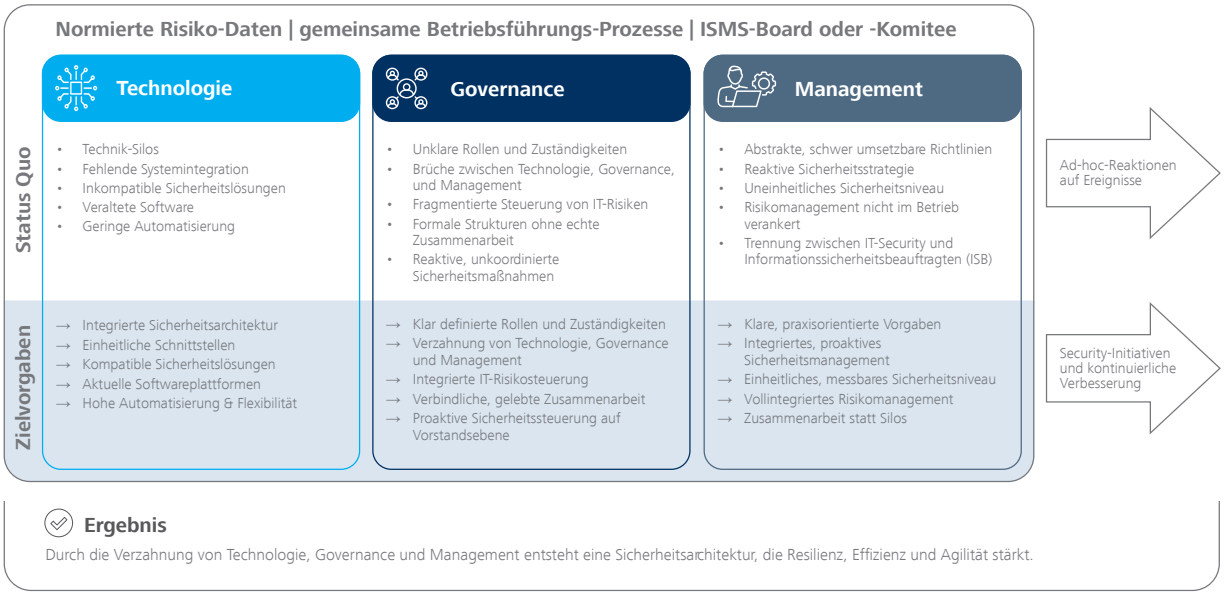
Noch immer arbeiten viele Organisationen in Cybersecurity-Technik-Silos. Über die Jahre haben sich Technologie-Stacks entwickelt, getrieben von Bedrohungslagen, Innovationen und Zufällen. Diese bilden bis heute die Grundlage für Erkennung und Reaktion auf Cybervorfälle.

„Historisch gewachsen" erklärt zwar Ineffizienzen, doch tatsächlich entstehen viele Probleme, weil technische Security-Lösungen kein konsistentes Ökosystem bilden. Zu viele Brüche behindern Automatisierung und erschweren die flexible Anpassung an neue Bedrohungen. Diese fehlende Integration erzeugt „horizontale Systembrüche" innerhalb derselben Sicherheitsschicht.

Mit Blick auf nachhaltige Effekte prägt der Security-Spezialist AirITSystems den Begriff der „vertikalen Systembrüche": strukturelle Lücken zwischen Security-Technologien, Managementsystemen und geschäftskritischen Prozessen. Sie entstehen dort, wo Technologie-Stack, Betriebsführung und IT-Governance eigentlich ineinandergreifen sollten und führen zu ineffizientem Budgeteinsatz, falschen Prioritäten und Ressourcenknappheit in der proaktiven Cyberabwehr.

Die Symptome dieses strukturellen Problems sind deutlich:

- Richtlinien des Informationssicherheitsbeauftragten (ISB) erscheinen technischen Spezialisten oft zu abstrakt und schwer umsetzbar.
- Security-Maßnahmen werden meist reaktiv implementiert, statt von Projektbeginn an integriert.
- Das Sicherheitsniveau ist uneinheitlich: Während die Perimetersicherung oft stark ausgebaut ist, bleibt die Cloud-Absicherung schwach.
- Methodisches Risikomanagement ist im operativen IT-Betrieb häufig nicht ausreichend verankert.
- Fehlende Architekturstandards und unklare Steuerung führen zu horizontalen Systembrüchen in Security-Technologien.



Verzahnte Security-Strategien: Strukturelle Herausforderungen erkennen und proaktiv lösen (Bild: AirITSystems GmbH)

Die Ursachen liegen häufig in der organisatorischen IT-Struktur. Vertikale Systembrüche deuten auf ungelöste Führungsfragen hin.

Sicherheitsmanagement im Elfenbeinturm

Die Verantwortlichen für IT-Security agieren häufig zu isoliert vom Beauftragtenwesen. Dadurch entstehen oft komplexe Informationssicherheits-Managementsysteme (ISMS), in denen Verantwortliche in einem kontinuierlichen Verbesserungsprozess die Sicherheit vermeintlich erhöhen, ohne IT-Security-Experten und zugrundeliegende Technologien ausreichend einzubeziehen.

Das Top-Management definiert den Rahmen für das anzustrebende Sicherheitsniveau, bezieht dabei Informationssicherheits-Experten ein und bestellt einen Beauftragten für die Steuerung der Informationssicherheit. Dieser entwickelt verbindliche Vorgaben und implementiert das Regelwerk als Geschäftsanweisungen. Die operativen IT-Einheiten sind anschließend verantwortlich, diese Vorgaben umzusetzen und mit geeigneten Technologien und Prozessen darauf zu reagieren.

In der Praxis sind viele Sicherheitstechnologien und begleitende Betriebsprozesse bereits von IT-Fachexperten initiiert worden. Firewalls und Schadcodescanner sind etabliert, oft lange vor der formellen Dokumentation durch den Informationssicherheitsbeauftragten. Dadurch wird der ISB von den Experten als wenig unterstützend wahrgenommen. Um diese Lagerbildung zu überwinden, müssen organisatorische Barrieren abgebaut und die Zusammenarbeit etabliert werden.

Organisatorische Brüche als Sicherheitsrisiko

Es fehlt an verbindenden Elementen zwischen dem formalen ISMS-Paperwork und der technischen Umsetzung. Die Symptome resultieren aus nicht verzahnten vertikalen Brüchen in der Organisationsstruktur. Zuständigkeitsgrenzen verhindern oft die enge Zusammenarbeit, was für die Querschnittsfunktion Sicherheit kontraproduktiv ist.

Klare Regelungen zu Zuständigkeiten und Verantwortlichkeiten sind Kernpflicht der Geschäftsführung, des Vorstands oder der Behördenleitung. Wird diese Pflicht vernachlässigt, können Schadenersatzforderungen und strafrechtliche Konsequenzen drohen.

Der Automatismus, Beauftragte für Informationssicherheitsmanagement, Risikomanagement und Datenschutz zu bestellen, senkt die Haftungsrisiken der Führungsebene. Gleichzeitig führt er oft dazu, dass die oberste Leitung sich zu sehr auf formale Bestellungen beschränkt.

Die Organisation erreicht mit Normanforderungen den gewünschten Reifegrad bei Managementsystemen, Schnittstellen und Zuständigkeiten nur langsam. Gleichzeitig zwingen der dynamische IT-Markt und die Schnelllebigkeit der Angreifer die IT zu reaktivem Handeln. Lösungen werden von Technikern beschafft, implementiert und vom IT-Betrieb dann mühsam am Laufen gehalten. So entstehen fragmentierte IT-Systeme, die kaum noch zu verteidigen sind.

Ganzheitliche Sicherheitsstrategien

Das reine Ausweiten von Organisationen durch Managementsysteme und Beauftragte in Stabsstellen reicht nicht aus. Unternehmenssicherheitsziele müssen stärker in die Geschäftsstrategie integriert werden, jedoch unter Berücksichtigung rechtlicher und branchenspezifischer Anforderungen. Daraus entsteht die Notwendigkeit, diese in eine passende Sicherheitsarchitektur zu übersetzen. Doch was bedeutet es konkret, Sicherheit am Business auszurichten?

Die Integration rechtlicher, technischer und organisatorischer Perspektiven ist essenziell und erfordert Dolmetscher: Business-Analysten, Enterprise-Architekten sowie Experten für Informationssicherheit, Datenschutz und Cybersecurity arbeiten mit Business-Vertretern, Controllern und Risikomanagern in einem interdisziplinären Gremium für Unternehmenssicherheit, das direkt an die oberste Führung berichtet.

IT-Risiken müssen ernsthaft im allgemeinen Risikokatalog verankert und zugänglich gemacht werden, denn unterschiedliche Fachsprachen und Komplexität führen häufig zu Integrationsbrüchen. Risiken werden oft pauschal bewertet oder verschwinden hinter Sammelbegriffen wie Patch- oder Benutzermanagement. Eine verstärkte Kooperation zwischen IT und Controlling ist zukünftig notwendig, um Bewertungsmaßstäbe zu vereinheitlichen und IT-Risiken unternehmensweit transparent zu machen. Das Risikomanagement steuert so Investitionen, priorisiert Maßnahmen und löst Abhängigkeiten.

Erweitert man Governance-Funktionsstellen um Business-Vertreter und orientiert das Risikomanagement konsequent am Organisationszweck inklusive der IT-Risiken, entsteht die Grundlage für die Steuerung von Verbesserungspotenzialen, Schwachstellen und Risiken. Einzelbeauftragte werden durch agile, multidisziplinäre Teams ersetzt, was eine moderne, schnelle und effektive Steuerungsstruktur gewährleistet. ■

SECaaS oder Insellösungen?

Security-as-a-Service verspricht aktuelle Schutzmechanismen ohne eigene IT-Sicherheitsinfrastruktur. Doch was steckt dahinter, für wen lohnt sich das Modell und worauf sollten Unternehmen achten?

Von Stefan Tiefel, noris network AG

Security-as-a-Service (SECaaS) bedeutet, IT-Sicherheitsfunktionen an spezialisierte Anbieter auszulagern. Die Dienste kommen aus der Cloud, ähnlich wie bei SaaS-Angeboten. Unternehmen mieten Sicherheitstechnologien, die von Experten betreut und regelmäßig aktualisiert werden. Häufig ist das Zero-Trust-Prinzip integraler Bestandteil.

noris
Halle 7, Stand 7–212

Im Gegensatz zur traditionellen IT-Sicherheit, bei der Unternehmen Hardware und Software selbst verwalten, basiert SECaaS auf Cloud-Technologie. Das spart Ressourcen und erhöht die Flexibilität. Gleichzeitig ersetzen Zero-Trust-Strategien das „Vertrauen durch Standort“: Sie verifizieren jeden Zugriff, bevor sie ihn gewähren.

Modulare Bausteine

Security-as-a-Service-Angebote bestehen typischerweise aus verschiedenen Komponenten, die Unternehmen bedarfsgerecht kombinieren können:

- Identity and Access Management (IAM): Steuerung des Datenzugriffs
- Netzwerkschutz: Firewalls und Intrusion Detection
- Endpunktschutz: Schutz für Geräte wie Laptops oder Smartphones
- Cloud-Sicherheit: Schutz für Plattformen wie Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS)
- Data Loss Prevention (DLP): Verhinderung unbeabsichtigter Datenverluste
- Zero-Trust-Architekturen: Verhindern unautorisierter Zugriffe durch strikte Zugriffskontrollen

Vorteile und Risiken

Das SECaaS-Modell bietet mehrere Vorteile: Es ermöglicht hohe Flexibilität und Skalierbarkeit, da Unternehmen neue Nutzer oder Funktionen unkompliziert hinzufügen können. Statt hoher Anfangsinvestitionen fallen planbare monatliche Gebühren an. Zudem profitieren Kunden vom Fachwissen der Anbieter, die eine Rund-um-die-Uhr-Überwachung, schnelle Reaktionszeiten und kontinuierliche Weiterentwicklung der Sicherheitslösungen gewährleisten. Die automatische Aktualisierung der Systeme und die konsequente Umsetzung von Zero-Trust-Prinzipien stellen weitere Pluspunkte dar.

Diesen Vorteilen stehen jedoch auch Risiken gegenüber: Die Abhängigkeit vom Anbieter (Vendor-Lock-in) kann problematisch werden, besonders wenn ein Wechsel erforderlich wird. Datenschutzrechtliche Bedenken müssen sorgfältig geprüft werden, und Unternehmen müssen der Cloud-Infrastruktur von Drittanbietern ein gewisses Vertrauen entgegenbringen.

Einfache Integration

Die Einführung von SECaaS gestaltet sich meist unkompliziert, sofern die technischen Grundvoraussetzungen erfüllt sind. Die meisten Anbieter unterstützen ihre Kunden beim Setup, bei Schulungen und der fortlaufenden Betreuung. Zero-Trust-Konzepte lassen sich schrittweise integrieren und an bestehende Systeme anpassen. Bei der Auswahl eines Dienstleisters sollte man auf transparente Preismodelle, auf einen zuverlässigen Support, auf DSGVO-Konformität und auf Zertifizierungen (z. B. ISO 27001) achten.

Neben technischen Aspekten spielen rechtliche Vorgaben und Compliance-Anforderungen eine zentrale Rolle bei der Entscheidung für SECaaS. Entscheidend ist, dass die Datenverarbeitung in europäischen Rechenzentren oder unter gleichwertigen Datenschutzstandards erfolgt. Zertifizierungen schaffen zusätzliche Sicherheit und Nachvollziehbarkeit.

Unternehmen müssen zudem das Prinzip der geteilten Verantwortung (Shared-Responsibility-Model) berücksichtigen: Bestimmte Aufgaben übernimmt der Anbieter, während andere eindeutig beim Kunden verbleiben. Diese Verantwortlichkeiten sollten vertraglich klar geregelt sein. ■

TÜVNORD

OT-Cybersicherheit für Industrial Automation und Control Systems (IACS):

Vom Risiko zur Resilienz: Mit dem Seminar zum OT-Security Manager (TÜV®)

Warum OT-Cybersicherheit heute unverzichtbar ist

Produktionsanlagen, Energieversorgung, Logistik – sie alle basieren auf Operational Technology (OT). Diese Systeme sind das Herzstück moderner Industrieprozesse. Doch mit der zunehmenden Vernetzung von IT und OT steigt die Gefahr: Cyberangriffe auf industrielle Steuerungssysteme (IACS) sind längst keine Seltenheit mehr. Die Folgen? Produktionsausfälle, Sicherheitsrisiken, hohe Kosten und Reputationsschäden.
Die EU-Richtlinie NIS-2 und die internationale Norm IEC 62443 setzen klare Anforderungen: Unternehmen müssen ihre OT-Systeme systematisch schützen – und das nicht nur technisch, sondern auch organisatorisch und strategisch.

Die zentralen Aufgaben der OT-Cybersicherheit

OT-Cybersicherheit ist mehr als Firewalls und Virenscanner.
Sie umfasst:

- **Risikomanagement:** Welche Bedrohungen existieren für Ihre Anlagen? Welche Schwachstellen sind kritisch?
- **Zieldefinition:** Welche Sicherheitsniveaus (Security Levels) sind für Ihre Systeme angemessen?
- **Zonenbildung:** Welche Bereiche müssen voneinander getrennt werden, um Angriffsflächen zu minimieren?
- **Verantwortlichkeiten:** Wer trägt wofür die Verantwortung – vom Management bis zur Technik?
- **Kontinuierliche Überwachung:** Wie stellen Sie sicher, dass Ihre Schutzmaßnahmen dauerhaft wirken?

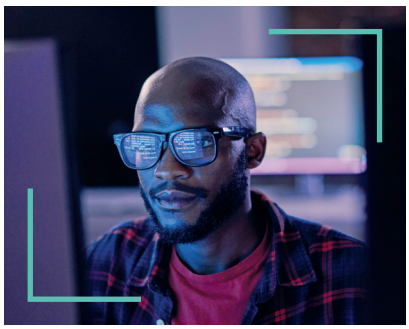
Eine starke OT-Cybersicherheitsstrategie schützt nicht nur vor Angriffen, sondern sorgt für stabile Produktionsabläufe und rechtliche Sicherheit. Sie erfüllt Anforderungen wie NIS-2, schafft Vertrauen bei Kunden und Partnern und steigert die Effizienz durch klare Prozesse. Gleichzeitig bleiben Ihre Anlagen über den gesamten Lebenszyklus hinweg zuverlässig und sicher – ein echter Wettbewerbsvorteil für Ihr Unternehmen.

Die wichtigsten Schritte zur Umsetzung

1. **Analyse der OT-Umgebung:** Verstehen Sie Ihre Systeme und deren Abhängigkeiten
2. **Einführung eines Managementsystems:** Strukturierte Prozesse für Sicherheit und Compliance
3. **Integration in bestehende Frameworks:** OT-Sicherheit wird Teil Ihrer Unternehmensstrategie
4. **Schulung und Sensibilisierung:** Alle Beteiligten müssen die Risiken kennen und handeln können
5. **Audit und Review:** Regelmäßige Überprüfung und Anpassung Ihrer Maßnahmen

Unterstützung für Unternehmen

- OT-Cybersicherheit strategisch steuern und gesetzeskonform umsetzen: **Das Seminar OT-Security Manager (TÜV®)**



Schlüsselrolle in der OT-Cybersicherheit übernehmen!

Das 4-tägiges Seminar vermittelt praxisnahes Wissen zur IEC 62443 und NIS-2 – speziell aus Managementperspektive. Mit Fallstudien, Workshops und einem TÜV-Zertifikat sind Sie bestens gerüstet, Ihre OT-Sicherheit auf das nächste Level zu bringen.

Alle Details zum Seminar: **OT-Security Manager (TÜV®)**

Vom Zertifikatschaos zur Krypto-Agilität:

Der Weg zur modernen Public-Key-Infrastruktur

Über Jahre gewachsene Zertifikatslandschaften stoßen heute an ihre Grenzen. Steigende Anforderungen durch Cloud, IoT und Quantenkryptografie machen ein Umdenken erforderlich. Wie Organisationen von manueller Verwaltung zur modernen, skalierbaren Public-Key-Infrastruktur (PKI) gelangen können, zeigt dieser Beitrag.

Von Thomas Weber, ID Security

Die Zertifikatsverwaltung ist in vielen Organisationen von gewachsenen Strukturen geprägt: Über Jahre entstandene Infrastrukturen treffen auf knappe interne Ressourcen, was eine strukturierte Verwaltung erschwert. Obwohl der Bedarf an Zertifikaten kontinuierlich gestiegen ist, wurden die Prozesse nur unzureichend angepasst. Certificate Automation bleibt vielfach Wunschdenken.

Parallel dazu beschleunigt die IT-Transformation den Zertifikatsbedarf: Microservices, DevOps, Cloud und das Internet of Things lassen die Zahl der Zertifikate rasant anwachsen. Zahlreiche Organisationen verwalten TLS/SSL-, Code-Signing-, Geräte- und Client-Zertifikate noch manuell – ein Vorgehen, das erhebliche Risiken für Ausfälle und Sicherheitslücken birgt.

Spätestens wenn der Chief Information Security Officer (CISO) Fragen stellt wie „Sind wir Post-Quantum-ready?“ oder „Wo finde ich eine Übersicht aller kryptografischen Assets?“, wird deutlich, dass einfache Excel-Tabellen nicht mehr ausreichen. Die zentrale Herausforderung lautet: Wie gelingt der Umstieg auf eine moderne, skalierbare und zukunftssichere Public-Key-Infrastruktur?

Awareness und Strategien

Ein professionelles Vorgehen beginnt mit Transparenz: Grundlage ist die vollständige Inventarisierung aller Zertifikate, Certification Authorities (CAs) und kryptografischen Assets. Nur auf dieser Basis lassen sich gezielte Modernisierungsschritte umsetzen. Unterstützung bieten spezialisierte Tools, die Schlüssel, Zertifikate, Algorithmen, Bibliotheken und Protokolle systematisch erfassen. Ein standardisiertes Inventar der Kryptokomponenten – vergleichbar mit einer Stückliste für Software (Software Bill of Materials, SBOM), jedoch auf kryptografische Assets zugeschnitten – wird im sogenannten Cryptography Bill of Materials (CBOM) abgebildet (siehe Infokasten).

Darauf aufbauend folgt die Definition eines Zielbildes: Welche Architektur soll künftig gelten? Eine zentrale PKI oder mehrere spezialisierte Instanzen? On-Premises oder als Software as a Service (SaaS)? Ziel ist ein tragfähiges Architekturmodell, das skalierbar ist und zugleich regulatorischen sowie branchenspezifischen Anforderungen entspricht.

Einführung eines modernen CLM-Systems

Mit diesen Zielen im Blick folgt die Auswahl eines Certificate-Lifecycle-Management-(CLM)-Systems, das nicht nur Automatisierung verspricht, sondern auch umfassende Sichtbarkeit, Self-Service-Möglichkeiten, Governance-Funktionen und eine echte Policy-Steuerung bietet.

Denn Automatisierung allein reicht nicht – sie muss an konkreten Zielen ausgerichtet sein. Daneben sind Zertifikats-Discovery, Workflow-Automatisierung und Integrationen mit bestehenden Systemen essenziell für den Einsatz eines CLMs. Neben Rollen und Verantwortlichkeiten werden auch Genehmigungsketten (Approval-Workflows) im CLM abgebildet. So entsteht eine stabile Basis, die Wildwuchs und Ausfälle verhindert.

In der IT-Landschaft übernimmt das CLM die Funktion einer zentralen Steuerungs- und Integrationsschicht. Es kann klassisch On-Premises betrieben werden, wo es sich eng an bestehende interne PKI-Infrastrukturen und Sicherheitsvorgaben anlehnt, oder in der Cloud, wo es durch Skalierbarkeit und Anbindung an moderne Platt-

formdienste zusätzliche Flexibilität bietet. Besonders interessant ist ein hybrides Modell: Ein CLM in der Cloud kann mit einer lokalen PKI kombiniert werden und so eine Brücke zwischen bestehenden Strukturen und neuen Cloud-Architekturen schlagen. Diese Positionierung ermöglicht es Unternehmen, zunächst ihre Prozesse zentral zu konsolidieren und zu automatisieren, um dann schrittweise – wenn regulatorisch und strategisch sinnvoll – eine vollständige Migration in die Cloud vorzubereiten.

Standardisierte Protokolle wie ACME, CEP/CES oder EST bieten bereits eine breite Unterstützung für die automatische Ausstellung, Verlängerung und den Widerruf von Zertifikaten. Ein zukunftsorientiertes CLM geht jedoch darüber hinaus und stellt zusätzlich eine REST-API bereit. Diese Schnittstelle ist im DevOps-Umfeld besonders wertvoll, weil sich Zertifikatsprozesse damit nahtlos in CI/CD-Pipelines, Container-Orchestrierungen oder individuelle Business-Applikationen integrieren lassen. Zertifikate werden so zu einem automatisierten, unsichtbaren Bestandteil des Entwicklungs- und Betriebsprozesses – und nicht länger zu einem manuellen Engpass.

Dabei gilt es aber auch, die technologische Zukunftssicherheit im Blick zu behalten. Das ältere SCEP-Protokoll hat im Netzwerkumfeld lange gute Dienste geleistet, erfüllt jedoch moderne Sicherheitsanforderungen nicht mehr und ist für eine Quantum-safe-Strategie ungeeignet. Unternehmen sollten daher frühzeitig Pläne entwickeln, um von SCEP auf zeitgemäßere Protokolle zu migrieren.

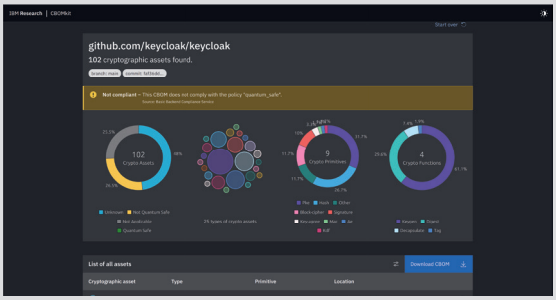
Intelligente Discovery-Verfahren

In der Praxis reicht ein einfaches Port-Scanning längst nicht mehr aus. Zwar lassen sich so Zertifikate auf offenen Services identifizieren, doch bleibt der Blick oberflächlich. Fortschrittliche Methoden setzen auf intelligentes Port-Scanning, bei dem zusätzlich die Konfigurationen von Web- oder Applikationsservern ausgelesen werden. So lässt sich nicht nur ermitteln, welche Zertifikate eingesetzt werden, sondern auch, welche kryptografischen Algorithmen zugelassen sind – ein entscheidender Faktor, um mögliche Schwachstellen frühzeitig zu erkennen.

Darüber hinaus können weitere Verfahren zum Einsatz kommen: Die Synchronisation mit CA-Datenbanken deckt ungemanagte Zertifikate auf, die bislang außerhalb des CLM geführt werden. Netzwerksniffing – meist mit dedizierten Hardware-Appliances – bietet zusätzliche Einsichten in den laufenden Verkehr. Ebenso wichtig ist das Filesystem-Scanning, das gezielt nach lokalen Keystores sucht und diese in das CLM integriert. Damit wird nicht nur die Transparenz erhöht, sondern auch der Grundstein für das automatisierte Management dieser Keystores gelegt.

Cryptography Bill of Materials (CBOM)

Ein vergleichsweise neues Konzept im Kontext von Zertifikats- und Schlüsselmanagement ist die Cryptography Bill of Materials (CBOM). Darin werden kryptografische Eigenschaften dokumentiert – von Algorithmen, Zertifi katen, Protokollen und Schlüsseln bis zu sicherheitsrelevanten Werten wie Tokens, Nonces oder Passwörtern.



Guter Einstieg: CBOMkit von IBM (OpenSource), https://github.com/IBM/cbomkit (Bild: ID Security)

Wesentlich ist, dass Discovery nicht als einmalige Bestandsaufnahme verstanden wird, sondern als kontinuierlicher Prozess: Die gefundenen Zertifikate und Schlüssel müssen fortlaufend im Policy-Modul des CLM mit den unternehmensspezifischen Sicherheitsrichtlinien abgeglichen werden. Nur durch diese laufende Risikoanalyse lassen sich veraltete Algorithmen, schwache Schlüssel oder falsch konfigurierte Zertifikate rechtzeitig identifizieren. ■

Automatisierung mit einem CLM

Als zentrales Backend einer Zertifikatsverwaltung steuert eine CLM alle Prozesse für interne und externe PKI Systeme. Flexible Dashboards ermöglichen die Darstellung relevanter Daten und bevorstehender Ereignisse.

Modernes CLM: CEMA von ID Security, www.id-security.com (Bild: ID Security)

Reifegrad der KI und Auswirkungen auf die Risikoexposition

Experten diskutieren auf der it-sa, ob KI die Sicherheitslandschaft revolutioniert oder nur ein weiteres Werkzeug ist

Die zunehmende Nutzung von Künstlicher Intelligenz (KI) in der Cybersicherheit wirft grundlegende Fragen zur Verteidigungsstrategie auf. Bis 2026 könnte sich zeigen, ob KI nur ein weiteres Werkzeug oder eine echte technologische Revolution darstellt. Sicherheitsexperten stehen vor der Herausforderung, das richtige Maß an Vertrauen und Kontrolle für KI-Systeme zu finden.

Von Bastian Hallbauer, Kafka Kommunikation

Die Häufung von Schwachstellen und erfolgreichen Angriffen auf KI-Systeme zeigt die Verwundbarkeit dieser Technologie. Gleichzeitig entwickeln Cyberkriminelle eigene KI-Tools oder nutzen vorhandene Systeme durch geschicktes Prompting für ihre Zwecke.

Cloudflare
in Halle 7A–226

KnowBe4
in Halle 6–105

Proliance
in Halle 7–205

Für IT-Sicherheitsverantwortliche stellt sich die Frage, wie viel Vertrauen sie der KI schenken können – und aufgrund von Ressourcenmangel vielleicht auch müssen. Sie müssen entscheiden, wie viel Governance von KI oder mit KI sie zulassen können oder müssen und wie sie diese Kontrollebene außerdem so flexibel halten, dass sie mit den nächsten Sprüngen mithalten kann.

Auf einem Panel auf der it-sa werden die Teilnehmer Stefan Henke, RVP DACH bei Cloudflare, Dr. Martin Krämer, Security Awareness Advocate bei KnowBe4 und Florian Müller Head of Product & Technology bei Proliance dieses Thema diskutieren.

Martin Krämer sieht in KI eine große Chance für die Cybersicherheit, insbesondere Agentic AI verspricht Effizienz- und Qualitätssteigerungen, die bei der Verteidigung entscheidende Verbesserungen liefern können. „Es geht darum, KI wohlüberlegt, in großem Umfang und mit mehrschichtigen Abwehrmaßnahmen einzusetzen“, gibt Stefan Henke zu Bedenken, doch „wer zögert, riskiert, nicht nur von Angreifern überholt zu werden, sondern auch von Wettbewerbern.“

Florian Müller teilt die Einschätzung, sieht aber einen Unterschied im Reifegrad und in der Governance: „Unkuratiert eingesetzte KI erhöht die Komplexität der Sicherheitslandschaft und schafft neue Angriffswege.“

Doch auch die andere Seite setzt auf KI. Sie ermöglicht Cyberkriminellen Exploits aufzudecken oder großflächige Social Engineering-Attacken mit geringem Aufwand durchzuführen. Speziell in der Cloud kann so ein Angriff in unter zehn Minuten gelingen. Letztlich stärkt KI also beide Seiten, Verteidiger aber auch Angreifer. Für Henke ist daher entscheidend, wer ihre Fähigkeiten effektiver nutzt.

Governance als Schlüsselfaktor

KI vergrößert allerdings auch die Angriffsfläche. Krämer ist der Meinung, „dass Effizienzsteigerungen bei der Verteidigung sie möglicherweise kleiner oder wenigstens einfacher zu bewältigen erscheinen lassen.“ Müller pflichtet ihm bei, „wenn KI als Kontrollverstärker wirkt, kann sie für weniger unerkannte Schwachstellen und deren schnellere Schließung sorgen.“ Es kommt also auf die richtige Governance an, die für Henke ein „lebendiges Rahmenwerk, ein Betriebssystem des Vertrauens“ sein muss: „Im Kern sollten klare Grenzen dafür definiert werden, wie KI-Systeme in Sicherheitsumgebungen trainiert, eingesetzt und überwacht werden.“ Krämer ergänzt die für ihn wichtigen Faktoren: „Transparenz und Nachvollziehbarkeit, menschliche Kontrolle und Resilienzsteigerung, Robustheit, und Verantwortlichkeit.“

Wie KI für die IT-Sicherheit richtig eingebettet wird, soll auf dem Panel am Mittwoch, den 8. Oktober von 13:00 bis 13:30 Uhr auf der it-sa in Halle 7, Forum D unter der Moderation von <kes>-Chefredakteur Norbert Luckhardt diskutiert werden. ■

TREND MICRO™ | Global Leader in Cybersecurity

Proaktive Sicherheit beginnt hier.

Ihr Weg zu Innovationen beginnt mit einer Cybersecurity-Plattform, die Risikomanagement, Security Operations und mehrschichtigen Schutz in sich vereint.

Machen Sie Security zum Innovationstreiber mit Trend Vision One™.

Erfahren Sie mehr unter **trendmicro.com/visionone**

Besuchen Sie uns auch auf der it-sa 2025 in Nürnberg:
Halle 7, Stand 7-137 & 7-139

Digitale Souveränität

Deutschland wohnt technologisch zur Miete

Deutschland fordert digitale Souveränität – lebt im Alltag aber den US-Stack. Zwischen Forderungen, Selbsteinschätzung und gelebter Praxis klaffen große Lücken. Katharina M. Schwarz, Head of Global Affairs bei Myra Security, legt anhand neuer Studiendaten dar, wie es um die digitale Souveränität hierzulande bestellt ist und wo die größten Hürden liegen.

Von Katharina M. Schwarz, Myra Security

Kaffeeduft erfüllt den Raum, die Dashboards leuchten grün. Nichts deutet auf Probleme hin – bis die Finanzabteilung auf die neue Lizenzrechnung hinweist. Der Preis zieht an, die Klauseln auch. „Was, wenn der Anbieter morgen die Regeln ändert?", fragt der CISO. Niemand antwortet. Man hat sich eingerichtet im bequemen Schatten eines globalen Ökosystems, das sich anfühlt wie eigene Infrastruktur – aber jemand anderem gehört.

Fragen wie aus diesem beispielhaften Szenario dürften sich viele Entscheidende in den vergangenen Monaten gestellt haben. Diskussionen rund um die digitale Souveränität sind überall zu finden. Doch wo steht Deutschland hier genau? Antworten hierzu liefert die Studie „The State of Digital Sovereignty 2025". Im Auftrag von Myra befragte Civey dafür 1500 IT-Entscheidende in Deutschland.

Europäische Lösungen für Public- und KRITIS-Sektor

Konsens im Maschinenraum: 84,4 Prozent der IT-Verantwortlichen fordern, dass Staat und Betreiber kritischer Infrastrukturen vorrangig europäische Anbieter nutzen. „Ja, auf jeden Fall" übertrumpft sogar das vorsichtigere „Eher ja". Nur 8,3 Prozent sprechen sich dagegen aus. Das ist ein klares Mandat – und ein Auftrag an Beschaffung, Regulierung und Budgets, diese Linie konsequent zu fahren. Gleichzeitig zeigt die Studie aber auch: In den eigenen Unternehmen bleibt die Umsetzung zäh; weniger als ein Drittel plant binnen 24 Monaten die Einführung europäischer Software, fast die Hälfte winkt ab. Die Sonntagsreden sagen das eine, die Wochenpläne das andere.

Abhängigkeiten dort, wo es weh tut

Besonders in wichtigen Zukunftsfeldern, in denen sich kritische und sensible Prozesse – und damit auch Daten – bündeln, hängen Unternehmen am digitalen US-Tropf. 39,7 Prozent empfinden eine starke bis sehr starke Abhängigkeit bei Cloud-Services, 39,5 Prozent in der Cybersicherheit; bei KI-Infrastruktur sehen 36,6 Prozent dasselbe Muster. In der Praxis nutzen nur 20,5 Prozent europäische Security-Lösungen; bei KI-Infrastruktur sind es mit 10,2 Prozent sogar noch weniger. In Cloud-Umgebungen bleibt der EU-Anteil ebenfalls unter 25 Prozent.

Ein Blick auf die „grünen Zonen" relativiert nur wenig: In Enterprise Resource Planning (ERP) und Finanzsoftware ist Europa traditionell stark – 39,6 Prozent beziehungsweise 41,5 Prozent nutzen bereits europäische Lösungen, die wahrgenommene Abhängigkeit fällt dort deutlich geringer aus. Diese Inseln sind jedoch nur ein Hoffnungsschimmer, solange wichtige Bereiche wie Cloud, KI und Security fest in US-Hand bleiben.

Wahrnehmungslücke: Des Kaisers neue digitale Kleider

Die Studie zeigt eine doppelte Blindstelle. Erstens: Viele Entscheidende kennen europäische Alternativen nicht. In ERP, Customer Relationship Management (CRM) und Finanzen nennen knapp die Hälfte konkrete Anbieter; bei Collaboration und KI liegt die Bekanntheit nur bei 21,8 beziehungsweise 21,9 Prozent. Selbst in der Security wissen nur 32,4 Prozent von europäischen Optionen. Sichtbarkeit entscheidet – wer Alternativen nicht kennt, migriert nicht. Die Folge ist eine anhaltende Präferenz für US-Lösungen.

Zweitens: Viele überschätzen die eigene Unabhängigkeit. In der KI-Infrastruktur nutzen nur 10,2 Prozent europäische Lösungen, aber mehr als die Hälfte bewertet die

Abhängigkeit als schwach oder nicht vorhanden. In der Security liegt die Nutzung europäischer Produkte bei 20,5 Prozent – trotzdem schätzen 47,2 Prozent der Befragten die Abhängigkeit als gering ein. Souverän im Selbstbewusstsein, aber im digitalen Sinne weitgehend nackt.

Wechselbereitschaft: Mehrheit hält an US-Lösungen fest

Nur 20,4 Prozent der befragten Unternehmen befinden sich bereits aktiv in der Einführung einer oder mehrerer europäischer Lösungen. Weitere 12,3 Prozent planen dies innerhalb der nächsten zwei Jahre. Parallel dazu bleibt das Lager der Zauderer groß: 47,7 Prozent planen gar keinen Umstieg, 17,4 Prozent sind unentschieden oder wissen es nicht. Ein umfassender Trend zu mehr digitaler Souveränität ist bislang nicht zu erkennen.

Was braucht es also, um Entscheidende vom Wechsel zu überzeugen? Leistungsparität ist dabei das wichtigste Kriterium: 69,9 Prozent der IT-Entscheidenden würden auf europäische Software umsteigen, wenn diese die gleiche Funktionalität und Zuverlässigkeit wie die bestehende Lösung bietet. Datensicherheit ist nahezu ebenso relevant: 69,4 Prozent nennen sie als Hauptmotiv für einen Wechsel. Zwei Drittel (66,5 Prozent) der Unternehmen wären bei deutlich niedrigeren Kosten bereit, auf europäische Lösungen umzusteigen. Ein weiterer Faktor: Für 62,5 Prozent der Befragten ist die garantierte Datenspeicherung in der EU ein entscheidendes Kriterium für die zukünftige Nutzung europäischer Software.

Politik und Praxis: Rückenwind statt Rezepte aus der Mottenkiste

Frankreich hat mit dem 2021 gestarteten Programm „Parcours de cybersécurité“ gezeigt, wie staatliche Förderung die digitale Souveränität stärken kann. Unter der Leitung der nationalen Cybersicherheitsbehörde ANSSI wurden 945 Einrichtungen finanziell unterstützt, darunter Kommunen, Krankenhäuser und weitere öffentliche Institutionen. Das Programm umfasste standardisierte Audits und die Realisierung von über 3000 Sicherheitsmaßnahmen wie die Härtung von Systemen, Netzwerksegmentierung und Backup-Strategien. Die Einrichtungen trugen lediglich einen 30-prozentigen finanziellen Eigenanteil an den nötigen Maßnahmen. Im Schnitt investierten sie aber 30 Prozent mehr als nötig. Letztlich stieg der durchschnittliche Cyber-Reifegrad der Teilnehmenden durch das Projekt von „D+“ auf „B“.

Finanzielle Anreize sind ein zentraler Hebel. Mehr als die Hälfte der Entscheidenden würde bei entsprechender Förderung einen Wechsel zu europäischen Anbietern erwägen. Ein in Deutschland eingeführter „Souveränitäts-Check“ bei öffentlichen IT-Beschaffungen – wie er bereits für Hoster existiert – könnte die Prüfung europäischer Alternativen rechtlich verankern und deren Sichtbarkeit erhöhen.

Fazit: Souveränität heißt nicht Autarkie

Die Daten der Studie sprechen eine deutliche Sprache: breite Zustimmung für europäische Lösungen in KRITIS, kritische Abhängigkeiten bei Cloud, KI und Security, Wissenslücken bei Alternativen und eine Wechselbereitschaft, die an harte Kriterien gebunden ist. Europa muss nun eine entsprechende technologische Landschaft aufbauen. Dabei geht es nicht um Autarkie, sondern darum, einen Gegenpol zur Dominanz der US-Techgiganten zu schaffen. Klar, dieser wird nicht von heute auf morgen entstehen – aber weiterhin nur auf Sicht zu fahren, ist keine Option. Langfristig wird der Markt in Deutschland und Europa hierdurch diverser, stärker und innovativer. Ein Markt, der tatsächliche Wahlfreiheit und damit reelle Souveränität bietet. ■

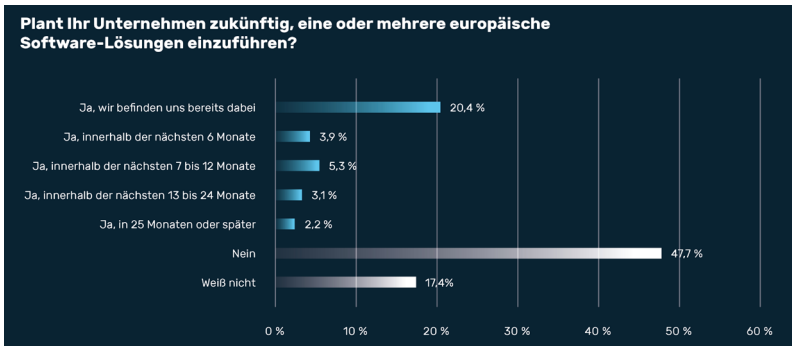
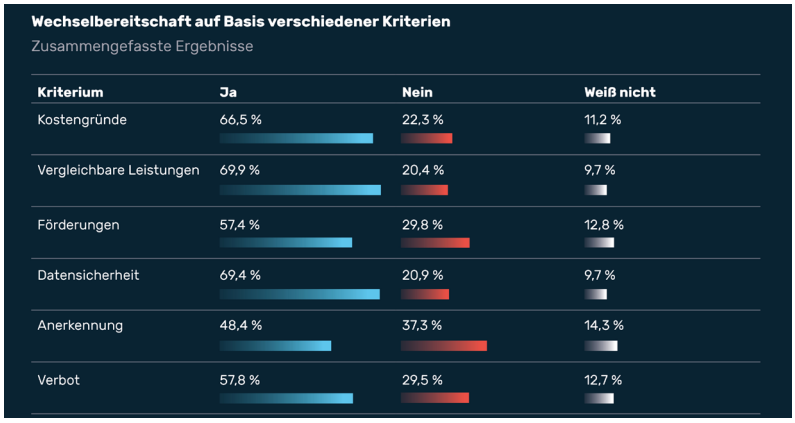


Abbildung 1: Fast die Hälfte aller IT-Entscheidenden plant innerhalb der nächsten zwei Jahre keine Einführung europäischer Softwareprodukte. (Bild: Myra Security)



Kriterium	Ja	Nein	Weiß nicht
Kostengründe	66,5 %	22,3 %	11,2 %
Vergleichbare Leistungen	69,9 %	20,4 %	9,7 %
Förderungen	57,4 %	29,8 %	12,8 %
Datensicherheit	69,4 %	20,9 %	9,7 %
Anerkennung	48,4 %	37,3 %	14,3 %
Verbot	57,8 %	29,5 %	12,7 %

Abbildung 2: Bei den Kriterien für einen Wechsel dominieren vor allem Leistung, Datensicherheit und Kosten. (Bild: Myra Security)

Myra Security
Halle 7, Stand 7–204

Vision 2026: Sicherheit, die mitwächst

Unternehmen verlagern ihre IT-Infrastruktur zunehmend in hybride Cloud-Umgebungen. Diese Fragmentierung schafft jedoch neue Angriffsflächen für Cyberkriminelle. Ein neuer Sicherheitsansatz soll dieses Problem lösen.

Von Lothar Geuenich, Marco Eggerling und Thomas Boele, Check Point Software Technologies

Im Jahr 2026 wird Cybersicherheit nicht länger als Kostenfaktor betrachtet, sondern als strategischer Business Enabler für Innovation, Resilienz und Wachstum. Dafür benötigen Organisationen ein Sicherheitsmodell, das sich genauso dynamisch weiterentwickelt wie ihre IT-Infrastruktur.

Komplexität schafft Angriffsflächen

Moderne Unternehmen verlagern geschäftskritische Workloads zunehmend in hybride Umgebungen, verteilt über eigene und fremde Rechenzentren, Multi-Cloud-Modelle und Software-as-a-Service (SaaS)-Dienste. Doch genau diese Fragmentierung wird von Angreifern systematisch ausgenutzt. Laut Check Point Research verzeichneten deutsche Organisationen zuletzt im Schnitt 1286 Angriffe pro Woche. Bei erfolgreichen Kompromittierungen bleiben Angreifer teils mehrere Tage unentdeckt – Zeit, die für erhebliche Schäden genutzt wird. Ohne übergreifende Transparenz und koordinierte Abwehrmechanismen bleiben selbst hohe Investitionen in Einzellösungen oft wirkungslos.

Check Point Software Technologies
Halle 6, Stand 6–328

Integrierter Sicherheitsansatz durch Mesh-Architektur

Als Antwort auf diese Herausforderung etabliert sich die sogenannte Hybrid Mesh Architecture (HMA). Diese Architektur verbindet grundlegende Sicherheitsfunktionen wie Bedrohungsabwehr, Richtliniendurchsetzung, dynamische Segmentierung und Telemetrie in einem vernetzten Framework über alle Kontrollpunkte hinweg.

Das Ergebnis ist eine adaptive, skalierbare Sicherheitsstruktur, die auf jede Bedrohung konsistent reagiert, unabhängig davon, wo sie auftritt. Durch zentrale Threat Intelligence und herstellerübergreifende Integration entsteht eine einheitliche Sicht auf Bedrohungen. KI-gestützte Analysen erkennen abweichende Muster frühzeitig, lösen automatisierte Reaktionen aus, isolieren kompromittierte Segmente in Echtzeit und passen Richtlinien dynamisch an.

Verkürzte Reaktionszeiten und mehr Kontrolle

Mit HMA verkürzen Unternehmen nicht nur die Zeit bis zur Erkennung (Mean-Time-to-Detect, MTTD) und die Zeit bis zur Reaktion (Mean-Time-to-Respond, MTTR) drastisch, sie gewinnen auch Kontrolle über ein fragmentiertes System zurück. Eine Bedrohung auf einem Endpunkt löst unmittelbar Schutzmaßnahmen aus, wie das Sperren von Zugriffen oder zusätzliche Authentifizierungsstufen, ganz im Sinne eines Zero-Trust-Modells. In der Folge entsteht ein durchgängiger Schutz von der Edge bis zur Cloud: hochautomatisiert, skalierbar und zukunftsfähig.

Von Insellösungen zu integrierter Resilienz

Die Cyberbedrohungslage wird sich bis 2026 weiter verschärfen, aber Organisationen können vorbereitet sein. Die Hybrid Mesh Architecture ist der Schlüssel zu einer ganzheitlichen, intelligenten Sicherheitsstrategie. Sie verwandelt fragmentierte Sicherheitslandschaften in adaptive Schutzsysteme. Entscheidungsträger sollten jetzt die Weichen für eine Abkehr von isolierten Tools hin zu einer konsolidierten Architektur stellen, die nicht nur schützt, sondern Schäden aktiv mindert.

Check Point Software Technologies unterstützt Organisationen mit BSI-zertifizierten Sicherheitslösungen mit EAL4+ und dem C5-Testat. ■

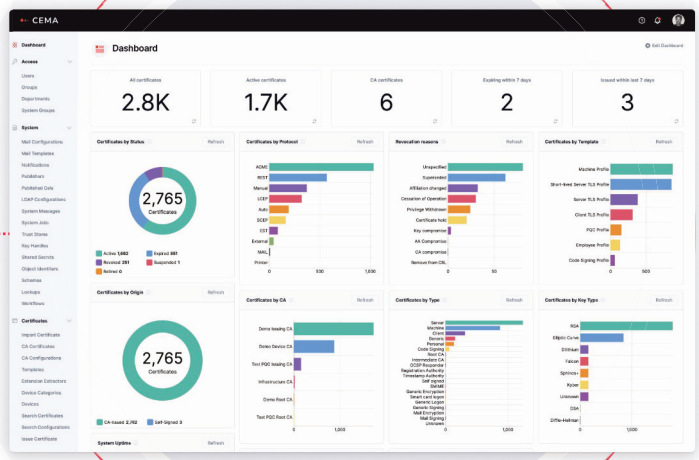
ID Security
by intelliCard

Automatisierung der Zertifikatsverwaltung

Reduzierung von Betriebs- und Sicherheitsrisiken

Einheitliches PKI-Frontend

Enterprise-Grade Zertifikatsmanagement



Krypto-Agilität

Compliance durch Transparenz

Prozess und System Integration

Automatisierung der Zertifikatsverwaltung

Einheitliches PKI-Frontend

- Schnittstelle zu internen & öffentlichen CA
- Zentrales Inventar

Krypto-Agilität

- Integration in CBOM & Discovery-Tools
- Nachverfolgung von Schlüsseln & Algorithmen

Prozess und System Integration

- Flexible Workflows & Alarmsystem
- Genehmigungs und Eskalationsverfahren

Enterprise-Grade Zertifikatsmanagement

- Zugriffskontrolle & Rollenmodelle
- Integration in Sicherheitsinfrastruktur

Compliance durch Transparenz

- Aktuelle Reports & Statistiken
- Dashboard mit allen kritischen Informationen

Automatisierung der Zertifikatsverwaltung

- Breite Enrollment Verfahren
- Unterstützt moderne DevOps-Werkzeuge

From Design to Operation your Experts in *ID*entity Security

→ Visit for more info: www.id-security.com

IT-SA BESUCHEN SIE UNS

07-09 OCT | **Halle 9, Stand 9-346**
TeleTrust Messestand

Digitale Zwillinge in der Cybersicherheit

Den Angreifern einen Schritt voraus

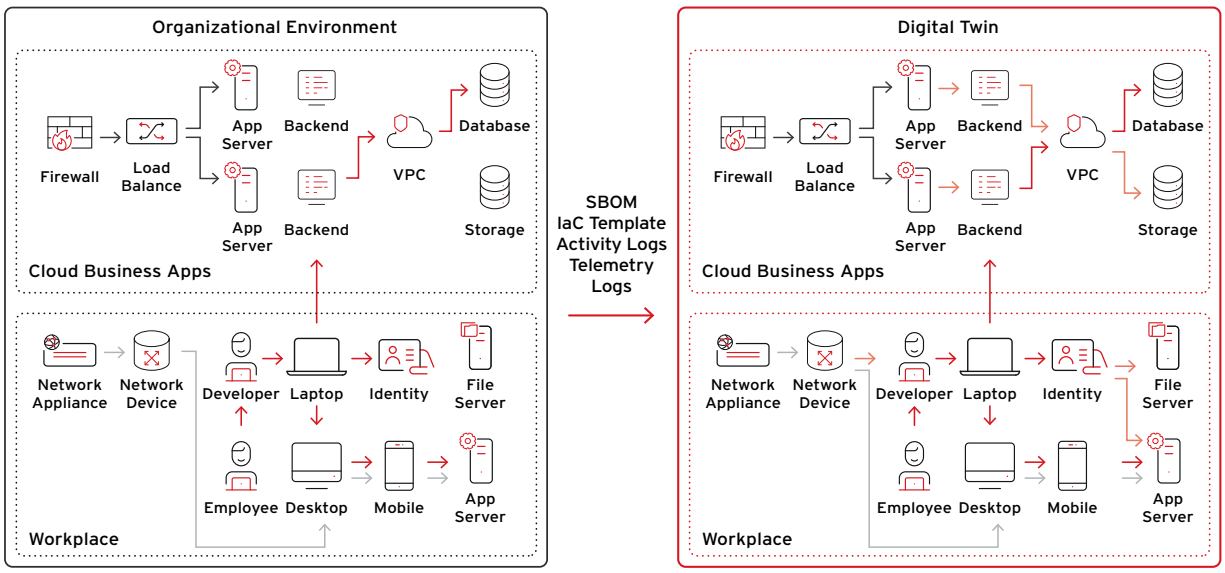
Indem digitale Zwillinge IT-Umgebungen präzise virtuell abbilden, ermöglichen sie proaktive Cybersicherheit auf einem neuen Level: Unternehmen können Risiken kontinuierlich simulieren, Abwehrmaßnahmen realitätsnah testen und strategische Entscheidungen auf fundierter Basis treffen – bevor Angreifer Schaden anrichten.

Von Tobias Grabitz, Trend Micro

Cyberkriminelle setzen zunehmend künstliche Intelligenz ein, um Angriffe zu skalieren, Schwachstellen automatisiert zu identifizieren und gezielt auszunutzen. Mit Large Language Models (LLMs) erstellen sie täuschend echte Phishingmails und entwickeln kontinuierlich neue Malware-Varianten. KI ermöglicht heute Kampagnen in bisher ungeahntem Ausmaß und Tempo. Schneller als je zuvor können Bedrohungsakteure nach der Erstinfektion ihre Rechte erweitern und lateral im Netzwerk vordringen. Um sich vor dieser massiven Bedrohungswelle zu schützen, brauchen auch Security-Teams Verteidigungsmaßnahmen in Maschinengeschwindigkeit – nicht nur für eine schnelle Erkennung und Reaktion, sondern auch für ein kontinuierliches, proaktives Risikomanagement. Wer es schafft, Bedrohungen vorherzusehen, kann seine Security-Strategie zielgerichtet stärken, um den Angreifern einen Schritt voraus zu sein. Eine entscheidende Rolle spielen dabei Cybersecurity Digital Twins.

Definition und Funktionsweise

Ein digitaler Zwilling ist ein virtuelles Abbild eines physischen Produkts, Prozesses oder Systems. Er wird kontinuierlich mit Echtzeitdaten gespeist, um Verhalten, Interaktionen und Zustände zu simulieren, zu analysieren und zu überwachen – ohne die reale Umgebung zu beeinträchtigen. In der Industrie wird dieses Konzept seit Jahren erfolgreich eingesetzt, etwa zur Überwachung technischer Anlagen oder zur Optimierung von Wartungsintervallen. Übertragen auf die Cybersicherheit bildet ein Digital Twin die sicherheitsrelevante Struktur und das Verhalten einer digitalen Umgebung ab. Dabei geht es nicht um eine vollständige Kopie, sondern um eine Modellierung der Elemente, die für den jeweiligen Anwendungszweck relevant sind. So erfasst ein Cybersecurity Digital Twin die Infrastruktur, Datenflüsse, Identitäten, Kontrollmechanismen und Verhaltensweisen mit angemessener Genauigkeit, um



Im Einsatz: Digitaler Zwilling in der Cybersecurity (Quelle: Trend Micro)

aussagekräftige Simulationen und Validierungen zu ermöglichen.

Technologische Voraussetzungen

Digitale Zwillinge sind kein neues Konzept. In der Cybersicherheit halten sie aber erst jetzt Einzug, weil bisher die technischen Voraussetzungen fehlten. Erst die Kombination aus fortschrittlicher Telemetrie, skalierbaren Cloud-Infrastrukturen und KI ermöglicht es, komplexe digitale Umgebungen kontinuierlich und realitätsnah zu modellieren. Moderne Security-Umgebungen erzeugen enorme Mengen an Streaming-Daten, die in den digitalen Zwilling einfließen, sodass ein präzises, lebendiges Risikomodell entsteht. Auf Cloud-Architekturen lässt sich das virtuelle Abbild praktikabel, kosteneffizient und sicher betreiben. KI-Agenten und LLMs wiederum kommen zum Einsatz, um Angreiferverhalten dynamisch zu simulieren, intelligente Testszenarien zu entwerfen und automatisiert Schlussfolgerungen zu ziehen. So können sich Security-Teams besser auf neue Bedrohungen vorbereiten und den Angreifern zuvorkommen.

Die Bedeutung von proaktiver Security ist heute hinlänglich bekannt: Viele Unternehmen haben bereits Maßnahmen wie Application Security Testing, Pentesting oder gar Red Teaming etabliert. Diese sind zweifellos wertvoll, stellen aber immer nur eine Momentaufnahme dar. Da solche Maßnahmen mit einem hohen finanziellen und manuellen Aufwand verbunden sind, erfolgen sie nur sporadisch. In dynamischen Umgebungen, in denen sich Konfigurationen, Systeme und Risiken permanent verändern, reicht das nicht weit genug. Digitale Zwillinge ermöglichen dagegen eine automatisierte, kontinuierliche Sicherheitsbewertung.

Praktische Anwendungsbeispiele

Welche Vorteile ein Cybersecurity Digital Twin bringt, lässt sich am besten anhand von konkreten Use Cases darstellen:

_____ **Auf High-Impact-Angriffsszenarien vorbereiten:** Im virtuellen Abbild simulieren KI-Agenten das Verhalten, die Ziele und Taktiken potenzieller Angreifer. Sobald neue Threat Intelligence verfügbar ist, setzen sie diese automatisiert um. Gleichzeitig analysieren sie die Auswirkungen in Echtzeit und testen die Wirksamkeit der Abwehrstrategien. So erhalten Security-Teams validierte Ergebnisse und Entscheidungsgrundlagen, um die Sicherheit gezielt zu verbessern.

_____ **Investitionen in die Sicherheit strategisch planen:** Viele Unternehmen entscheiden anhand von Branchentrends, Compliance-Vorgaben oder schlichtweg aus dem Bauch heraus über neue Security-Technologien. Wie wirksam die Investitionen tatsächlich sind, lässt sich schwer messen. Im Cybersecurity Digital Twin können Entscheidungsträger dagegen unter realen Bedingungen testen, welchen Einfluss welche Maßnahmen auf das Sicherheitsniveau haben. Indem sie neue Technologien, veränderte Richtlinien oder Architektur-Anpassungen vorab durchspielen, sind sie in der Lage, Investitionen evidenzbasiert und strategisch zu planen.

_____ **Die Resilienz stärken:** Digitale Zwillinge zeigen nicht nur technische Abhängigkeiten, sondern auch die Folgen von Störungen für Entscheidungen und Geschäftskontinuität. Ausfallszenarien lassen sich simulieren, ohne die Produktivsysteme zu beeinträchtigen. So erhalten Führungskräfte Einblick, wie Assets, Datenflüsse und Geschäftsprozesse zusammenhängen, und können ihre Disaster-Recovery-Strategien verbessern.

Implementierungsvoraussetzungen

Damit ein Cybersecurity Digital Twin wirksam funktioniert, benötigt er hochqualitative Telemetrie. Unvollständige oder veraltete Daten können die Simulationen verzerren und zu falschen Sicherheitsentscheidungen führen. Genauso wichtig ist die Skalierbarkeit: Da sich IT-Umgebungen stetig weiterentwickeln, muss auch der Digitale Zwilling mitwachsen, ohne an Leistung oder Aussagekraft zu verlieren. Außerdem darf das System keine isolierte Insellösung sein, sondern sollte sich nahtlos in bestehende IT-, OT- und Cloud-Landschaften integrieren. Nicht zuletzt ist es wichtig, den digitalen Zwilling auch selbst vor Cyberangriffen zu schützen. Schließlich enthält er sensible Informationen über Assets, Schwachstellen und Angriffswege, die nicht in falsche Hände geraten dürfen. Hier gelten dieselben Security-Empfehlungen wie für alle geschäftskritischen Systeme: mehrschichtige Sicherheitskontrollen und regelmäßige Härtungsmaßnahmen.

Mensch und Technologie

Während Cyberkriminelle in KI-Geschwindigkeit angreifen, können wir ihnen mit gleicher Kraft begegnen. Digitale Zwillinge versetzen uns in die Lage, unsere Security-Posture kontinuierlich proaktiv an neue Risiken anzupassen, sodass wir den Angreifern einen Schritt voraus sind. Trend Vision One stellt ein leistungsfähiges digitales Abbild auf Basis von agentenbasierter KI und NVIDIA NIM Microservices in einem Plattformansatz bereit. Trotz Automatisierung und KI bleibt der Mensch dabei unverzichtbar. Auch künftig braucht es kompetente Security-Mitarbeiter, die die Ziele des digitalen Zwillings definieren, ihn strategisch steuern und seine Ergebnisse interpretieren. Im Zusammenspiel werden menschliche Expertise und moderne Technologie zum schlagkräftigen Team, das künftigen Sicherheitsherausforderungen selbstbewusst begegnen kann. ■

KI-Governance: Pflicht oder Wettbewerbsvorteil?

ISACA macht Unternehmen fit für die KI-Governance der Zukunft

Künstliche Intelligenz (KI) revolutioniert unseren Arbeitsalltag. Doch für europäische Unternehmen bedeutet die rasante Entwicklung der KI auch einen enormen Druck: Das neue EU KI-Gesetz fordert umfassende Anpassungen von ihnen. Im Spannungsfeld zwischen Innovation und strenger Regulierung übernimmt ISACA eine entscheidende Rolle als Navigator.

Von Chris Dimitriadis, ISACA

Der jüngste ISACA AI Poll zeigt: Bereits 83 Prozent der IT- und Geschäftsexperten in Europa sind überzeugt, dass ihre Mitarbeitenden KI nutzen. Gleichzeitig hinkt die Absicherung dieser Entwicklung dramatisch hinterher: Nur 31 Prozent der Unternehmen verfügen über eine umfassende KI-Richtlinie. Diese Diskrepanz birgt erhebliche Risiken, die durch das EU KI-Gesetz nun eine neue Dimension erhalten. Denn neben den möglichen operativen, finanziellen oder reputationsbezogenen Schäden kommen auch rechtliche Konsequenzen hinzu.

EU KI-Gesetz erhöht Handlungsdruck

Mit dem neuen KI-Gesetz treten schrittweise entscheidende Verpflichtungen in Kraft, die weitreichende Auswirkungen auf Governance, Transparenz und Haftung in Bezug auf KI-Systeme haben. Die Regulierungen dienen zwar dazu, Vertrauen und Sicherheit zu gewährleisten. Für europäische Unternehmen können sie aber auch einen signifikanten Wettbewerbsnachteil gegenüber Regionen mit weniger strengen Vorgaben bedeuten: Ressourcen werden für Compliance gebunden, die Innovationsgeschwindigkeit kann leiden.

Als globaler Verband für IT-Governance, Cybersecurity und -Audit sieht ISACA hier eine kritische Führungsaufgabe. Um die Potenziale der KI sicher zu nutzen und die neuen Anforderungen des KI-Gesetzes strategisch zu erfüllen, sind robuste Governance-Rahmenwerke und qualifiziertes Personal unerlässlich. ISACA steht seit über 55 Jahren für den Aufbau von digitalem Vertrauen und die Professionalisierung der Tech-Belegschaft. Mit praxisnahen Leitfäden und Best Practices hilft ISACA Unternehmen dabei, den Spagat zwischen Compliance und Agilität zu meistern und Vertrauen als Wettbewerbsvorteil zu etablieren. Denn Innovation braucht einen sicheren Rahmen.

Balance zwischen Innovation und Compliance

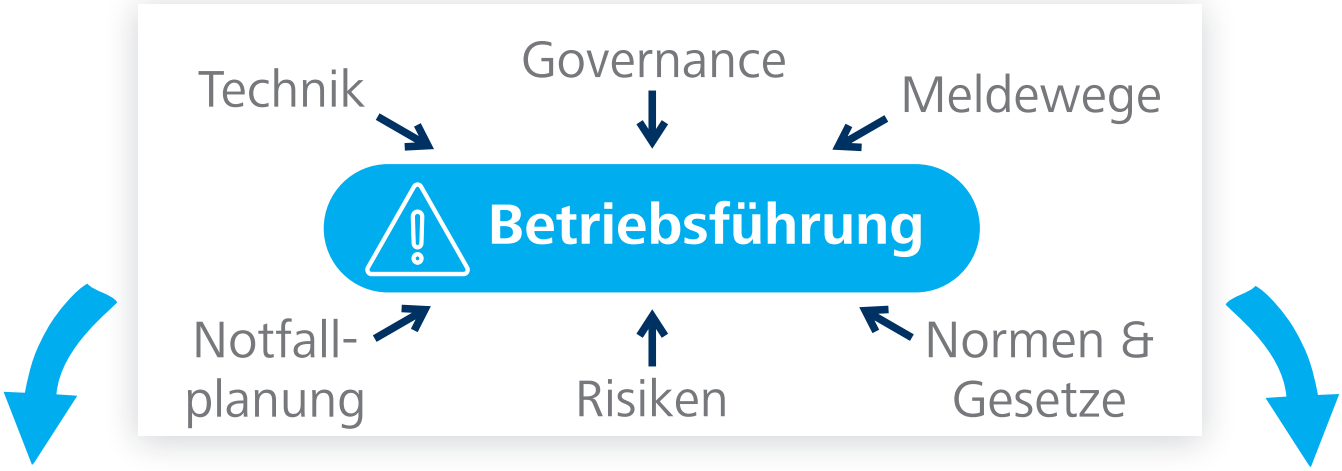
Besonders die Rolle von Auditoren entwickelt sich weiter und wird im Zeitalter der KI-Governance unverzichtbar. Sie sind entscheidend, um KI-Systeme unabhängig zu prüfen, zu steuern und zu sichern. Die Qualifikationslücke stellt dabei ein erhebliches Compliance-Risiko dar: 42 Prozent der Fachleute glauben, ihr KI-Wissen innerhalb der nächsten sechs Monate erheblich verbessern zu müssen.

ISACA (www.isaca.org) adressiert diese Lücke mit international anerkannten Zertifizierungen. Von CISA und CISM bis hin zu neuen, spezialisierten Zertifizierungen wie AAIA (AI Audit & Assurance) und AAISM (Advanced in AI Security Management), vermittelt ISACA das spezifische Wissen, das Fachkräfte benötigen, um sich für die neuen Anforderungen der KI-Ära zu rüsten. Fortbildung kann nicht warten – sie ist entscheidend für den Schutz von Innovationen und die Aufrechterhaltung des Vertrauens in die digitale Wirtschaft. ■

KOMPETENZ SCHAFFT SICHERHEIT
www.airitsystems.de

AirIT SYSTEMS

Sicherheit entsteht dort, wo Silos enden & Zusammenarbeit beginnt.



Unser Lösungsansatz: Compliance, IT & Security - nahtlos verzahnt!

Betriebsführungshandbücher schließen die Lücke zwischen ISMS & Technik.

Jetzt Vorlage kostenlos anfordern!

- ✓ Betriebsführungshandbücher unterstützen IT-Verantwortliche bei einer sicheren und hochwertigen IT-Betriebsführung.
- ✓ Verbessert die betriebliche Effizienz und unterstützt die Einhaltung von Standards wie ISO 27001.
- ✓ **Jetzt Mustervorlage IT-Betriebsführungshandbuch, Schwerpunkt Firewall sichern!**

AirITSystems
IT- und Sicherheitslösungen von erfahrenen KRITIS-Experten
Wir sind ein Gemeinschaftsunternehmen der Flughäfen Hannover und Frankfurt. Unsere Herkunft ist der Flughafen. Damit sind Sicherheit und das Zusammenspiel zahlreicher Komponenten in einem komplexen System unser tägliches Geschäft: eine Vielzahl von Transaktionen, kritische Verfügbarkeit und als klare Anforderung höchste Sicherheit. Diese einzigartige Flughafenerfahrung übertragen wir und unsere zertifizierten Spezialisten mit derselben Sorgfalt auch auf alle anderen Branchen.

www.airitsystems.de

Lernen Sie uns kennen!

07.10. – 09.10.2025
it-sa 2025 Nürnberg
Stand 7-105

it-sa 2025: IT-Sicherheitshersteller ESET stellt die Vertrauensfrage

Sicherheit braucht heute mehr als Technik: Unternehmen müssen auf Herkunft, Rechtskonformität und Verlässlichkeit von Herstellern und Lösungen vertrauen können. ESET gibt auf der it-sa 2025 in Halle 9, Stand 434 fundierte Antworten auf technische, rechtliche und strategische Herausforderungen.

Von Michael Klatte, ESET Deutschland GmbH

Wer die it-sa in Nürnberg besucht, erwartet hauptsächlich neue Produkte. ESET liefert seit Jahren aber mehr als das, nämlich strategische Konzepte für ganzheitliche Cybersicherheit. Ob Multi-Secured Endpoint, Zero Trust oder Prevention First – im Mittelpunkt standen nie einzelne Lösungen, sondern Sicherheitsarchitekturen. Auch 2025 geht es am ESET-Stand nicht um die eine Super-Securitysoftware, sondern um eine Haltung: Vertrauen.

Damit reagiert ESET auf das veränderte Messepublikum. Längst kommen nicht mehr nur technische Spezialisten, sondern auch Firmenchefs. Denn mit Vorgaben wie NIS-2 stehen sie heute persönlich in der Verantwortung für IT-Sicherheit. Sie müssen entscheiden, wem sie ihre Sicherheitsarchitektur anvertrauen und wie diese Entscheidungen nach innen und außen belegbar sind.

ESET beantwortet die Vertrauensfrage auf mehreren Ebenen: mit nachvollziehbarer Herkunft, mit einer skalierbaren Plattform und mit einem modernen Verständnis für die Rolle des Mitarbeiters.

Vertrauensdefizite als Risiko

Die politische und wirtschaftliche Lage erhöht den Druck auf Unternehmen, bei der Auswahl ihrer IT-Sicherheitsanbieter genau hinzusehen. Gesetzliche Vorgaben verlangen klare Verantwortlichkeiten, auch auf Ebene der

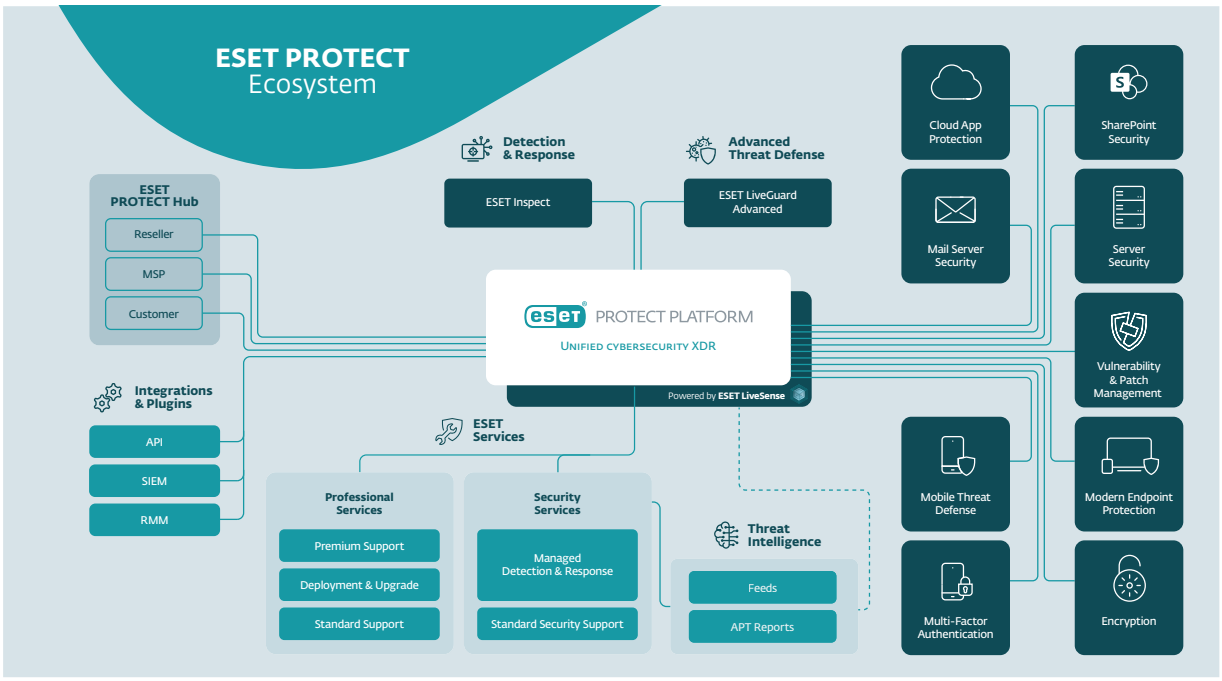


Abbildung 1: Das ESET PROTECT Ecosystem integriert Cloud-Schutz, Endpoint-Sicherheit, Bedrohungsabwehr und zentrale Verwaltung in einer Plattform. (Bild: ESET)

Geschäftsführung. Gleichzeitig verunsichern geopolitische Spannungen viele Entscheider. Die Frage, ob ein Anbieter aus einem Drittstaat im Krisenfall noch rechtssicher agieren kann, wird zur realen Risikoabwägung. Wer IT-Sicherheit auslagert, muss darauf vertrauen können, dass gesetzliche Standards eingehalten und Daten souverän verarbeitet werden.

Herkunft schafft Verlässlichkeit

Im Mai 2025 hat ESET über 1200 IT-Entscheider aus Deutschland, Österreich und der Schweiz befragt, inwieweit die Herkunft eines Security-Herstellers für sie eine Rolle spielt. Die Studie liefert ein klares Bild: Die Herkunft eines IT-Sicherheitsanbieters „Made in EU“ ist für viele Unternehmen zu einem der wichtigsten Auswahlkriterien geworden. Zwei Drittel der Befragten würden sich bei der nächsten Beschaffung gezielt für einen Anbieter aus Europa entscheiden.

In regulierten Branchen wie Gesundheitswesen, Finanzdienstleistung oder Industrie ist in Deutschland die Präferenz für europäische Anbieter besonders hoch. Dort, wo die Einhaltung von DSGVO, NIS-2 oder DORA geprüft wird, zählt nicht nur der technische Funktionsumfang, sondern die Nachvollziehbarkeit von Entwicklung, Support und Datenverarbeitung.

Vertrauen in die Lösung: Eine Plattform, viele Antworten

Vertrauen in den Anbieter allein genügt selbstverständlich nicht, denn auch die Lösung selbst muss technisch überzeugen, regulatorisch belastbar und langfristig tragfähig sein. Für die wachsenden Anforderungen durch Gesetze, Verordnungen und neuerdings auch Cyberversicherer braucht es mehr als punktuelle Schutzmechanismen. Wichtig ist ein konsistenter, kontrollierbarer Sicherheitsansatz, der sich in bestehende Strukturen integrieren lässt und dabei nachvollziehbar bleibt.

ESET bietet als Antwort darauf die ESET PROTECT Plattform. Sie ist modular aufgebaut, cloudbasiert oder lokal installierbar und umfasst Endpoint Security, Mobile Security, Server-Schutz, Full Disk Encryption, Cloud Office Security, XDR-Funktionen, E-Mail-Schutz, Gerätekontrolle, Multi-Faktor-Authentifizierung und mehr. Nahezu alle Module werden über eine zentrale Konsole verwaltet. Die Plattform ermöglicht detaillierte Richtliniendefinition, Mandantenfähigkeit und vollständige Protokollierung zur rechtskonformen Nachweisführung. Das schafft nicht nur technische Übersicht, sondern auch Vertrauen in die Nachvollziehbarkeit und Konformität von Sicherheitsmaßnahmen.

Exemplarisch für die vielen Optimierungen und Verbesserungen, die ESET permanent in seine Technologien und Lösungen einbaut, stehen auf der it-sa-Agenda folgende Neuigkeiten:

_____ Die neue ESET Ransomware Remediation-Funktion erweitert das ESET Ransomware Shield um eine intelligente Backup-Lösung, die im Fall eines Angriffs eine sichere Wiederherstellung der betroffenen Daten ermöglicht. Wichtiger Vorteil: Anders als herkömmliche Backup-Methoden, die auf der sogenannten „Windows Volu-

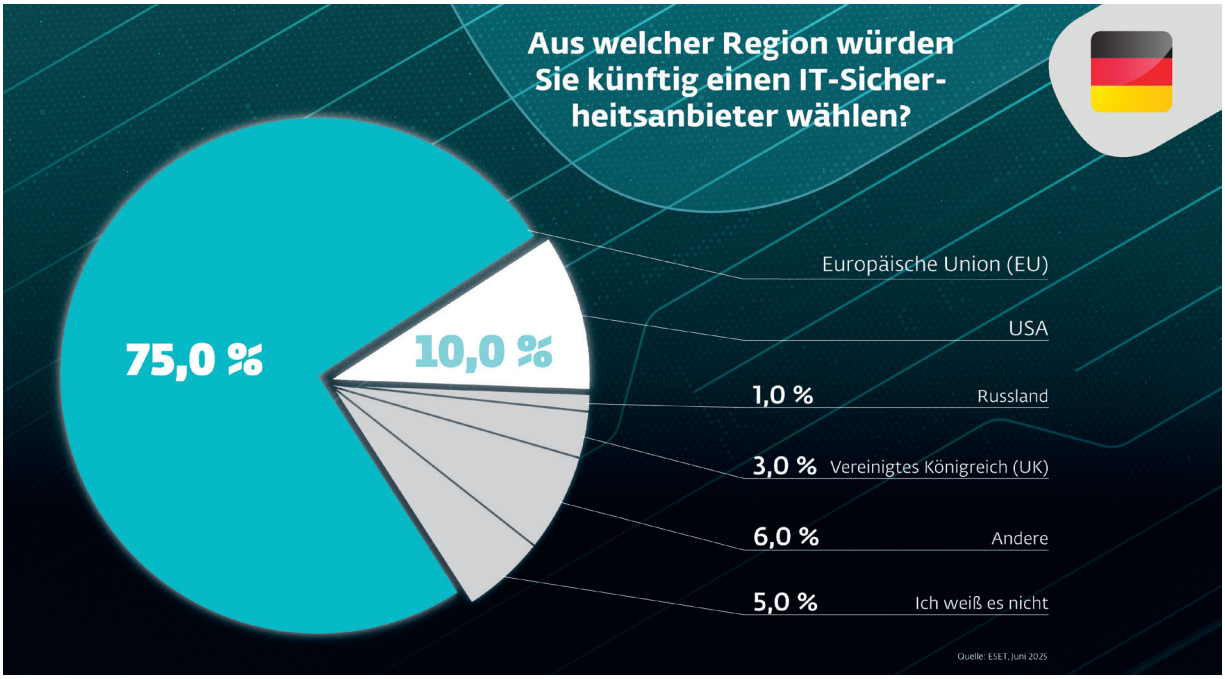


Abbildung 2: Drei Viertel der Befragten bevorzugen einen IT-Sicherheitsanbieter aus der Europäischen Union, während die USA mit 10 % deutlich abgeschlagen auf Platz zwei liegen. (Bild: ESET)

me Shadow Copy“ basieren, kann die ESET-Lösung nicht von Angreifern manipuliert oder gelöscht werden. Die Backups werden in einem geschützten Speicherbereich abgelegt, auf den Schadsoftware keinen Zugriff hat.

_____ ESET Cloud Office Security (ECOS) schützt Microsoft 365 und Google Workspace vor Malware, Phishing und Spam. Zuletzt wurden der Anti-Spoofing- und Homoglyphen-Schutz zur Erkennung und Blockierung von Phishing-Versuchen durch gefälschte E-Mail-Absender und manipulierte URLs hinzugefügt. Die neue E-Mail-Rückruf-Funktion ermöglicht es Administratoren, verdächtige E-Mails nachträglich aus Postfächern zu entfernen. Zudem wurden neue konfigurierbare Dashboards mit anpassbaren Komponenten für eine bessere Übersicht und eine effektivere Richtlinienverwaltung integriert. Die Einbindung in ESET PROTECT sorgt für konsistente Schutzkonzepte in hybriden Arbeitsumgebungen.

ESET
Halle 9, Stand 434
www.eset.de/itsa

_____ Die PROTECT-Plattform ist vollständig API-fähig und erlaubt über ESET Connect die Anbindung an eine Vielzahl von SIEM-, SOAR- oder Ticketing-Systemen. Sicherheitsereignisse können über Syslog exportiert, Workflows automatisiert und Reports in bestehende Audit-Prozesse übernommen werden. So wird die Plattform Teil der Unternehmenssteuerung, nicht nur der IT-Abwehr.

_____ ESET Threat Intelligence bietet ab sofort insgesamt 15 verschiedene Feeds an. Darüber hinaus bietet die Lösung nun drei verschiedene Level für APT-Reports an, die sich im Umfang der Services unterscheiden, von denen Kunden neben den Berichten Gebrauch machen können.

Vertrauen in den Service: ESET MDR

Mit ESET MDR erhalten Unternehmen Zugang zu einem vollständig KI-gestützten Monitoring- und Reaktionsdienst. Die Basis bildet eine automatische Analyse sicherheitsrelevanter Ereignisse durch künstliche Intelligenz in Kombination mit verhaltensbasierter Auswertung. Meldungen erfolgen priorisiert und in Echtzeit über die zentrale Managementkonsole. Für Unternehmen mit hohem Schutzbedarf steht ESET MDR Ultimate zur Verfügung. Diese Version erweitert den KI-basierten Ansatz um direkte Unterstützung durch erfahrene Sicherheitsexperten. Analysten übernehmen bei Bedarf die Detailbewertung, geben konkrete Handlungsempfehlungen oder leiten Incident-Response-Maßnahmen ein. Alle Schritte sind dokumentiert, auditierbar und rechtskonform.

ESET MDR ist auch für Managed Service Provider verfügbar. Über die ESET-MSP-Administrator-Konsole lässt sich der Dienst mandantenfähig verwalten und flexibel abrechnen. Die Kombination aus Automatisierung und menschlicher Expertise schafft Sicherheit auf Augenhöhe – auch für Kunden im Outsourcing-Modell.

Awareness als letzte Verteidigungslinie

Mit dem ESET Cybersecurity Awareness Training (ECAT) adressiert ESET das größte Risiko der Cybersicherheit: den Menschen. Die Plattform bietet modulare, interaktive Schulungen mit Gamification-Elementen, realistischen Phishing-Simulationen und adaptiven Kursen für verschiedene Zielgruppen.

Unternehmen erhalten Reporting-Dashboards, Nutzerfortschrittskontrolle und Möglichkeiten zur automatisierten Nachschulung. Die Inhalte decken Themen wie Social Engineering, Passwortsicherheit, Datenschutz, mobile Sicherheit und Compliance-Fragen ab. Regelmäßige Updates berücksichtigen aktuelle Bedrohungstrends und regulatorische Anforderungen. Wer in seine Mitarbeiter investiert, investiert in eine vertrauenswürdige Sicherheitskultur. ■

Impressum

DATAKONTEXT GmbH

Augustinusstraße 11 A, 50226 Frechen (DE)
Tel.: +49 2234 98949-30
Fax: +49 2234 98949-32
redaktion@datakontext.com,
www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Handelsregister
Amtsgericht Köln, HRB 82299

Bankverbindung:
UniCredit Bank AG, München,
IBAN: DE34 7002 0270 0015 7644 54

Zurzeit gültige Anzeigenpreisliste:
Nr. 43 vom 01. Januar 2025

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel.: +49 6728 289003, anzeigen@kes.de

Media-Daten: Unsere Mediadaten finden Sie online auf www.kes.de/mediadaten.

Herstellungsleitung und Vertrieb:
Dieter Schulz, dieter.schulz@datakontext.com,
Tel.: +49 2334 98949-99

Satz: Dirk Hemke (SatzPro), Krefeld;
Markus Miller (Satz+Bild), München

Druck: QUBUS media GmbH
Beckstraße 10, 30457 Hannover

Titelbild: [M] NürnbergMesse / Thomas Geiger

IT-SICHERHEIT
Management und Technik

<kes>
Die Zeitschrift für
Informations-Sicherheit

Yulia - stock.adobe.com

Wir sind IT-Sicherheit!

Besuchen Sie uns auf der it-sa 2025.

Halle 7 **Stand 106**

IT-Sicherheit ist Vertrauenssache

Machen Sie Ihr Unternehmen NIS2-Ready mit ESET Technologien aus der Europäischen Union

ESET® Digital Security
Progress. Protected.

eset.de/nis2

<kes> + <kes> SPECIAL

Die perfekte Kombination für CISO & Co

- ✓ Verlagsbeilage mit wechselnden Mitherausgebern
- ✓ auf ein Thema fokussierte Beiträge der Mitherausgeber
- ✓ Printausgabe liegt <kes> bei
- ✓ digitales eMagazine kostenfrei verfügbar

weitere Specials hier kostenfrei downloaden:
kes.info/archiv/specials/

- ✓ führende Fachzeitschrift in der IT-Sicherheit
- ✓ hohes technisches Niveau und redaktionell unabhängig
- ✓ offizielles Organ des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- ✓ nur im Abonnement erhältlich unter: datakontext.com/kes

<kes> genauer kennenlernen?
Einfach kostenfreies Probeheft anfordern unter:
kes.info/service/probeheft/

LESEPROBE <kes> AUF DEN FOLGESEITEN

weitere Leseproben unter: kes.info/archiv/leseproben/

DATAKONTEXT

Vererbte Verwundbarkeiten

KI-generierter Code – eine wachsende Bedrohung für die Softwaresicherheit

Generative Modelle künstlicher Intelligenz (KI) unterstützen Entwickler zunehmend beim Programmieren von Software. Was als Revolution der Produktivität gefeiert wird, birgt jedoch erhebliche Risiken für die Cybersicherheit. Unser Autor sieht einen besorgniserregenden Trend: Die wachsende Abhängigkeit von KI-generierten Codevorschlägen könnte so zu einer Flut neuer Sicherheitslücken in aktuellen und zukünftigen Softwareprojekten führen.

Von Daniel dos Santos, Rotterdam (NL)

Das Kernproblem KI-automatisierter Softwareentwicklung liegt in den Trainingsdaten der genutzten Large Language-Models (LLMs): Diese Modelle werden mit enormen Mengen an Code trainiert – in manchen Fällen Open-Source-Code und in vielen Fällen Code, der Sicherheitslücken enthält. Wenn Entwickler generative KI-Tools nutzen, replizieren und verstärken die Modelle anschließend in den Trainingsdaten vorhandene unsichere Programmierpraktiken in beispiellosem Ausmaß.

Besonders problematisch: Die Sicherheitsmängel im generierten Code sind oft subtil und schwer zu erkennen, da sie in syntaktisch korrektem Code eingebettet sind. Dies schafft ein falsches Sicherheitsgefühl bei Entwicklern, die möglicherweise nicht jede Zeile des KI-generierten Codes akribisch überprüfen.

Alarmierender Forschungsstand

Wissenschaftliche Untersuchungen bestätigen diese Bedenken mit alarmierenden Zahlen. Wissenschaftler des Center for Cybersecurity der New York University (NYU) stellten kurz nach dessen Veröffentlichung fest [1], dass etwa 40 % des von GitHub Copilot generierten Codes bekannte Sicherheitslücken enthielten (vgl. Abb. 1).

Ebenso beunruhigend sind die Ergebnisse einer Studie an der Stanford University [2], die zeigte, dass Entwickler, die LLMs verwenden, eher dazu neigen, unsicheren Code zu produzieren – und gleichzeitig ein übermäßiges Vertrauen in dessen Sicherheit zu haben. Diese gefährliche Kombination aus technischen Mängeln und menschlichem Fehlverhalten potenziert die Risiken.

Typische Schwachstellen in KI-Code

Die durch KI-generierte Software eingeführten Schwachstellen umfassen ein breites Spektrum (vgl. Abb. 2):

_____ *Unsichere Standardeinstellungen:* KI-generierte Konfigurationen enthalten oft schwache Sicherheitseinstellungen wie leicht zu erratende Passwörter oder zu großzügige Zugriffsrechte.

_____ *Klassische Schwachstellen:* KI-Modelle generieren häufig Code, der anfällig für lang bekannte Sicherheitsprobleme wie SQL-Injection und Cross-Site-Scripting (XSS) ist.

_____ *Supply-Chain-Angriffe durch Abhängigkeiten:* Ein aktuelles Beispiel hat eine besonders raffinierte Angriffsform gezeigt, bei der Angreifer Softwarepakete mit Namen registrieren, die von KI-Systemen halluziniert wurden, sodass der generierte Code automatisch diese bösartigen Abhängigkeiten einbindet. Gleichzeitig kann KI auch selbstständig unsicheren Code erzeugen und veröffentli-

Abbildung 1: Eine Forschungsarbeit an der NYU [1] fand in 40 % des von Github Copilot generierten Programmcodes bekannte Sicherheitslücken.

Abbildung 2: Typische Schwachstellen (qualitativ) in KI-generiertem Code

chen, der später als Abhängigkeit in anderen Projekten verwendet wird.

_____ *Fehlerhafte Implementierung von Standards und RFCs:* Wenn KI Code basierend auf technischen Standards generiert, können Missverständnisse oder Mehrdeutigkeiten in den Spezifikationen zu kritischen Sicherheitslücken führen. Die Forescout-Forschungsprojekte Amnesia:33 [3] und Name:Wreck [4] haben bereits vor einigen Jahren gezeigt, dass Fehlinterpretationen von RFCs (etwa beim TCP Urgent Pointer und der DNS-Kompression) zu wiederkehrenden Schwachstellen führen.

Dass die meisten dieser Schwachstellen nicht neu sind, hilft dabei wenig. Die KI reproduziert bekannte Sicherheitsprobleme, welche die Cybersecurity-Community seit Jahren zu bekämpfen versucht – nun aber in exponentiell größerem Umfang.

Darüber hinaus können KI-Modelle selbst anfällig für Angriffe sein, die zu Malicious Code führen. Als Beispiele sind hierzu Prompt-Injection (Angreifer gestalten Eingaben so, dass sie Sicherheitsschranken umgehen) und Data-Poisoning (Angreifer schleusen bösartige Daten in die Trainingsphase ein, um später schädliche Ergebnisse zu erzeugen) zu nennen.

Produktivität versus Sicherheit

Die Vorteile der generativen KI für die Softwareentwicklung sind unbestreitbar: Entwickler können Code schneller schreiben, repetitive Aufgaben automatisieren und komplexe Probleme mit KI-Unterstützung lösen. Diese Produktivitätssteigerung hat jedoch ihren Preis: Sicherheitslücken werden dabei in einem Tempo eingeführt, das die menschlichen Kapazitäten zur Erkennung und Behebung überfordert.

Diese wachsende Anhäufung von unbehobenen Sicherheitsmängeln wird oft als „Security Debt" bezeichnet – eine Metapher, welche die langfristigen Kosten kurzfristiger Produktivitätsgewinne veranschaulicht. Je länger diese Schulden unbezahlt bleiben, desto größer wird das Risiko kostspieliger Sicherheitsverletzungen!

Zudem sind die Auswirkungen dieses Problems nicht auf einzelne Unternehmen beschränkt: Da KI-generierter Code auch in Open-Source-Bibliotheken und gemeinsam genutzten Komponenten landet, können sich Schwachstellen kaskadenartig durch das gesamte Software-Ökosystem verbreiten.

Risiken bei Security-Tools

Ein oft übersehenes Risiko betrifft überdies den Einsatz von KI zur Generierung von Sicherheitsmaßnahmen selbst. KI-generierter Code für Sicherheitsanwendungen mag zwar nicht unmittelbar angreifbar sein, kann sich jedoch als ineffektiv beim Erkennen und Blockieren von bösartigem Verhalten erweisen. Dies betrifft beispielsweise

_____ Erkennungsregeln in Netzwerk-Intrusion-Detection-Systemen (NIDS),

Literatur

[1] Hammond Pearce, Baleegh Ahmad, Benjamin Tan, Brendan Dolan-Gavitt, Ramesh Karri, Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions, Dezember 2021, https://arxiv.org/abs/2108.09293

[2] Neil Perry, Megha Srivastava, Deepak Kumar, Dan Boneh, Do Users Write More Insecure Code with AI Assistants?, Dezember 2023, https://arxiv.org/abs/2211.03622

[3] Daniel dos Santos, Stanislav Dashevskyi, Jos Wetzels, Amine Amri, Amnesia:33, How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices, Forescout Research Labs Report, Dezember 2020, www.forescout.com/resources/amnesia33-how-tcp-ip-stacks-breed-critical-vulnerabilities-in-iot-ot-and-it-devices/

[4] Daniel dos Santos, Stanislav Dashevskyi, Amine Amri, Jos Wetzels, Shlomi Oberman, Moshe Kol, Name: Wreck, Breaking and fixing DNS implementations, Forescout Research Labs & JSOF Report, April 2021, www.forescout.com/resources/namewreck-breaking-and-fixing-dns-implementations/

_____ Signaturen in Endpoint-Detection-and-Response-Lösungen (EDR),
_____ YARA-Regeln zur Malware-Erkennung,
_____ aber auch andere Sicherheitsfilter und -mechanismen.

Wenn KI unsichere oder unzureichende Sicherheitsmaßnahmen generiert, entstehen Lücken in der Verteidigungslinie, die Angreifer ausnutzen können – ein doppeltes Risiko für die Cybersicherheit.

Strategien zur Risikominimierung

Um die mit KI-generiertem Code verbundenen Risiken zu minimieren, ist ein mehrdimensionaler Ansatz erforderlich:

_____ **Rigoroser Code-Review:** Menschliche Überwachung bleibt entscheidend, um Sicherheitslücken zu erkennen, die KI-Modelle übersehen. Das Vier-Augen-Prinzip sollte strikt eingehalten werden – besonders bei sicherheitskritischen Komponenten.
_____ **Automatisierte Sicherheitstests:** Die Integration von Sicherheitsanalysetools direkt in die Entwicklungspipeline kann helfen, um Schwachstellen möglichst in Echtzeit zu identifizieren. Tools zur statischen Codeanalyse, Software-Composition-Analysis sowie dynamische Sicherheitstests sollten daher standardmäßig implementiert werden.
_____ **Entwickler-Schulungen:** Die Sensibilisierung von Entwicklern für die potenziellen Fallstricke KI-generierten Codes und die Förderung einer gesunden Skepsis sind unerlässlich. Entwickler sollten verstehen, dass KI ein Werkzeug ist – kein Ersatz für Sicherheitsexpertise.
_____ **Überprüfung von Abhängigkeiten:** Es braucht strenge Kontrollen für Code-Abhängigkeiten, um Supply-Chain-Angriffe zu verhindern. Dazu sollte man alle externen Bibliotheken und Pakete gründlich validieren, bevor man sie in eigene Projekte integriert.
_____ **Besondere Vorsicht bei der Implementierung von Standards:** Wo KI zur Implementierung technischer Standards dient, sollten die Ergebnisse unbedingt von Experten überprüft werden, die mit den Fallstricken und Mehrdeutigkeiten der Spezifikationen vertraut sind.
_____ **Sorgsame KI-Security:** Nicht zuletzt müssen auch KI-Tools und -Modelle selbst sicher entwickelt werden – unter Verwendung von Eingabevalidierung und kontinuierlicher Überwachung.

Fazit

Während generative KI beginnt, die Softwareentwicklung zu revolutionieren, bringt ihre aktuelle Implementierung erhebliche Sicherheitsherausforderungen mit sich. Die Bequemlichkeit und Geschwindigkeit, die sie bietet, sind mit dem Risiko verbunden, eine Flut neuer Schwachstellen in unsere digitale Infrastruktur einzuführen.

Unternehmen sollten KI-gestützte Entwicklungstools dennoch nicht meiden, sondern einen proaktiven und sicherheitsbewussten Ansatz verfolgen. Die Integration von Sicherheitsüberlegungen in jeden Schritt des KI-gestützten Entwicklungsprozesses ist letztlich entscheidend, um die Vorteile dieser Technologie zu nutzen, ohne die Sicherheit und Integrität der Codebasis zu gefährden.

Die Zukunft der sicheren Softwareentwicklung liegt nicht in der kategorischen Ablehnung von KI, sondern in der intelligenten Kombination von KI-Effizienz mit menschlicher Sicherheitsexpertise. Nur so lässt sich das volle Potenzial der generativen KI ausschöpfen, ohne ein unkalkulierbares Sicherheitsrisiko einzugehen. ■

Daniel dos Santos ist Senior Director und Leiter der Forschungsabteilung von Forescouts Cybersecurity-Forschungsabteilung Vedere Labs und ist Mitglied mehrerer Vereinigungen zum Austausch von Bedrohungsdaten wie EE-ISAC, OT-ISAC, ETHOS und CISA JCDC.