Präsentiert von
www.it-business.de

OKTOBER 2025

ISSN 1864-0907 • 7,- €

IT-BUSINESS

IT Security made in Germany

Powered by:

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

G DATA CyberDefense

TRUST IN GERMAN SICHERHEIT

ANZEIGE G DATA

Für eine souveräne und sichere digitale Zukunft – "IT Security made in Germany" als Leitbild

Die digitale Transformation schreitet in rasantem Tempo voran – und mit ihr wachsen die Bedrohungen für unsere IT-Infrastrukturen, Wirtschaft und Gesellschaft. Cyber-Angriffe sind längst Realität. Klar ist: Ohne IT-Sicherheit gibt es keine digitale Souveränität. Genau hier setzt die TeleTrusT-Initiative "IT Security made in Germany" an. Unter dem Dach des Bundesverbands IT-Sicherheit (TeleTrusT) vereint sie deutsche Anbieter von Sicherheitslösungen, um gemeinsame Stärken sichtbar zu machen – in Markt, Politik und öffentlichem Diskurs.

IT-Sicherheit muss zur gesamtgesellschaftlichen Aufgabe werden. Die Vision einer "Cyber-Nation Deutschland", formuliert von BSI-Präsidentin Claudia Plattner, benennt zentrale Handlungsfelder: Cyber-Sicherheit priorisieren, Resilienz stärken, Technologiekompetenz fördern, Digitalisierung vorantreiben, den Cyber-Markt entwickeln – und all das pragmatisch umsetzen.

Der Bundesverband IT-Sicherheit unterstützt diese Vision und hat sie mit einem eigenen Positionspapier untermauert. Doch sie darf kein Appell bleiben. Notwendig sind konkrete Maßnahmen, Investitionen und politische Impulse.

Deutschland und Europa müssen technologische Souveränität aktiv gestalten: durch einen starken IT-Sicherheitsmarkt mit europäischen Anbietern, durch klare gesetzliche Rahmenbedingungen und die konsequente Ablehnung von Verschlüsselungsschwächung oder staatlichen Backdoors. Vertrauen ist das Fundament digitaler Infrastrukturen – und darf nicht verspielt werden.

Die öffentliche Hand trägt besondere Verantwortung: Sie muss nicht nur regulieren, sondern auch Vorbild sein – durch den Einsatz sicherer Technologien, fördernde Vergabepolitik und den Aufbau interoperabler Infrastrukturen. Gerade kleine und mittlere Unternehmen benötigen gezielte Unterstützung, um Innovationen "Made in Germany" zur Marktreife zu bringen.

Diese Sonderpublikation zeigt die Leistungsfähigkeit der deutschen IT-Sicherheitsbranche: Qualität, Integrität und Innovationskraft. Doch diese Wirkung entfaltet sich nur, wenn Politik, Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammenarbeiten – mit dem Ziel, die digitale Zukunft sicher und werteorientiert zu gestalten.

"IT Security made in Germany" ist mehr als ein Slogan: Es ist ein Qualitätsversprechen und Ausdruck einer Haltung, die Sicherheit, Datenschutz und Nutzerfreundlichkeit vereint. Diese Haltung braucht Sichtbarkeit, Unterstützung – und politischen Willen, digitale Abhängigkeiten zu reduzieren und eigene technologische Wege zu gehen.

Cyber-Sicherheit ist kein Hindernis, sondern ein Enabler – für digitale Geschäftsmodelle, für Vertrauen in Technologie und für eine resiliente Gesellschaft. Dass das gelingt, zeigen die hier präsentierten Unternehmen: Deutschland kann Cyber-Nation sein – wenn wir es gemeinsam wollen. □

IT SECURITY MADE IN GERMANY

Die Initiative: Vertrauen hat einen Namen 6

IT-SICHERHEIT UND GESETZGEBUNG

Verantwortlich für die Resilienz: To-Do-Liste für Systemhäuser im Zeitalter von NIS2 und DORA 10

Cybersicherheit für Produkte und Anwendungen: Cyber Resilience Act der EU – was Sie wissen müssen 16

DIGITALE SOUVERÄNITÄT: MEHR VERTRAUEN IN "MADE IN EU"

TeleTrusT Positionspapier: Vision der Cyber-Nation Deutschland 20

Datensouveränität ist alternativlos: Warum Kollaborations-Software "Made in Germany" sein sollte 24

Digitale Souveränität im Gesundheitswesen: Keine Macht den US-Servern 30

REDAKTION

Editorial 3

Impressum / Inserenten 58

CYBERSICHERHEIT

Sicherheit mit System: Warum ein Managed SOC die IT besser schützt als Virenschutz allein 34

Cybersicherheitsstrategie: Sechs Gartner-Empfehlungen für CISOs 40

AWARENESS DER MITARBEITER

BSI appelliert an Chefetage: In acht Schritten zum Security-Awareness-Programm 46

44 % denken, sie seien sicher: Deutschen Angestellten fehlt das Bewusstsein für Cyberangriffe 48

KÜNSTLICHE INTELLIGENZ ALS IT-RISIKO

Beratung und Überwachung bei Künstlicher Intelligenz: Was Datenschutzbehörden für die KI-Aufsicht planen 50

Neue Herausforderungen für den Identitätsschutz: Wie mit KI der Identitätsdiebstahl noch bedrohlicher wird 54

TeleTrusT-Initiative "IT Security made in Germany"

"ITSMIG" ("IT Security made in Germany") wurde 2005 auf Initiative des Bundesministeriums des Innern (BMI), des Bundesministeriums für Wirtschaft und Technologie (BMWi) sowie Vertretern der deutschen IT-Sicherheitswirtschaft etabliert und 2008 in einen eingetragenen Verein überführt. Sowohl BMI als auch BMWi hatten eine Schirmherrschaft übernommen.
Nach intensiven Erörterungen sind TeleTrusT und ITSMIG 2011 übereingekommen, dass sich auf ihren Handlungsfeldern Synergien erschließen lassen. Zukünftig werden die ITSMIG-Aktivitäten unter dem Dach des TeleTrusT als eigenständige Arbeitsgruppe "ITSMIG" fortgeführt.

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

Die TeleTrusT-Arbeitsgruppe "ITSMIG" verfolgt das Ziel der gemeinsamen Außendarstellung der an der Arbeitsgruppe mitwirkenden Unternehmen und Institutionen gegenüber Politik, Wirtschaft, Wissenschaft und Öffentlichkeit auf deutscher, europäischer bzw. globaler Ebene. BMWi und BMI sind im Beirat der Arbeitsgruppe vertreten.

ISX IT-Security Digital Conference

EMPOWERING DIGITAL SOVEREIGNTY & SECURE AI INNOVATION

18. November | Digital

WERDE PARTNER

Du möchtest Partner der ISX werden?

Dann melde Dich bei mir!
Marlene Stelmach
E-mail: marlene.stelmach@vogel.de

ERLEBE DIE DIGITALE ISX!

Sichere Dir Dein kostenfreies Ticket unter
www.isxconference.de/digital#Anmeldung

EINE VERANSTALTUNG DER
VOGEL IT AKADEMIE

Vertrauen hat einen Namen

Mit der Vergabe des Vertrauenszeichens "IT Security made in Germany" an deutsche Anbieter erleichtert der Bundesverband IT-Sicherheit e.V. (TeleTrusT) Endanwendern und Unternehmen die Suche nach vertrauenswürdigen IT-Sicherheitslösungen.

Träger des Vertrauenszeichens "IT Security made in Germany" (Stand 11.09.2025)

- 8com GmbH & Co. KG
- Accellence Technologies GmbH
- AceBIT GmbH
- achelos GmbH
- Achtwerk GmbH & Co. KG
- ads-tec GmbH
- agilimo Consulting GmbH
- AirID GmbH
- Alpha Strike Labs GmbH
- Alter Solutions Deutschland GmbH
- ANMATHO AG
- Anqa IT-Security GmbH
- Antago GmbH
- APRO Computer & Dienstleistung GmbH
- ASOFTNET
- arcitects IT Security GmbH
- arian IT Service GmbH
- ATIS systems GmbH
- Atruvia AG
- AUCONET Solutions GmbH
- AUTHADA GmbH
- authenton GmbH
- AWARE7 GmbH
- axxessio GmbH
- Bare.ID GmbH
- BAYOOSOFT GmbH
- Bechtle GmbH & Co. KG
- Beta Systems IAM Software AG
- Biteno GmbH
- blueteam GmbH
- Bosch CyberCompare
- Build38 GmbH
- Bundesdruckerei GmbH
- BvL.com GmbH
- CBT Systems & Services GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- CERTIX IT-Security GmbH
- Cherry Digital Health GmbH
- COGNITUM Software Team GmbH
- COMback Holding GmbH
- comcrypto GmbH
- comforte AG
- comtime GmbH
- Condition-ALPHA Digital Broadcast Technology Consulting
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- Cybersense GmbH
- dacoso GmbH
- dal33t GmbH
- DARZ GmbH
- DATAGROUP Defense IT Services GmbH
- DATAKOM GmbH
- DATUS AG
- Dawa Systems GmbH
- DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
- DERMALOG Identification Systems GmbH
- Detack GmbH
- DF Deutsche Fiskal GmbH
- DFN-CERT Services GmbH
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- Dirk Losse Consulting
- ditis Systeme Niederlassung der JMV GmbH & Co.
- Dreyfield & Partner Deutschland GmbH
- DriveLock SE
- D-Trust GmbH
- DTS Systeme GmbH
- EBRAND AG
- eCom Service IT GmbH
- ecsec GmbH
- EgoMind GmbH
- enclaive GmbH
- Enginsight GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- essentry GmbH
- evolutionQ GmbH
- Exploit Labs GmbH
- FAST LTA GmbH
- floragunn GmbH
- FP Digital Business Solutions GmbH
- FZI Forschungszentrum Informatik
- G DATA CyberDefense AG
- genua GmbH
- glacier ac GmbH
- GORISCON GmbH
- HDPnet GmbH
- HiScout GmbH
- HK2 Rechtsanwälte
- i2solutions GmbH
- if(is) - Institut für Internet-Sicherheit
- Infineon Technologies AG
- INFODAS GmbH
- Inlab Networks GmbH
- INNOSYSTEC GmbH
- innovaphone AG
- Insentis GmbH
- INSYS MICROELECTRONICS GmbH
- intarsys GmbH
- intelliCard Labs GmbH
- isits AG International School of IT Security
- ISL Internet Sicherheitslösungen GmbH

Die Verwendung des markenrechtlich geschützten TeleTrusT-Vertrauenszeichens "IT Security made in Germany" wird interessierten Anbietern durch TeleTrusT auf Antrag und bei Erfüllung der nachstehenden Kriterien zeitlich befristet gestattet:

1. Der Unternehmenshauptsitz muss in Deutschland sein.
2. Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.
3. Die angebotenen Produkte dürfen keine versteckten Zugänge ("Backdoors") enthalten.
4. Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in Deutschland stattfinden.
5. Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen.

Die aktuelle Liste können Sie einsehen unter: www.teletrust.de/itsmig/zeichentraeger □

- ITConcepts PSO GmbH
- ITSG GmbH
- itWatch GmbH
- keepbit IT-SOLUTIONS GmbH
- keyONE GmbH
- KOBIL GmbH
- Kopiaconsulting GmbH
- KraLos GmbH
- Kroll Strategieberatung GmbH
- LANCOM Systems GmbH
- LEIBOLD Sicherheits- und Informationstechnik GmbH
- limes datentechnik® gmbh
- Linogate GmbH
- LocateRisk UG
- MACONIA GmbH
- maincubes Holding & Service GmbH
- Maltego Deutschland GmbH
- MaskTech GmbH
- Materna Virtual Solution GmbH
- MB connect line GmbH
- MGR Integration Solutions GmbH
- Mitigant GmbH
- M&H IT-Security GmbH
- MTRIX GmbH
- Mühlbauer ID Services GmbH
- NCP engineering GmbH
- NetComProtect
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- Nexis GRC GmbH
- nicos AG
- nicos cyber defense GmbH
- Nimbus Technologieberatung GmbH
- OctoGate IT Security Systems GmbH
- ondeso GmbH
- ONEKEY GmbH
- Opexa Advisory GmbH
- OTARIS Interactive Services GmbH
- O&O Software GmbH
- P3KI GmbH
- pen.sec AG
- Pently GmbH
- PFALZKOM GmbH
- Pix Software GmbH
- PORTFORMANCE GmbH
- procilon GmbH
- ProLog GmbH
- PSW GROUP GmbH & Co. KG
- QGroup GmbH
- real-cis GmbH
- RedMimicry GmbH
- retarus GmbH
- Robin Data GmbH
- Rohde & Schwarz Cybersecurity GmbH
- r-tec IT Security GmbH
- SAMA PARTNERS Business Solutions GmbH
- sayTEC AG
- Schönhofer Sales and Engineering GmbH
- SCHUTZWERK GmbH
- Schwarz Cyber Technologies GmbH & Co. KG
- Secorvo Security Consulting GmbH
- secrypt GmbH
- SECUDOS GmbH
- SECUINFRA GmbH
- secunet Security Networks AG
- Secure Service Provision GmbH
- Securepoint GmbH
- SECURITYSQUAD GmbH
- secuvera GmbH
- SEPPmail - Deutschland GmbH
- sequrium GmbH
- SerNet GmbH
- signotec GmbH
- SoSafe GmbH
- Spike Reply GmbH
- SRC Security Research & Consulting GmbH
- Star Finanz GmbH
- Steganos Software GmbH
- suresecure GmbH
- SVA System Vertrieb Alexander GmbH
- syracom consulting AG
- TDT AG
- TE-SYSTEMS GmbH
- Tech-Prax GmbH
- telent GmbH
- TG alpha GmbH
- TKUC GmbH
- TÜV Informationstechnik GmbH
- TÜV Rheinland i-sec GmbH
- TÜV SÜD Akademie GmbH
- TWINSOFT biometrics GmbH & Co. KG
- Uniscon GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- VisionmaxX GmbH
- Voleatech GmbH
- water IT Security GmbH
- whitemacs GmbH
- Würzburger Versorgungs- und Verkehrs GmbH
- XignSys GmbH
- XnetSolutions KG
- Zertificon Solutions GmbH

Transparenz schafft Sicherheit

Die hochsichere Cloud ist Open-Source-basiert

Open Source ist kein Sicherheitsrisiko, wie immer noch viele denken – im Gegenteil erhöht quelloffene Software die Sicherheit. Auch der erste für Verschlusssachen freigegebene Cloud-Stack in Deutschland beruht maßgeblich auf Open-Source-Bausteinen. Von Andreas Rückriegel, secunet

In einer Welt zunehmender geopolitischer Spannungen ist digitale Souveränität kein abstraktes Ziel, sondern eine Notwendigkeit. Gerade öffentliche Stellen und kritische Infrastrukturen (KRITIS) benötigen Kontrolle über ihre Daten und die Gewissheit, dass diese wirklich sicher sind – auch und vor allem in der Cloud. Für Unternehmen, die Betriebsgeheimnisse schützen wollen, gilt ähnliches. Doch die Realität sieht oft anders aus, digitale Souveränität spielt bei der Wahl des Cloud-Anbieters oft nur eine untergeordnete Rolle. Dabei muss klar sein: Wer vorrangig oder gar ausschließlich auf proprietäre Technologie US-amerikanischer Anbieter setzt, gibt einen Teil seiner Unabhängigkeit her. Das Gegenmodell sind souveräne Cloud-Angebote Made in Germany. Meist beruhen diese Lösungen auf Open-Source-Bausteinen – und zwar aus gutem Grund: Quelloffene Software ist die sicherere und auf Dauer günstigere Alternative zu der proprietären, intransparenten Technologie der US-basierten Hyperscaler.

Nachprüfbarkeit statt „Black Box“

Ist eine Software, deren Quellcode von jedem eingesehen werden kann, nicht per se unsicher? Im Gegenteil: Kennt ein Hacker beispielsweise den Verschlüsselungsmechanismus einer Anwendung, wird er die Daten dennoch nicht entschlüsseln können. Die Einsehbarkeit der Funktionsweise ist also kein Risiko. Mangelnde Einsehbarkeit hingegen schon: Dann ist nicht zu ermitteln, ob eine Software z. B. Sicherheitslücken, Hintertüren oder auch einen „Kill-switch“ enthält.

Daher sind Open-Source-Lösungen vorzuziehen – nicht trotz, sondern gerade wegen hoher Sicherheitsanforderungen. Die Transparenz verhindert zudem den berüchtigten Vendor-Lock-in, also die Abhängigkeit von einem einzelnen Anbieter. Durch diesen Effekt müssen Verwaltungen mitunter spätere unerwünschte Änderungen des Funktionsumfangs oder drastische Erhöhungen von Lizenzgebühren einfach hinnehmen – schließlich besteht keine Ausweichmöglichkeit zu einem anderen Anbieter. Low-Code/No-Code-Plattformen beeindrucken anfangs mit hohem Tempo, führen dann aber in die Sackgasse in Form vielfältiger

Abhängigkeiten. Open Source ist das adäquate Gegenmittel.
Ein weiterer Punkt: In der deutschen Verwaltung existieren unzählige Fachverfahren, für deren Modernisierung jetzt ein Zeitfenster besteht. Es lohnt sich, sie neu zu denken und auf offene, modulare Cloud-native Architekturen zu setzen. Hierfür bietet secunet die ideale Entwicklungs- und Betriebsplattform.

Ein souveräner Weg in die Cloud

Für Unternehmen und Behörden mit besonderen Sicherheitsanforderungen hat secunet ein Portfolio Open-Source-basierter, souveräner Cloud-Lösungen aufgebaut, die eine große Bandbreite von Compliance-Anforderungen abdecken können: von der Public Cloud mit IT-Grundschutz-Zertifikat, C5-Testat und zertifizierten deutschen Rechenzentren bis hin zur hochsicheren Private-Cloud-Lösung für besonders schützenswerte Daten bis hin zu Verschlusssachen. Alles ist miteinander kombinierbar, bei Bedarf auch mit anderen Anbietern im Sinne eines Multi-Cloud-Setups.
Im Mai 2025 erhielt die SINA Cloud von secunet als erster Cloud-Stack eine Einsatzerlaubnis des BSI für Verschlusssachen bis einschließlich der Geheimhaltungsstufe GEHEIM. Diese Lösung basiert, wie die anderen Cloud-Angebote von secunet auch, maßgeblich auf Open-Source-Technologie.
Zunächst steht die SINA Cloud als On-Premises-Lösung bereit, die Kunden in ihren Rechenzentren selbst betreiben. Darüber hinaus ist eine von secunet betriebene Version als Infrastructure as a Service (IaaS)-Lösung in Vorbereitung. In dieser Variante wird die Plattform in deutschen, zertifizierten Rechenzentren von secunet laufen. Das entlastet vor allem Organisationen, die mit Verschlusssachen oder anderen hochsensiblen Daten umgehen müssen, aber keine Ressourcen für den Betrieb einer eigenen Cloud-Plattform dafür aufbauen wollen oder können.

KI-Anwendungen aus der Cloud

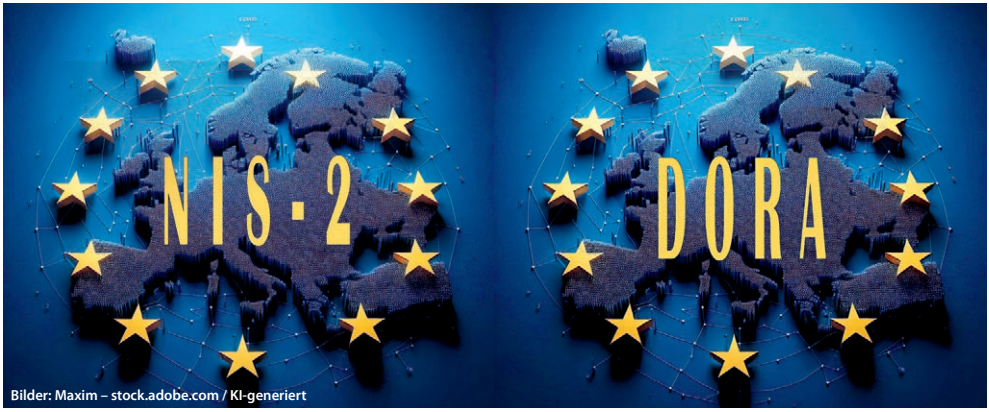
Bereits heute nutzen Kooperationspartner wie die Telekom die SINA Cloud als Grundlage für ihre eigenen Angebote. Zudem hat secunet ein gemeinsames Angebot mit NVIDIA und Hewlett Packard Enterprise (HPE) im Bereich Künstliche Intelligenz (KI) angekündigt. Diese Lösung wird dafür sorgen, dass moderne KI-Anwendungen in hochsensiblen Bereichen eingesetzt werden können – und zwar ohne lange Vorlaufzeiten. So kommen KI-Initiativen schnell vom PoC-Status in den rechtssicheren Praxisbetrieb – trotz höchster Anforderungen bei Regulatorik und Sicherheit.
Dieses Beispiel zeigt: Eine souveräne, Open-Source-basierte Cloud-Plattform Made in Germany kann nicht nur höchste Sicherheitsanforderungen bedienen und damit die Cloud-Transformation weiter vorantreiben. Sie kann auch darüber hinaus die Grundlage für zukunftsweisende Technologie-Innovationen liefern. ■

Andreas Rückriegel ist Vice President Cloud Services bei secunet.

To-Do-Liste für Systemhäuser im Zeitalter von NIS2 und DORA

NIS2 und DORA sind zwei große regulatorische IT-Themen. Doch was bedeutet ihre Umsetzung in der Praxis? Ein Systemhaus-Experte klärt auf, wie solche Projekte tatsächlich gestartet werden und welche System-Komponenten betrieben werden, um erfolgreich die Vorgaben zu erfüllen.

Von Dr. Stefan Riedl, IT-BUSINESS



Bilder: Maxim – stock.adobe.com / KI-generiert

Das Systemhaus achelos hat sich auf Cybersicherheit und digitale Identitäten spezialisiert und begleitet Unternehmen bei der Umsetzung regulatorischer Anforderungen wie NIS2 und DORA. Das fängt bei der strategischen Beratung an und geht über die Integration sicherheitskritischer Komponenten bis hin zum resilienten Betrieb.

Dr. Michael Jahnich, Direktor für Geschäftsentwicklung bei achelos, erläutert die wichtigsten Unterschiede in den Anforderungen zwischen NIS2 und DORA: „NIS2 ist eine sektorübergreifende Richtlinie, die auf eine bessere Cybersicherheit in kritischen Bereichen wie Energie, Gesundheit, Verkehr oder IT abzielt. DORA richtet sich hingegen speziell an Finanzunternehmen und deren IT-Dienstleister." Während NIS2 vor allem grundlegende Sicherheitsmaßnahmen und Meldepflichten verlangt, geht DORA deutlich tiefer ins IKT-Risikomanagement (Informations- und Kommunikationstechnologie). Dazu gehören laut Jahnich unter anderem regelmäßige Penetrationstests und konkrete Vorgaben zum Umgang mit ausgelagerten IT-Diensten. Kurz gesagt: NIS2 ist breiter angelegt, DORA regelt hingegen Details.

Public Key Infrastructure (PKI)

Bei achelos setzt man bei den Regelwerken stark auf eine Public Key Infrastructure (PKI). Der Manager führt aus: „Eine PKI stellt digitale Identitäten für Benutzer, Geräte und Dienste bereit." Sie ermöglicht demnach zertifikatsbasierte Authentifizierung, Ende-zu-Ende-Verschlüsselung und digitale Signaturen und sorgt dafür, dass sich Geräte und Personen sicher identifizieren können und Daten verschlüsselt übertragen werden. Genau diese kryptografischen Verfahren sind in NIS2 (Art. 21) und DORA (Art. 5, 9) explizit gefordert. In Kombination mit einem HSM (Hardware Security Module) zur Schlüsselabsicherung und einem Key Management System zur Prozesssteuerung entsteht eine hochsichere, skalierbare und auditierbare Infrastruktur.

IAM-Konzept gefordert

Doch wie können Unternehmen sicherstellen, dass ihre Zugriffs- und Identitätsmanagementsysteme den neuen EU-Regulierungen entsprechen. Laut Jahnich ist hier ein IAM-Konzept (Identity and Access Management) von entscheidender Bedeutung. Es handelt sich um ein Rahmenwerk und ein System von Prozessen und Technologien, die es Organisationen ermöglichen, digitale Identitäten und deren Zugang zu Ressourcen innerhalb eines Netzwerks oder einer Organisation zu verwalten. IAM sorgt dafür, dass die richtigen Personen Zugriff auf die richtigen Ressourcen zur richtigen Zeit und aus den richtigen Gründen haben. Die Hauptkomponenten von IAM umfassen:

- Benutzerverwaltung: Verwaltung von Benutzeridentitäten und -profilen, einschließlich der Erstellung, Pflege und Löschung von Benutzerkonten.
- Authentifizierung: Sicherstellen, dass Benutzer sind, wer sie vorgeben zu sein, oft durch Passwörter, biometrische Daten oder andere Authentifizierungsmethoden.
- Autorisierung: Bestimmen, welche Ressourcen einem Benutzer basierend auf seiner Identität und seinen Rollen zugänglich gemacht werden sollten.
- Rollenbasierte Zugriffskontrolle (RBAC): Definition und Verwaltung von Zugriffsrechten basierend auf Benutzerrollen innerhalb der Organisation.
- Single Sign-On (SSO): Bereitstellung eines zentralen Authentifizierungsdienstes für den Zugriff auf mehrere Anwendungen mit einem einzigen Anmeldevorgang.
- Multi-Faktor-Authentifizierung (MFA): Erhöhung der Sicherheit durch die Anforderung mehrerer Verifizierungsfaktoren vor dem Gewähren von Zugriff.

Das Gesamtkonzept muss stimmen

„IAM spielt eine kritische Rolle im Bereich der Cybersicherheit und im IKT-Risikomanagement, indem es hilft, das Risiko von unautorisiertem Zugriff und Datenverletzungen zu minimieren und die Einhaltung von Datenschutz- und Compliance-Anforderungen zu unterstützen", so Jahnich. Gefordert sei ein systemisches IAM-Konzept mit Multi-Faktor-Authentifizierung, rollenbasierter Zugriffskontrolle, starker Authentisierung und zentralem Credential-Management. Mit einem CMS (Credential-Management-System) können Unternehmen Smartcards oder Tokens verwalten, PIN-Vorgaben definieren, verlorene Medien sperren und Benutzer zentral steuern. Kombiniert mit einer PKI und einem unternehmensweiten Rollenmodell lassen sich Zugriffsvorgänge sicher und nachweisbar gestalten – wie es NIS2 und DORA fordern.

Zentrale Systemkomponenten

So stehen fünf technologische Kernsysteme im Fokus bei der Umsetzung solcher Projekte:

- PKI: zertifikatsbasierte Authentifizierung & Verschlüsselung

⇨

- HSM: physisch abgesicherte Schlüsselaufbewahrung
- KMS: operatives Schlüsselmanagement & Zugriffskontrolle
- CLM: automatisiertes Zertifikats-Lifecycle-Management
- CMS: Verwaltung digitaler Identitätsträger

„Diese Komponenten sind einzeln wirksam, entfalten aber im Zusammenspiel ihre volle Stärke – mit vollständiger Auditierbarkeit und Compliance-Fähigkeit", kommentiert der Direktor für Geschäftsentwicklung.

Die Rolle von CMS

Unter CMS verstehen IT-ler häufig „Content-Management-System". Im NIS2-DORA-Umfeld geht es dabei aber um „Credential-Management-Systeme", die bei der Erfüllung der Anforderungen von NIS2 und DORA wichtig sind. „Ein CMS steuert die Ausgabe, Verwaltung und Sperrung physischer oder virtueller Identitätsträger – beispielsweise Smartcards oder Tokens", so Jahnich. „Es definiert PIN-Richtlinien, überwacht Nutzungsverläufe und ermöglicht die zentrale Governance von Zugriffsrechten." In Kombination mit zertifikatsbasierter Authentifizierung entstehe so eine starke MFA-Struktur – ein zentrales Element in beiden Regelwerken.

DORA, der Finanzsektor und die IKT-Dienstleister

Welche spezifischen Sicherheitsmaßnahmen fordert DORA im Finanzsektor für IKT-Dienstleister? Jahnich: „DORA verpflichtet IKT-Dienstleister im Finanzsektor zu umfassenden Sicherheitsmaßnahmen. Dazu zählen ein strukturiertes IKT-Risikomanagement, regelmäßige Penetrationstests (beispielsweise TLPT) sowie dokumentierte Prozesse zur Meldung von Sicherheitsvorfällen." Zudem verlange DORA klare Kontrollen bei Auslagerungen – etwa durch Exit-Strategien, Zugriffsschutz und vertraglich geregelte Sicherheitsstandards. Dienstleister müssen nachweisen, dass ihre Systeme technisch resilient, überwacht und sicher integriert sind – auch im Zusammenspiel mit den IT-Systemen ihrer Finanzkunden.

Der erweiterte Anwendungsbereich von NIS2

NIS2 hat den Anwendungsbereich deutlich erweitert: Neben klassischen KRITIS-Sektoren wie Energie, Gesundheit, Transport und Trinkwasser werden nun auch Bereiche wie Post- und Kurierdienste, Abfallwirtschaft, Hersteller kritischer Produkte (beispielsweise Elektronik, Maschinen, Chemikalien), digitale Infrastruktur (beispielsweise Cloud, DNS, Rechenzentren), Lebensmittelerzeugung sowie Teile der öffentlichen Verwaltung reguliert. Die Kriterien zur Einordnung orientieren sich an Unternehmensgröße, Umsatz und kritischer Bedeutung. Auch viele Mittelständler sind nun regulierungspflichtig.

Systemhäuser implementieren NIS2 und DORA

Systemhäuser wie achelos begleiten Unternehmen über alle Projektphasen hinweg – von der Anforderungsanalyse bis zum langfristigen Betrieb. „In der Planungsphase werden regulatorische Vorgaben mit unternehmensspezifischen Anforderungen abgeglichen, Sicherheitskonzepte entwickelt und eine passende Lösungsarchitektur entworfen", berichtet der Manager aus der Praxis. Anschließend erfolge in der Bereitstellung die Integration technischer Komponenten in bestehende Infrastrukturen, ergänzt durch Konfiguration, Tests und Schulungen. Die Inbetriebnahme umfasst Systemtests, Dokumentation und die technische Übergabe. Im Betrieb übernehmen Systemhäuser häufig Aufgaben wie Administration, Monitoring, Support oder Managed Services – auch in hochverfügbaren Umgebungen. Durch diese Unterstützung können Unternehmen sicherstellen,

dass ihre technischen Maßnahmen regulatorisch konform, nachhaltig betreibbar und revisionssicher umgesetzt werden, so der Anspruch.

Herausforderungen für IT-Dienstleister

Was bedeutet das für IT-Dienstleister, die solche Projekte übernehmen. Zunächst einmal stehen sie stärker in der Pflicht als bisher. „Wenn sie für Finanzunternehmen oder kritische Infrastrukturen arbeiten, müssen sie selbst nachweisen, dass ihre IT-Systeme sicher, stabil und überprüfbar sind", sagt Jahnich. Dazu gehören eigene Maßnahmen zur IT-Sicherheit, dokumentierte Prozesse für Vorfallmeldungen, technische Schutzmechanismen sowie die Teilnahme an Audits oder Penetrationstests. Damit seien IT-Dienstleister künftig nicht nur technische Zulieferer, sondern Teil der regulatorisch verantwortlichen Wertschöpfungskette.

Was bedeuten NIS2 und DORA für IT-Dienstleister?

Erweiterte Verantwortlichkeiten
IT-Dienstleister stehen mit NIS2 und DORA vor gestiegenen Anforderungen. Sie müssen verstärkte Cybersicherheitsmaßnahmen implementieren und signifikante Vorfälle melden. Im Finanzsektor sind IT-Anbieter verpflichtet, strenge IKT-Risikomanagementanforderungen zu erfüllen, die umfassende Sicherheitstests, Überwachung und regelmäßige Berichterstattung umfassen.

Compliance und Zertifizierung
Beide Regelwerke verlangen von IT-Dienstleistern, ihre Sicherheitsprotokolle zu überprüfen und möglicherweise neu zu strukturieren, um den vorgeschriebenen Standards zu entsprechen.

Erhöhte Zusammenarbeit
IT-Dienstleister müssen eng mit ihren Kunden und behördlichen Stellen zusammenarbeiten, um Sicherheitsanforderungen zu erfüllen und eine reibungslose Zusammenarbeit im Krisenfall sicherzustellen.

Marktchancen und Wettbewerbsfähigkeit
IT-Dienstleister, die sich erfolgreich an die neuen Anforderungen anpassen und die Einhaltung der Vorschriften sicherstellen, können ihren Kundenstamm erweitern und ihre Marktposition stärken.

Risiko- und Krisenmanagement
Es wird erwartet, dass IT-Dienstleister effektive Strategien für Risiko- und Krisenmanagement entwickeln, um Ausfallzeiten und finanzielle Verluste ihrer Kunden zu minimieren und die kontinuierliche Dienstleistungsbereitstellung zu gewährleisten. □


Bild: achelos

Kurzvita: Dr. Michael Jahnich

Dr. Michael Jahnich ist Direktor für Geschäftsentwicklung bei achelos in Paderborn. Seit 2020 verantwortet er den Bereich der Planung und Lieferung von Key-Management-Lösungen, insbesondere Public-Key-Infrastrukturen, für industrielle und moderne Verkehrsanwendungen. Jahnich ist promovierter Elektroingenieur der Automatisierungs- und Regelungstechnik und seit mehr als 25 Jahren in dem Thema Cybersicherheit in unterschiedlichen Anwendungsgebieten tätig.

Datensouveränität „Made in Germany“

In der digitalen und vernetzten Welt ist ein belastbares IT-Sicherheitskonzept unverzichtbar für sichere und effiziente Geschäftsprozesse. Für europäische Firmen bedeutet das, ihre sensiblen Daten zu schützen und dabei gesetzliche Vorgaben einzuhalten. Unternehmen sehen sich heutzutage mit immer komplexeren Cyberbedrohungen konfrontiert, während der Schutz und die Kontrolle über sensible Daten zunehmend an Bedeutung gewinnen. Welche Maßnahmen sollte man ergreifen, um Datensouveränität „Made in Germany“ effektiv umzusetzen?

Ein zukunftsfähiges IT-Sicherheitskonzept muss technische Qualität, regulatorische Konformität, vertrauenswürdige Partnerschaften und die Wahrung der Datensouveränität berücksichtigen. Es gilt: Wer nicht weiß, wo und wie seine Daten verarbeitet werden, riskiert die Kontrolle über seine Sicherheit.

Ein modernes Sicherheitskonzept muss ganzheitlich gedacht und zentral gesteuert sein. Modulare Lösungen sorgen für Flexibilität bei neuen Anforderungen. Skalierbarkeit verhindert Sicherheitslücken beim Unternehmenswachstum. Nicht nur die Integration von VPN, Firewalls, Endpoint-Security oder Zero Trust zählt. Entscheidend ist die Strategie dahinter: Welche Daten sind schützenswert? Wer erhält wann Zugriff? Wie werden Zugriffsrechte verwaltet?

Datensouveränität als strategisches Ziel

Datensouveränität ist längst mehr als nur ein theoretisches Konzept und sollte für Unternehmen ein strategisches Ziel sein. Das bedeutet, jederzeit zu wissen, wo Daten gespeichert sind und wie sie verarbeitet werden. Souveränität bedeutet: Keine Abhängigkeit von undurchsichtigen Systemen. Mit zertifizierten Anbietern aus Deutschland bleibt die Kontrolle über Technik und Datenschutz. Compliance ist nur möglich, wenn Datensouveränität gewährleistet ist. Diese lässt sich nur dann zuverlässig erreichen,

wenn auch die eingesetzten Technologien transparent, nachvollziehbar und rechtlich abgesichert sind.
IT-Security „Made in Germany“ steht für Transparenz, Verlässlichkeit und Datenschutz.

„Made in Germany" – flexibel und sicher

Im globalen Wettbewerb gewinnen die Herkunft und Transparenz von IT-Lösungen zunehmend an Bedeutung. Als deutscher Hersteller steht NCP für IT-Security „Made in Germany“. So leisten wir unseren Beitrag zu einer wichtigen gesellschaftlichen Aufgabe – Anwendern in Deutschland und Europa erstklassige Alternativen zu bieten.
Für die Nutzer unserer Lösungen im VS-NfD Umfeld ist das selbstverständlich. Doch auch bei Großunternehmen, im Public & Government Bereich sowie im Mittelstand gilt für NCP: Hochsensible Informationen verdienen konsequenten Schutz.
Unternehmen und Behörden legen zunehmend Wert auf Partner, deren Produkte datenschutzkonform sind und deren Entwicklungsprozesse transparent nachvollziehbar sind. IT-Security „Made in Germany“ ist ein Qualitäts- und Sicherheitsversprechen: nachvollziehbare Entwicklung, rechtliche Absicherung und uneingeschränkte Kontrolle über die eigenen Daten.
NCP erfüllt diese Anforderungen konsequent. Wir stehen mit Entwicklung, Support und Hosting in Deutschland für Transparenz, technische Qualität und digitale Souveränität. Unsere Kunden erhalten leistungsfähige Produkte und behalten die Hoheit über sensible Daten ohne versteckte Abhängigkeiten oder undurchsichtige Zugriffsrechte. NCP ist vom BSI als „Qualifizierter Hersteller“ zertifiziert und stellt hochsichere VPN-Lösungen zur Verfügung, die für die Geheimhaltungsstufen VS-NfD, NATO RESTRICTED und EU RESTRICTED eingesetzt werden dürfen. Zertifizierungen nach BSI-Vorgaben schaffen zusätzliche Verlässlichkeit und Vertrauen. ■

Weitere Informationen zu den Neuheiten von NCP erfahren Sie auf der it-sa 2025 an unserem Stand 7A-516!

Cyber Resilience Act der EU – was Sie wissen müssen

Der EU-Rat hat den Cyber Resilience Act verabschiedet. Die wichtigsten Informationen und Antworten zum neuen Beschluss, der die Cybersicherheit von Hard- und Software in der EU sicherstellen soll, lesen Sie hier.

Von Melanie Staudacher, Security-Insider

Am 10. Oktober 2024 hat der Rat der EU-Innenministerinnen und Innenminister in Brüssel den Cyber Resilience Act (CRA) verabschiedet. Der CRA ist die erste europäische Verordnung, die eine verbindliche Mindestanforderung an die Cybersicherheit für vernetzte Produkte vorgibt. Betroffen sind Anwendungen und Produkte, die auf dem EU-Markt erhältlich sind. Das Ziel des CRA ist es, die Cybersicherheit in der Europäischen Union zu erhöhen.

Bild: Maxim – stock.adobe.com / KI-generiert

Bundesinnenministerin Nancy Faeser (SPD) sagte: „Vernetzte Produkte erleichtern unseren Alltag, können aber auch von Kriminellen ausgenutzt werden. Deshalb müssen sie sicher sein.“ Man müsse sich darauf verlassen können, dass ein vernetztes Gerät, das man bei sich trägt oder zu Hause hat, kein Sicherheitsrisiko ist.

Wann tritt der Cyber Resilience Act in Kraft?

Mit der Verabschiedung des EU-Rates am 10. Oktober 2024 tritt der CRA ab sofort in Kraft. Ab November 2027 müssen Unternehmen Produkte, die digitale Elemente enthalten, an die Cybersicherheitsanforderungen anpassen. Ansonsten dürfen sie sie nicht in der EU verkaufen. Andere Verpflich-

tungen des CRA, wie die Meldepflicht der Hersteller bei Kenntnis von ausgenutzten Sicherheitslücken, gelten bereits ab August 2026.

Welche Produkte fallen unter den CRA?

Zu den Produkten, die künftig die Anforderungen des CRA erfüllen müssen, gehören alle vernetzten Geräte. Dazu gehören

- industrielle Hardware und Software wie IoT-Geräte, PLCs und Sensoren,
- Software-Produkte wie Desktop-, Web- und mobile Applikationen sowie Betriebssysteme und
- Software- und Hardware-Produkte für die private Nutzung wie Smart-Home-Geräte und mobile Endgeräte.

Welche Pflichten ergeben sich aus dem CRA?

Der Cyber Resilience Act nimmt alle beteiligten Wirtschaftsakteure in die Pflicht: Hersteller, Importbetriebe und Handel. Sie müssen künftig sicherstellen, dass die von ihnen vertriebenen Produkte den Cybersicherheitsanforderungen genügen und entsprechend ausgewiesen sind. Darüber hinaus werden mit dem CRA den Beteiligten weitreichende Informations-, Transparenz- und Aufklärungspflichten auferlegt. Hersteller müssen außerdem die Agentur der Europäischen Union für Cybersicherheit (ENISA) innerhalb von 24 Stunden über IT-Schwachstellen und Cybervorfälle informieren. Innerhalb von 72 Stunden müssen weitere Details zur Art der Sicherheitslücke und mögliche Gegenmaßnahmen folgen. Natürlich müssen die Anbieter auch regelmäßig Sicherheitsupdates veröffentlichen.

Was passiert bei Nichteinhaltung des CRA?

Wer sich nicht an die Anforderungen des CRA hält, muss mit Sanktionen rechnen. Je nach EU-Mitgliedstaat und Schwere des Verstoßes können diese variieren. Grundsätzlich kann eine Nichteinhaltung zu hohen Geldstrafen führen: Bis zu 15 Millionen Euro oder bis zu 2,5 Prozent des gesamten jährlichen Umsatzes, je nachdem, welcher Betrag höher ist. Weitere Konsequenzen können sein:

- Aussetzung der Marktzulassung: Produkte, die nicht den Anforderungen des Cyber Resilience Act entsprechen, müssen eine Einschränkung ihrer Marktzulassung befürchten.
- Rückruf von Produkten: Bei schwerwiegenden Sicherheitsmängeln könnten einzelne Produkte zurückgerufen werden.
- Schadensersatz: Unternehmen können zur Zahlung von Schadensersatz an Verbraucher oder andere Unternehmen verpflichtet werden, wenn durch das Nichteinhalten des Cyber Resilience Act ein Schaden entstanden ist.
- Strafverfahren: In schweren Fällen können Strafverfahren gegen die Verantwortlichen eingeleitet werden.
- Reputationsschäden: Verstöße gegen den Cyber Resilience Act können zu erheblichen Reputationsschäden führen. Diese können sich negativ auf Kundenbeziehungen auswirken.

Erkennung mit CE-Kennzeichen

Ausgewiesen werden die Produkte mit dem bereits vertrauten CE-Kennzeichen. Verbraucher können daran künftig erkennen, dass ein vernetztes Gerät die Anforderungen des CRA erfüllt.

Dem Bundesministerium des Inneren und für Heimat zufolge ist die deutsche Wirtschaft gut auf die neuen Regelungen vorbereitet. Die Hersteller können sich mit dem IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) schon jetzt die Einhaltung der Cybersicherheitsanforderungen freiwillig auszeichnen lassen. □

Souveräne Cybersicherheit mit G DATA Managed Extended Detection and Response

Cyberangriffe nehmen rasant zu und damit auch die Herausforderungen für Unternehmen. Viele IT-Verantwortliche sind mit der effektiven Absicherung der IT-Systeme überfordert. Es mangelt an Zeit, Personal und tiefgreifendem Fachwissen. IT-Sicherheit ist unter diesen Bedingungen kaum leistbar. Die Lösung für das Problem ist G DATA 365 | MXDR (Managed Extended Detection and Response).

Überwachung rund um die Uhr durch G DATA

Cyberattacken sind heute oft individualisiert und dateilos. Angreifer nutzen ungeschlossene Sicherheitslücken in Anwendungen oder Betriebssystemen aus oder sie setzen auf Phishing, um an Zugangsdaten zu kommen. Als Resultat sind Unternehmen über lange Zeit arbeitsunfähig. Ein hundertprozentiger proaktiver Schutz vor Attacken ist kaum möglich. Es kommt daher darauf an, die Vorgänge im Netzwerk zu überwachen, schädliche Aktivitäten aufzuspüren und sofort richtig darauf zu reagieren. Genau dies leistet die deutsche Security-Operation-Center-Lösung (kurz SOC): G DATA 365 | MXDR.

24/7-Rundumschutz

Ein erfahrenes Analystenteam überwacht bei G DATA 365 | MXDR das Netzwerk rund um die Uhr. Die Managed-SOC-Expertinnen und -Experten haben alle Vorgänge im Blick und betreiben Threat Hunting: Sie analysieren verdächtige Aktivitäten und Unregelmäßigkeiten, um schädliche Vorgänge aufzudecken. Für die Analyse von Aktionen steht den Fachleuten eine moderne Sensorik zur Verfügung. Handelt es sich um einen Angriff, erfolgt eine umgehende Reaktion, um diesen zu beenden – zu jeder Tages- und Nachtzeit. Hierdurch wird eine Attacke in der Anfangsphase gestoppt, bevor der Schaden groß ist. IT-Verantwortliche werden über Vorfälle informiert und finden in der Webkonsole zusätzlich alle relevanten Informationen. Sie können auch nachvollziehen, welche Maßnahmen ergriffen wurden. Zusätzlich führt das Analystenteam Root-Cause-Analysen (RCA) durch, um die Ursachen von Sicherheitsvorfällen zu identifizieren und daraus fundierte und für Kundinnen und Kunden verständliche Handlungsempfehlungen in deutscher Sprache abzuleiten.

G DATA CyberDefense

TRUST IN GERMAN SICHERHEIT

Starke technologische Basis

G DATA 365 | MXDR basiert auf selbst entwickelten Security-Komponenten. Diese werden kontinuierlich weiterentwickelt, um sicherzustellen, dass sie immer auf dem neuesten Stand der IT-Sicherheit sind.
Unternehmen und Partnern stehen persönliche Ansprechpartner zur Seite, unterstützt von einem preisgekrönten deutschsprachigen 24/7-Support. G DATA setzt bei seiner Managed-SOC-Lösung auf eine direkte persönliche Betreuung. Beim Onboarding berät das Cyber-Defense-Unternehmen individuell und thematisiert dabei aktiv das Thema Datenschutz. Dabei wird unter anderem festgelegt, auf welchen Endpoints welche spezifische Response stattfinden soll. Das Onboarding erfolgt wahlweise durch G DATA oder gemeinsam mit einem IT-Security-Dienstleister.

Deutscher Cyber-Defense-Partner

Die Bedeutung der digitalen Souveränität in Europa nimmt stetig zu. Unternehmen können sich heute nicht mehr voll auf außereuropäische Anbieter verlassen. Daher sind die Themen Vertrauen und Souveränität bei der Wahl des passenden Managed-SOC-Anbieters sehr wichtig. G DATA CyberDefense ist in Deutschland ansässig und unterliegt damit den strengen deutschen Datenschutzrichtlinien. Zudem bietet der Spezialist als einziger auf dem Markt einen SOC-Service an, der vollständig aus Deutschland ist. Am deutschen Unternehmenssitz sind das Analystenteam, der Support und die Entwicklung angesiedelt. Darüber hinaus befinden sich auch die Server in Deutschland. Dieses deutsche Komplettpaket bietet nur G DATA an. Der Cyber-Defense-Spezialist steht für qualitativ hochwertigen Schutz vor Cyberbedrohungen „Made in Germany“. ■

Auf der it-sa 2025 ist G DATA CyberDefense in Halle 7a, Stand 314 zu finden. Neben der Standpräsenz erwartet das Fachpublikum ein umfangreiches Programm: Am 7. Oktober 2025 findet um 14:30 Uhr ein Workshop statt zum Thema digitale Souveränität mit dem IT-Sicherheitsrechtsexperten Prof. Dr. Dennis-Kenji Kipker. Mehr Informationen und Anmeldung unter: www.gdata.de/it-sa


Bild: G DATA CyberDefense AG

Vision der Cyber-Nation Deutschland

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) hat sein im Februar 2025 veröffentlichtes Positionspapier „Cyber-Nation“ überarbeitet und erneuert. Neu sind konkrete Forderungen, etwa zu Backdoor-Verboten, europäischer Cloud-Souveränität und staatlicher Beschaffung von IT-Services und -Produkten.

Von Jürgen Paukner, Security-Insider

Bild: png-jpeg-vector – stock.adobe.com / KI-generiert

Das TeleTrusT-Positionspapier „Cyber-Nation“ formuliert zentrale Ziele und konkrete Maßnahmen, um Deutschland zur Cyber-Nation zu entwickeln. Die zweite Version des Papiers enthält mehrere neue Elemente. Diese berücksichtigen insbesondere geopolitische Entwicklungen, regulatorische Rahmenbedingungen und neue strategische Impulse. Dabei wird die Rolle der Politik als Impulsgeber und langfristiger Unterstützer benannt. Version zwei des Positionspapiers formuliert explizit, dass eine erfolgreiche Umsetzung der Cyber-Nation-Strategie nur im Zusammenspiel von Politik, Wirtschaft, Forschung, Behörden und Zivilgesellschaft möglich ist.

Berücksichtigung geopolitischer Entwicklungen

Die neue Version bezieht sich vor allem auf aktuelle internationale Entwicklungen. Dazu zählen die US-amerikanische Digital- und KI-Strategie wie das Stargate-Projekt. TeleTrusT fordert einen europäischen Gegenentwurf, insbesondere im Hinblick auf technologische Souveränität und Rechenzentrumsinfrastruktur.

Außerdem nimmt die neue Fassung Bezug auf eine im Frühjahr 2025 veröffentlichte Meldung des Bundesamts für Sicherheit in der Informationstechnik (BSI). Darin nimmt das Amt Stellung zur technologischen Souveränität im Kontext „Cyber Dominance“. Damit wird die Verzahnung staatlicher und zivilgesellschaftlicher Strategien zur digitalen Selbstbestimmung betont. In diesem Zuge erkennt TeleTrusT Kunst, Kultur, Medien, Militär und Zivilgesellschaft als integrale Teile einer sicheren digitalen Ordnung an. Das erweitert das ursprüngliche Zielbild. Dieses fokussierte sich zuvor stärker auf klassische IT- und Wirtschaftsakteure.

Konkrete Maßnahmen

Die neue Fassung des Positionspapieres enthält zusätzlich konkrete Forderungen, darunter:

- Verbot von Backdoors oder geschwächter Verschlüsselung,
- mehr Zentralisierung statt Fragmentierung in der Governance,
- klare politische Bekenntnisse zu kompromissloser IT-Sicherheit,
- Aufbau von Sicherheitsinfrastrukturen auf Basis gemeinsamer europäischer Werte.

Diese Forderungen sollen die digitale Souveränität und Resilienz Deutschlands nachhaltig absichern und stärken. Nicht nur auf strategischer Ebene, sondern auch durch praxisnahe, umsetzbare und verbindliche Maßnahmen. □

SEPPmail.cloud – höchste Sicherheit, ganzheitliche Datenhoheit

Vertrauliche Angebote, Vertragsunterlagen oder persönliche Daten werden täglich per E-Mail versendet – oft, ohne dass klar ist, wo die Daten tatsächlich gespeichert werden. Für Unternehmen bedeutet das ein unnötiges Risiko: Wer nicht genau weiß, in welchem Land seine E-Mails liegen, gibt die Kontrolle über sensible Informationen aus der Hand. SEPPmail.cloud bietet hier eine klare Antwort: eine souveräne Cloud-Lösung, 100 % in Deutschland gehostet, unter europäischem Recht und vollständig DSGVO-konform.

Minimaler Aufwand – maximale Sicherheit

SEPPmail.cloud kombiniert E-Mail-Verschlüsselung, digitale Signaturen, sicheren Großdatei-Transfer, die Übertragung von übergroßen Files und zentrales Disclaimer-Management in einer einzigen Plattform. Der Betrieb erfolgt komplett in der Cloud – ohne zusätzliche Hardware oder komplexe Installationen vor Ort. Unternehmen profitieren so von einer schnellen Einführung und minimalem Administrationsaufwand.

Umfassender Schutz durch intelligente Filtertechnologie

Ein integrierter Cloud-Filter sorgt mit einer überdurchschnittlich hohen Erkennungsrate für effektiven Schutz vor Phishing, Malware, Spam und gezielten Angriffen wie Spear-Phishing oder CEO-Fraud. Sicherheitsrichtlinien lassen sich individuell anpassen und zentral über ein intuitives Dashboard verwalten – effizient, transparent und jederzeit erweiterbar.

Flexibilität, Kostentransparenz und Souveränität

Das Pay-per-Use-Modell macht SEPPmail.cloud besonders wirtschaftlich. Unternehmen zahlen nur für tatsächlich genutzte Leistungen und können die Lösung nahtlos in Microsoft 365, Hybrid- oder On-Prem-Umgebungen integrieren. Die souveräne Cloud-Architektur stellt sicher, dass alle Daten ausschließlich in sicheren europäischen Rechtsräumen bleiben. Zusätzlich wird jede E-Mail mit einem SwissSign-Zertifikat signiert. SEPPmail.cloud vereint höchste Sicherheit, souveräne Datenhaltung und volle Kontrolle – ein starkes Paket für Unternehmen, die Wert auf Datenschutz und Verlässlichkeit legen. ■


SEPPMAIL.cloud
Gemeinsam auf Wolke E-Mail-Sicherheit
höchste Sicherheit
ganzheitliche Datenhoheit
intelligente Filtertechnologie
100 % in Deutschland betrieben
seppmail.com/de

Warum Kollaborations-Software „Made in Germany“ sein sollte

Steigende Anforderungen an den Datenschutz und die wachsende Bedeutung von Datensouveränität machen Kollaborations-Software „Made in Germany“ immer wichtiger. Das übergeordnete Ziel für Unternehmen muss dabei sein, die vollständige Kontrolle über ihre Daten zu behalten – vom Speicherort über die Verarbeitung bis zu den Zugriffsrechten.

Von Volkan Gümüs, Materna Virtual Solution

Bild: MH – stock.adobe.com / KI-generiert

Die Probleme beginnen bereits bei der Definition. Denn obwohl in der öffentlichen Debatte um den Datenschutz immer wieder Forderungen nach souveränen Lösungen zur Verarbeitung und Speicherung von Daten zu vernehmen sind, verschwimmen dabei schnell die Begrifflichkeiten. Was versteckt sich also in Wirklichkeit hinter der oft zitierten Datensouveränität? Grundlegend bezeichnet das Konzept die Fähigkeit und das Recht eines Unternehmens, einer Behörde oder einer Organisation, die vollständige Kontrolle über alle eigenen Daten zu behalten.

Souveränität und Verantwortung

Was auf den ersten Blick so klar wie leicht verständlich klingt, zieht auf den zweiten allerdings sehr viel weitere Kreise. Souveränität bedeutet in diesem Kontext nämlich auch jede Menge Verantwortung – für physische Speicherung, Verwaltung, Zugriffsrechte, Sicherheit und eine Nutzung der Daten im Einklang mit den immer höheren Anforderungen von gesetzlichen Vorgaben und Compliance-Richtlinien.

Grundsätzliches Umdenken ist gefordert

Wer Datensouveränität fordert, fordert damit in einer immer stärker Cloud-betriebenen digitalen Welt ein grundsätzliches Umdenken in Bezug auf die Art und Weise, wie wir mit Daten umgehen. Es ist nicht egal, bei welchem Anbieter, auf welcher Cloud und in welchem Land sie liegen. Ziel muss es daher sein, dass alle Organisationen zu jeder Zeit wissen und sicherstellen können, wo sich ihre Daten befinden, wer darauf zugreifen kann, für welchen Einsatz sie geeignet sind und welche rechtlichen sowie ethischen Vorgaben für sie im Einzelnen gelten.

Diese Forderungen sind wichtig und richtig. Sie stellen Unternehmen allerdings vor neue Herausforderungen bei der Suche nach dafür geeigneter Software und Anbietern – allen voran im Bereich der vulnerablen Kollaborationslösungen. Bei dieser zentralen Schnittstelle der internen und externen Kommunikation darf es in Zeiten von New-Work-Modellen keine Kompromisse geben. Das betrifft sowohl den oft als passiv eingestuften Datenschutz, der darauf ausgerichtet ist, bestehende Daten vor Missbrauch und unbefugtem Zugriff zu sichern, als auch die aktiven Ansätze einer ⇨

↳ Datensouveränität. Warum aktiv? Weil Unternehmen, Behörden und Organisationen damit nicht nur den Schutz, sondern die gesamte Kontrolle über die vollständige Lebensspanne der Daten verfolgen. Auf technologischer Seite muss die eingesetzte Softwarelösung für eine wirkliche souveräne Datenstrategie daher zahlreiche Anforderungen erfüllen.

Warum in die Ferne schweifen

Unternehmen wissen um die strikten Vorgaben der EU und insbesondere auch um die Restriktionen des deutschen Datenschutzgesetzes. Um die hohen Strafzahlungen und negativen Berichterstattungen zu vermeiden, ist eine DSGVO-konforme Software daher bereits als Standard anzusehen. Eine gefährliche Grauzone besteht allerdings weiter bei der großen Anzahl bekannter Anbieter aus den USA, die bei vielen Unternehmen weiterhin hoch im Kurs stehen.

Angespannte diplomatische Beziehungen

Besonders mit Blick auf die aktuelle politische Lage und die angespannten diplomatischen Beziehungen zwischen der EU und den Vereinigten Staaten ist die Zukunft für eine rechtskonforme und sichere Nutzung von US-Clouds und -Anbietern ohne separate Rechenzentren in Europa mehr als fraglich. Gut möglich, dass das bereits jetzt fragile Datenschutzabkommen für deutsche Unternehmen bald schon zu einem wirklichen Problem wird. Vor diesem Hintergrund gewinnen deutsche Anbieter mit lokaler Infrastruktur als Alternative an Bedeutung – da sie garantieren können, dass Daten innerhalb des nationalen beziehungsweise europäischen Rechtsrahmens gespeichert bleiben. Auch die transparente Verarbeitung von personenbezogenen Daten – ein wesentlicher Bestandteil der DSGVO – kann bei deutschen Anbietern vorausgesetzt werden und trägt ebenfalls zur Stärkung der Datenhoheit bei.

Souverän und containerisiert

Weil Software allerdings nicht gleich Software ist, lohnt ein genauerer Blick auf die Besonderheiten und Ansprüche, die Unternehmen stellen müssen. Ein immer wichtigerer Aspekt dabei: Wie sichert eine in Frage kommende Lösung Unternehmensdaten ab, wenn verteilt und mobil arbeitende Teams zu jeder Zeit und von jedem Ort aus auf Informationen zugreifen müssen? Erschwerend kommt hinzu, dass immer mehr Mitarbeiter ihre mobilen Endgeräte bequemerweise sowohl für dienstliche als auch private Zwecke einsetzen wollen – egal, ob im Rahmen eines BYOD- oder COPE-Modells.
Der Markt hat auf diese technologischen Herausforderungen bereits reagiert. Dabei haben sich insbesondere Container-Lösungen für mobile Geräte als unkomplizierter und sicherer Weg erwiesen. Sie erzeugen einen von den privaten Daten abgeschirmten Bereich, der den Zugriff auf Unternehmensdaten an eine PIN, Smartcard oder biometrische Verifizierung der User koppelt. Gleichzeitig verhindert die stringente Trennung auf technologischer Ebene den ungewollten Abfluss der Unternehmensdaten und deren Vermischen mit privaten Daten. Innerhalb des Containers können Nutzer auf sichere Office-Anwendungen, Tools zur Dokumentenverarbeitung sowie auf E-Mails, Kalender und Kontakte zugreifen. Auch gehärtete Browser mit einer Ende-zu-Ende-Verschlüsselung und vielfältigen Sicherheitskonfigurationen sind bereits erhältlich.

Auch ans Backend denken

Damit bieten Container-Lösungen einerseits eine komfortable Nutzererfahrung, die das Schutzniveau der Daten drastisch erhöht. Für eine souveräne Lösung ist allerdings auch das Gegenstück, also das Backend, die Infrastruktur und das Handeln der Anbieter notwendig. Ein guter Gradmesser dafür sind die Einschätzungen von offiziellen Stellen wie dem BSI, die

Lösungen auf Herz und Nieren testen. Entscheidend sind entsprechende Freigaben oder Einsatzempfehlungen für die Software in erster Linie in Behörden, für Unternehmen dienen sie allerdings ebenfalls als verlässliche Orientierung nach langfristig sicheren Kollaborationslösungen.

Zusätzliche Aspekte

Auf Administrationsebene sind bei der Auswahl aber noch mehr Aspekte entscheidend: Ist eine einfache, zentrale Verwaltung über ein intuitives MDM gegeben? Können IT-Admins verschiedene Berechtigungsstufen konfigurieren, Nutzergruppen definieren und persönlich ansprechen? Auch technologische Funktionen aus dem Bereich der Data Loss Prevention sollten vorhanden sein, etwa das Löschen von Daten aus der Ferne, sollte ein Endgerät verloren gehen oder gestohlen werden – zusätzlich zu den durchgehend verschlüsselten Geräten und Daten.

Langfristige Sicherheit und Souveränität

Datensouveränität ist die Summe vieler Entscheidungen. Sie beginnt bei der Auswahl technologischer Lösungen und Speicherorte, umfasst die Definition klarer Sicherheitsrichtlinien und erfordert eine kontinuierliche Anpassung an rechtliche und technologische Entwicklungen. Unternehmen, die ihre Datensouveränität aktiv gestalten, schaffen nicht nur Vertrauen bei Kunden und Partnern, sondern sichern sich langfristig einen strategischen Wettbewerbsvorteil. Gleichzeitig stärken sie ihre Resilienz gegenüber äußeren Einflüssen, indem sie Abhängigkeiten von unsicheren oder instabilen Drittstaaten reduzieren und sich gegen geopolitische oder wirtschaftliche Risiken wappnen.

Das Fundament dafür sind Lösungen „Made in Germany“ mit vertrauenswürdigen, geprüften Anbietern und Rechenzentren innerhalb der EU oder Deutschland, die allesamt den strengen Anforderungen der DSGVO unterliegen. Auch mit Blick auf die zukünftige Entwicklung von Datenschutzgesetzen ist nicht auszuschließen, dass das Hosten von Unternehmensdaten in Nicht-EU-Ländern langfristig als nicht legitim angesehen wird. Umso wichtiger ist der wachsende Markt für deutsche Software und lokale, sichere Infrastrukturen. □

Bild: Materna Virtual Solution

Über den Autor

Volkan Gümüs ist Geschäftsführer von Materna Virtual Solution. Er ist sich sicher, dass Datensouveränität keine Kompromisse und Grauzonen zulässt. „Auf der sicheren Seite sind Unternehmen daher nur mit Lösungen Made in Germany“, sagt Gümüs.

infodas
connect more. be secure.

Ganzheitliche Cybersecurity, vertrauensvolle Beratung & zugelassene Lösungen.

Für BOS, KRITIS & den öffentlichen Sektor!

SDoT Cross Domain Solutions

Sicherer Datenaustausch in sensitiven Netzwerken
Eingesetzt von NATO & ihren Mitgliedsstaaten
Militärisch & geheimdienstlich zugelassen

SDoT Secure Network Card

Digitale Souveränität Made in Germany
Einzigartige BSI-Zulassung
Manipulationssicher

Cybersecurity Consulting

Vertrauensvoller Partner des BSI
BSI IT-Grundschutz-Audits
VS-Zulassungsberatung
Security Testing

Applied Technology

Systemhärtung für sicherheitskritische Bereiche
Potenzialanalyse von AI-Anwendungsfällen
Datengetriebene Datenschutzberatung

GEHEIM

EU SECRET

NATO SECRET

Besuchen Sie uns auf der it-sa Expo&Congress in Halle 8-215!

infodas Cybersecurity.

Militärisch bewährt.

Spezialisiert auf hochregulierte & sensitive Bereiche!

Let´s get in touch!

info@infodas.de | +49 221 70912-0 | www.infodas.com

Keine Macht den US-Servern

Mehr Sicherheit, weniger Abhängigkeit: In Zeiten wachsender digitaler Risiken setzen Unternehmen wieder stärker auf europäische IT-Lösungen. Securepoint adressiert gezielt das Gesundheitswesen sowie KMU mit Lösungen, die auf digitale Souveränität ausgerichtet sind.

Von Natalie Forell, IT-BUSINESS

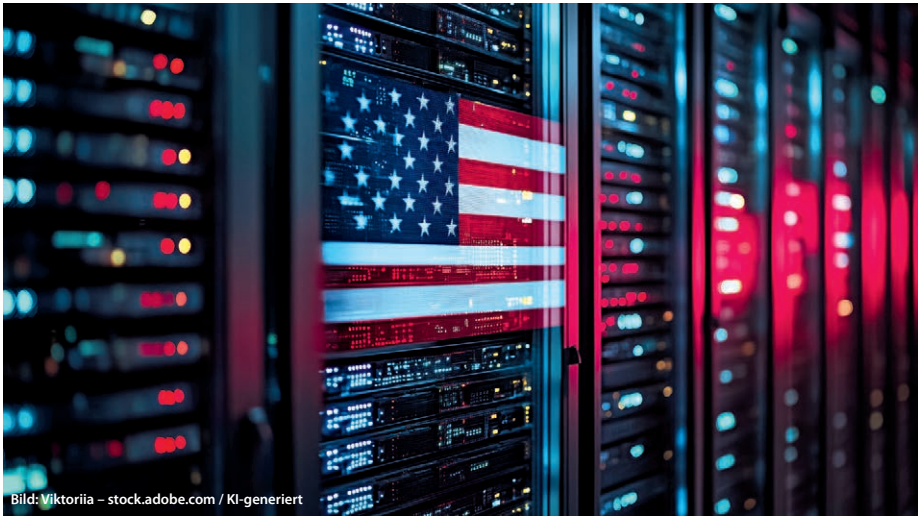


Bild: Viktoriia – stock.adobe.com / KI-generiert

Als die US-Regierung kurzfristig den Zugang zur öffentlichen CVE-Datenbank einschränkte, wurde einmal mehr deutlich: Wer auf amerikanische Infrastruktur baut, macht sich politisch abhängig. Für Securepoint ist die Lehre aus solchen Vorfällen eindeutig: Digitale Souveränität sollte oberste Priorität haben. Das Unternehmen aus Lüneburg setzt daher seit Jahren auf Partnerschaften mit deutschen und österreichischen Unternehmen. Auch intern nutzt man bevorzugt eigene Lösungen für beispielsweise Videokonferenzen oder Messaging – um systematische Abhängigkeiten zu vermeiden. Doch so ganz lässt sich das nicht verhindern. Völlige Unabhängigkeit sei derzeit kaum erreichbar, räumt Eric Kaiser, Produktmanager bei Securepoint, ein: „Deutschland hat sich lange zurückgelehnt und zu wenig investiert." Der europäische Markt sei dadurch in den Hintergrund geraten – vor allem gegenüber den großen US-Anbietern.

Mit 27 Vertriebsgebieten im DACH-Raum setzt Securepoint auf einen flächendeckenden Channel-Vertrieb, der vor allem kleinere Unter-

nehmen wie Arztpraxen oder Rechtsanwälte adressiert. Vor dem Hintergrund zunehmender geopolitischer Spannungen wächst das Interesse an europäischen Security-Lösungen spürbar. Endkunden beschäftigen sich zunehmend mit digitalen Abhängigkeiten und suchen nach Möglichkeiten, digitale Souveränität zu stärken. Gleichzeitig zeigt sich aber, dass IT-Sicherheit in vielen KMU noch nicht die oberste Priorität hat: Das Budget und die personellen Ressourcen sind stark begrenzt und Investitionen in die IT-Sicherheit müssen erst abgewogen werden.

Bewegung im Gesundheitswesen

Ein wichtiger Bereich für Securepoint ist das Gesundheitswesen. Die Sicherheitsrichtlinien der Kassenärztlichen Bundesvereinigung (KBV) wurden zuletzt verschärft – ab Oktober gelten diesbezüglich strengere Vorgaben. Selbst kleine Arztpraxen müssen künftig unter anderem Firewalls, Antivirenschutz und regelmäßige Backups nachweisen. Außerdem werden Awareness-Schulungen Pflicht. „Bei Arztpraxen war es immer schwer, IT-Security durchzusetzen – da kommt jetzt endlich Bewegung rein", sagt Kaiser. Der Sicherheitshersteller kooperiert in diesem Bereich mit Anbietern von Praxisverwaltungssystemen (PVS), in welche die IT-Security direkt integriert wird. Eric Kaiser erklärt: „Zuerst kam die Pflicht für die Ärzte, dann kamen Apotheken. Inzwischen müssen aber auch alle anderen Heilberufe wie Hebammen, Physiotherapeuten oder Ergotherapeuten an die Telematikinfrastruktur (TI) angeschlossen werden", erklärt Kaiser. „Dort laufen künftig alle Prozesse zusammen: Abrechnung, E-Rezept, elektronische Patientenakte. Und je mehr Berufsgruppen daran teilnehmen, desto größer wird natürlich auch der Markt."

Firewalls der Zukunft

Und auch auf technischer Ebene verändert sich der Markt: Cloud-basierte Security-Lösungen ersetzen zunehmend klassische Modelle. „Noch ist davon wenig zu spüren", sagt Kaiser, „aber wir bereiten uns vor". Ein Schritt in diese Richtung ist „Cloudshield" – Securepoint bietet damit die ersten Dienste für DNS-Sicherheit aus der Cloud an. IT-Sicherheitslösungen müssen flexibler sein, da Unternehmensdienste „wandern". Unternehmensdienste werden nicht mehr nur lokal betrieben, sondern über zentrale IT-Abteilungen oder neue Cloud-Services. Solche Dynamiken müssen sich bei Unternehmen dann natürlich auch in der Infrastruktur widerspiegeln – die Systeme müssen intelligent werden. „Das sind dann schon Firewalls", betont Kaiser. Die Technik würde dann nur anders genannt werden. Noch ist das Zukunftsmusik, aber mit ersten Lösungen bereitet sich Securepoint bereits darauf vor. Und dabei gilt: Abwägen, was sicher und sinnvoll ist. Denn: Nicht alles, was technisch umsetzbar ist, ist gleichzeitig auch sicher. □

„Deutschland hat sich lange zurückgelehnt und zu wenig investiert." Eric Kaiser, Produktmanager bei Securepoint

Advertorial TDT

Advertorial TDT

Warum ein Managed SOC die IT besser schützt als Virenschutz allein

Cyberkriminelle setzen auf komplexe und gezielte Angriffsvektoren, um Unternehmen zu attackieren – und klassischer Virenschutz stößt an seine Grenzen. IT-Verantwortliche müssen darauf mit modernen Security-Konzepten reagieren, die eine frühzeitige Reaktion auf Vorfälle ermöglichen und so für einen effektiven Schutz der IT-Infrastruktur sorgen. Ein Managed Security Operations Center (kurz Managed SOC) ermöglicht dies und sorgt trotz der Kosten für die Anschaffung und den Betrieb für einen schnellen Return of Invest.

Von Kathrin Beckert-Plewka, G DATA CyberDefense

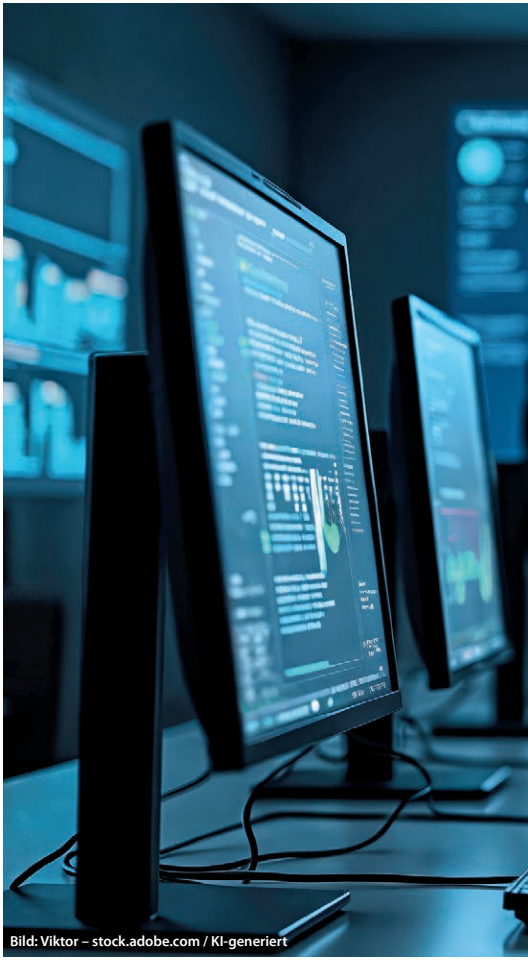


Bild: Viktor – stock.adobe.com / KI-generiert

Er war der Standard der IT-Sicherheit in Unternehmen: Über Jahre setzten IT-Verantwortliche auf klassischen Virenschutz und sorgten damit für sichere IT-Systeme. Auch heute ist er eine bewährte Sicherheitslösung, die mittlerweile aber an ihre Grenzen stößt.

Der Grund: Die Angriffsmuster haben sich im Laufe der Zeit verändert. In der Vergangenheit

setzten die Kriminellen bei Angriffen insbesondere auf Schadprogramme. Der eingesetzte Virenschutz erkannte und blockte den Schadcode durch seine umfangreichen Technologien zuverlässig.

Die Zeiten ändern sich

Heute ist die Strategie der Kriminellen eine andere: Bei vielen Angriffen kommt beim initialen Zugang zum Unternehmensnetzwerk kein Schadprogramm zum Einsatz, stattdessen laufen die Aktionen dateilos ab. Die Tätergruppen setzen zum Beispiel auf ungeschlossene Schwachstellen in Betriebssystemen oder Anwendungen, die im Unternehmen zum Einsatz kommen. Entweder stehen bisher keine Patches zum Schließen der Lücken zur Verfügung oder sie wurden noch nicht eingespielt – aufgrund ↪

- von Nachlässigkeit oder Zeit- beziehungsweise Personalmangel.

Weitere Angriffsvektoren sind Windows-Funktionen, oder die Kriminellen setzen auf individualisierte Attacken. Bei der zweiten Variante kommt Social Engineering zum Einsatz, beispielsweise in Form von speziellen Phishing-Mails. Die Angreifergruppen können über diese Methode an Zugangsdaten gelangen und dringen mit deren Hilfe in die IT-Systeme eines Unternehmens ein, spionieren dieses aus und vollziehen weitere Schritte der Angriffskette.

Eine klassische Virenschutzlösung ist nicht in der Lage, derartige Attacken aufzudecken. Hierzu müssen die IT-Infrastruktur permanent überwacht und die Logs aus den Analysesystemen ausgelesen und ausgewertet werden, um schädliche Aktionen zu erkennen.

Cyberangriffe sofort stoppen

Ein Managed SOC ermöglicht eine permanente Überwachung. Hier werden Logs zentral gesammelt und analysiert, sodass schädliche Aktionen aufgedeckt und gestoppt werden – und damit dateilose Angriffe beendet werden, bevor der Schaden groß ist. Die Abkürzung SOC steht dabei für Security Operations Center.

Im Regelfall ist eine gemanagte SOC-Lösung mit breit aufgestellten Sensorik-Systemen ausgerüstet, um alle bedenklichen und kriminellen Aktionen in den IT-Systemen eines Unternehmens aufzuspüren. Für diese Aufgabe kommt ein erfahrenes Analystenteam zum Einsatz, welches die IT-Infrastruktur rund um die Uhr überwacht und Vorgänge überprüft.

Verschafft sich jemand zum Beispiel plötzlich weitreichende Administrationsrechte, wird verifiziert, ob diese Handlung legitim war und ob ein Eingreifen nötig ist. So lässt sich verifizieren, ob die Aktion ein Teil einer Cyberattacke ist. Bestätigt sich ein Angriff, reagiert das Analystenteam umgehend und leitet Gegenmaßnahmen ein.

Der Vorteil liegt auf der Hand: Durch Managed SOC lassen sich Cyberattacken beenden, die sich im Anfangsstadium befinden und noch keinen oder nur einen geringen Schaden angerichtet haben.

Hier zeigt sich ein weiterer großer Vorteil von Managed SOC gegenüber einer Virenschutzlösung: Die Überwachung der IT-Systeme durch ein Analystenteam und die damit verbundene Response-Möglichkeit auf schadhafte Vorgänge im Netzwerk. Eine einfache Sicherheitslösung verfügt nicht über diesen Leistungsumfang.

24/7-Security

Cyberkriminelle greifen nicht nur zwischen 9 und 17 Uhr an, sondern auch nachts und an Wochenenden. IT-Sicherheit ist daher eine Rund-um-die-Uhr-Aufgabe und ein Managed-SOC-Analystenteam ist in einem 24/7-Schichtsystem aktiv. Nur so ist sichergestellt, dass eine passende Reaktion auf einen Vorfall umgehend erfolgt. IT-Teams in Unternehmen können diese Aufgabe oft nicht leisten, da sie viel Personal, Aufwand und auch spezielles Fachwissen erfordert. Durch das Tagesgeschäft sind die Mitarbeitenden bereits voll ausgelastet, sodass nur sehr wenig Zeit für IT-Sicherheit bleibt.

Im Bereich Security ist aber gerade auch der Fachkräftemangel ein riesiges Problem. In Deutschland fehlten 2023 fast 105.000 IT-Fachkräfte (Quelle: Cybersicherheit in Zahlen von G DATA CyberDefense, Statista und brand eins). Bis heute hat sich die Lage nicht verbessert.

Externes Fachwissen gegen die aktuellen Cybercrime-Trends

Innerhalb der IT ist Security ein eigenständiges Fachgebiet. IT-Mitarbeitende in Unternehmen können IT-Systeme aufbauen und andere Aufgaben übernehmen, sie haben aber kein ausreichendes IT-Sicherheits-Fachwissen. Für IT-Verantwortliche ist es daher sinnvoll, auf

externe Expertise zu setzen und damit auf eine gemanagte SOC-Lösung. Das Analystenteam ist fachlich immer auf dem neuesten Stand in Hinblick auf neue Angriffsvektoren und Cybercrime-Trends.
Von dem Wissen und der Erfahrung profitieren Unternehmen, gerade wenn es um Handlungsempfehlungen abseits der reinen Überwachung geht. Diese häufige Komponente eines Managed SOC sorgt für weitere IT-Sicherheit.

Cyberkriminelle sind nicht wählerisch

Prinzipiell ist jede Firma ein interessantes Angriffsziel für Cyberkriminelle. Tritt der Schadensfall ein, kann die wirtschaftliche Existenz eines Unternehmens schnell am seidenen Faden hängen – je nach Ausmaß des Angriffs. Daher ist ein Managed SOC grundsätzlich für alle Firmen mit umfangreichen IT-Systemen geeignet, um für mehr IT-Sicherheit zu sorgen. Allerdings ist der Einsatz einer derartigen Lösung für einen Kleinstunternehmer mit zwei bis drei Mitarbeitenden weniger sinnvoll, wenn dahinter keine komplexe IT-Infrastruktur steht. Hier stehen oft Kosten und Nutzen in keinem Verhältnis, sodass ein anderes Security-Konzept passender ist.
Ein Managed SOC schlägt mit etwa 10.000 bis 50.000 Euro im Monat zu Buche – je nach Funktionsumfang, Anzahl der Clients und der Qualität des Dienstleisters. Dazu kommen noch Onboarding-Kosten. Die tatsächlichen Ausgaben sind immer individuell zu betrachten. Sie sind aber deutlich niedriger als beim Aufbau eines selbst betriebenen SOCs. Großunternehmen und Konzerne haben oft ein selbst gemanagtes Security Operations Center.

Der Compliance verpflichtet

Die Frage, für welche Unternehmen ein Managed SOC geeignet ist, lässt sich aber nicht nur an der Größe festmachen, auch die Branchenzugehörigkeit ist ein guter Indikator. Beispielsweise sind Firmen, die dem Finanz- oder Gesundheitssektor angehören, oft einer sehr hohen Gefahr für Cyberangriffe ausgesetzt, weil sie mit sehr sensiblen Kunden- bzw. Patientendaten arbeiten. Gerade diese Unternehmen müssen hohen Regulatorik-Anforderungen gerecht werden.
Ein Beispiel hierfür ist die Network-and-Information-Richtline – kurz NIS oder der Cyber Resilience Act. Je nachdem, welche Regulatorik zu befolgen ist, sind Firmen hierdurch verpflichtet, weitgehende Sicherheitsmaßnahmen zu ergreifen und auch Meldepflichten einzuhalten. Bei NIS2 sind die Erkennung, Analyse, Eindämmung und Reaktion auf schädliche Vorfälle vorgeschrieben. Diese Aufgaben gehören auch zu den Tätigkeiten der Expertinnen und Experten von Managed SOC.
Generell ist dieses Konzept eine gute Lösung für Firmen, die einem hohen Cyberrisiko ausgesetzt sind. Anzudenken ist ein Einsatz aber auch, wenn die IT-Infrastruktur sehr komplex und hierdurch nur schwer zu überblicken ist. Das kann schon bei einem kleinen Mittelständler der Fall sein. □


Bild: G DATA CyberDefense

Über die Autorin

Kathrin Beckert-Plewka ist Public Relations Managerin bei G DATA CyberDefense.

Digitale Souveränität, IT-Sicherheit in Deutschland

Die geopolitischen, wirtschaftlichen und technologischen Entwicklungen der vergangenen Jahre haben eindrucksvoll gezeigt, wie essenziell digitale Souveränität, Resilienz und Sicherheit für den Wirtschaftsstandort Deutschland sind. Um digitale Souveränität zu gewährleisten, müssen Unternehmen und Institutionen die Kontrolle über ihre Daten im eigenen Land behalten – nicht nur aus Datenschutzgründen, sondern auch zur Wahrung ihrer strategischen Unabhängigkeit.

SAYTEC

Die sayTEC AG ist ein IT-Sicherheitsunternehmen und entwickelt Technologien, die genau diese Souveränität und Sicherheit gewährleisten. Hochsichere Netzwerkzugänge (Homeoffice und Client-Access-Lösungen), maßgeschneiderte Cloud-Lösungen, Hochgeschwindigkeits-Backup und ganzheitliche IT-Infrastrukturen – „Made in Germany". Eine moderne und wirtschaftlich sinnvolle IT-Infrastruktur verbunden mit einer nahezu 100-prozentigen Ausfallsicherheit. Mit den ganzheitlichen sayFUSE-Infrastrukturkonzepten (Server, Storage, Backup, ZeroTrust-Netzwerkanbindung, ...) können Unternehmen oder Organisationen die maximale digitale Souveränität, hohe Sicherheit und die absolute Kontrolle über Daten und Netzwerk erreichen.

Künstliche Intelligenz in der IT-Security

Auf der einen Seite ermöglicht KI die automatisierte Erkennung von Anomalien, Predictive Threat Analysis und die Abwehr komplexer Angriffe in Echtzeit. Auf der anderen Seite nutzen Cyberkriminelle KI für automatisierte Angriffe, Deepfakes und die Manipulation von Identitäten. Unternehmen benötigen daher intelligente Sicherheitsarchitekturen, die KI proaktiv als Angreifer erkennen und verteidigen.

Bei sayTEC beginnt deshalb alles mit der externen und internen Netzwerksicherheit. Eine 9-stufige, ineinandergreifende Zero-Trust-Sicherheitslösung (sayTRUST) erkennt KI-Angriffe und kann sie ins Leere laufen lassen. Damit ist der sichere Zugriff auf Unternehmensdaten und Anwendungen von überall möglich – im Büro, im Homeoffice oder am Flughafen.

Kontrolle über Daten im eigenen Land und Compliance

Europäische Unternehmen sind zunehmend gefordert, Lösungen zu implementieren, die Datenhaltung und -verarbeitung nach EU-Standards garantieren. Genau an dieser Stelle setzt die aufeinander abgestimmte Hard- und Softwarelösung von sayTEC an

und bietet eine jederzeit skalierbare Infrastrukturlösung (sayFUSE HCI Infrastructure), die sämtliche gesetzlichen Anforderungen und EU-Standards erfüllt.

sayTEC positioniert sich als ein hochleistungsfähiger, sicherer Anbieter für „Edge-to-Core"-IT-Infrastruktur, die besonders für Organisationen mit verteilten Standorten und hohen Sicherheitsanforderungen geeignet ist. Lese- und Schreibgeschwindigkeiten von 150 GB/s und die 45 PB-Referenz zeigen, dass sayTEC im obersten Leistungssegment Lösungen liefern kann.

Mit der Mandantenfähigkeit für große Organisationen mit verteilten Standorten bietet sayFUSE HCI Infrastructure „Network as a Service (NaaS)"-Varianten an. Ein disruptives Merkmal, das die Bereitstellung und Verwaltung von IT-Infrastruktur an dezentralen Standorten radikal vereinfacht und sicherer macht, mit erheblichen Kosteneinsparungen (keine zusätzlichen Investitionen vor Ort).

Hohe IT-Komplexität als Risiko für Sicherheitslücken

Mit der zunehmenden Vernetzung, hybriden IT-Landschaften, Cloud-Diensten, Microservices und einer wachsenden Zahl an Endpunkten steigt die Komplexität der Systeme. Diese Komplexität ist einer der größten Treiber für Sicherheitslücken und Schwachstellen:

- Unübersichtliche Infrastrukturen: Je mehr Systeme miteinander verbunden sind, desto schwieriger wird es, alle Abhängigkeiten zu erkennen und abzusichern.
- Fehlkonfigurationen: In komplexen Umgebungen sind Konfigurationsfehler nahezu unvermeidlich – und sie gehören zu den Hauptursachen für Datenlecks.
- Shadow IT und fehlende Transparenz: Mitarbeiter nutzen oft nicht genehmigte Tools oder Dienste, was Sicherheitsrichtlinien unterläuft und Angriffsflächen erweitert.
- Patch-Management: In verteilten, heterogenen Systemen ist es eine Herausforderung, Sicherheitsupdates zeitnah und vollständig einzuspielen.

Die Folge: Unternehmen sind anfälliger für Cyberangriffe, insbesondere für Zero-Day-Exploits, Ransomware und Supply-Chain-Angriffe. Die Reduzierung der Komplexität durch Standardisierung und Vereinfachung, automatisierte Sicherheitsprozesse sowie eine ZeroTrust-Architektur bietet die sayTRUST VPSC-Lösung.

Zusammenfassung

In einer Welt, in der Cyberbedrohungen täglich komplexer werden, reicht klassische IT-Sicherheit nicht mehr aus. Unternehmen benötigen strategische Sicherheitslösungen, die weit über den reinen Schutz von Systemen hinausgehen. Genau hier setzen sayTEC-Lösungen an – als zentrale Instanz für Planung, Umsetzung und Steuerung moderner IT-Infrastruktur und Cybersecurity-Maßnahmen.

sayTEC ist ein Spezialist, der eine perfekt aufeinander abgestimmte, hochsichere und ganzheitliche IT-Infrastruktur-Lösung nutzt, um eine höhere Ausfallsicherheit und Integrationsstufe zu erreichen, insbesondere in den Bereichen Zero Trust Security und „as-a-Service"-Bereitstellung für verteilte Netzwerke. Der „Made in Germany"-Ansatz und die nachgewiesene Eignung für sicherheitssensible Umgebungen verleihen sayTEC eine einzigartige Positionierung, die einen klaren Mehrwert gegenüber den großen, globalen Playern bietet , die diesen Grad an vertikaler Integration und spezifischen Fokus auf dezentrale „Network as a Service"-Sicherheit nicht in ihren Kernprodukten haben. ■

Sechs Gartner-Empfehlungen für CISOs

Der Einsatz von generativer KI, identitätsbasierte Angriffe und Burnout: Laut Gartner gehören diese Punkte zu den größten Herausforderungen für CISOs. Das Marktforschungsunternehmen gibt sechs Empfehlungen, die Sicherheitsverantwortliche umsetzen sollten. Von Marvin Djondo-Pacham

Bild: Vadim – stock.adobe.com / KI-generiert

Der Chief Information Security Officer (CISO) eines Unternehmens hat eine besondere Rolle inne. Er oder sie ist für die Entwicklung der organisationsweiten Cybersicherheitsstrategie verantwortlich. Dafür muss er zuerst eine Risikobewertung durchführen, die in jedem Unternehmen individuell ist, und darauf basierend Maßnahmen in die Wege leiten. Das Marktforschungsunternehmen Gartner hat sechs Empfehlungen für CISOs veröffentlicht, die helfen sollen, sich gegen aktuelle Cyberbedrohungen zu wappnen.

1. Unstrukturierte Daten sichern

Die meisten Sicherheitsbemühungen und finanziellen Ressourcen eines Unternehmens konzentrieren sich traditionell auf den Schutz strukturierter Daten wie Datenbanken. Die steigende Relevanz von generativer Künstlicher Intelligenz (GenAI) verändert laut Gartner jedoch die Art und Weise, wie Datensicherheitsprogramme funktionieren. Ihr Schwerpunkt verlagert sich auf den Schutz unstrukturierter Daten wie Texte, Bilder und Videos.

Der Grund dafür ist den Analysten zufolge, dass Texte, Bilder und Videos im Vergleich zu strukturierten Daten innerhalb einer Datenbank in der Regel schwieriger zu überwachen und abzusichern sind. Darüber hinaus kann der Einsatz von generativer KI für die Erstellung und Verarbeitung von unstrukturierten Daten neue Sicherheitsrisiken schaffen, die bisher nicht adressiert wurden. Diese Punkte sollten CISOs beim Einsatz von Sicherheitslösungen berücksichtigen.

2. Maschinenidentitäten kontrollieren und verwalten

Die Nutzung von GenAI, Cloud-Diensten, Automatisierung und DevOps-Praktiken hat zugenommen. Das führt zu mehr Maschinenkonten und Anmeldeinformationen für physische Geräte und Software-Workloads. Wenn Maschinenidentitäten unkontrolliert und unverwaltet bleiben, können sie die Angriffsfläche eines Unternehmens erheblich vergrößern. Kriminelle können sie nutzen und so direkten Zugriff auf sensible Daten, Systeme und Netzwerke erhalten.

Wie groß die Gefahr identitätsbasierter Angriffe ist, zeigt der „IBM X-Force Threat Intelligence Index 2024“. Laut der Studie ist die Übernahme legitimer Konten im Jahr 2023 erstmals der häufigste Einstiegspunkt für Cyberkriminelle gewesen. Insgesamt sind solche Angriffe um über 70 Prozent im Vergleich zum Vorjahr gestiegen. ⇨

⇨ Laut Gartner sollten CISOs mit ihren Teams eine Strategie zur Implementierung eines robusten Identity and Access Managements (IAM) entwickeln. Diese Vorgehensweise ist notwendig zum Schutz vor zunehmend identitätsbasierten Angriffen und sollte den Experten zufolge eine koordinierte unternehmensweite Anstrengung sein, für die die Security-Abteilung zuständig ist.
Eine Gartner-Umfrage, die zwischen August und Oktober 2024 unter 335 IAM-Verantwortlichen durchgeführt wurde, zeigt jedoch noch ein eher unbefriedigendes Ergebnis: IAM-Teams sind bisher nur für 44 Prozent der Maschinenidentitäten eines Unternehmens verantwortlich.

3. Den tatsächlichen Wert der KI messen

Bisher erzielen SRM-Verantwortliche (Security and Risk Management) bei ihren KI-Implementierungen Gartner zufolge gemischte Ergebnisse. Dies liege an verschiedenen Erfolgsfaktoren mit denen sie den Erfolg messen. Deshalb lautet die Empfehlung von Gartner, dass CISOs ihre Initiativen neu priorisieren und sich auf engere Anwendungsfälle mit direkt messbaren Auswirkungen konzentrieren sollten.
Das bedeutet unter anderem die Datenqualität sowie die Integration von KI-Lösungen zu verbessern und transparente Metriken für die Erfolgsmessung zu definieren. Diese taktischen Implementierungen richten KI-Praktiken und -Tools an vorhandenen Messgrößen aus, fügen sie in vorhandene Initiativen ein und erhöhen die Sichtbarkeit des tatsächlichen Werts von KI-Investitionen.

4. Cybersicherheitstechnologien optimieren

Laut einer Gartner-Umfrage unter 162 Unternehmen, die ebenfalls zwischen August und Oktober 2024 durchgeführt wurde, verwenden Organisationen durchschnittlich 45 Cybersicherheitstools. Da es im Bereich Cybersecurity über 3.000 Anbieter gibt, sollten SRM-Verantwortliche ihre Toolsets zum einen konsolidieren und zum anderen stets optimieren, um effizientere und effektivere Sicherheitsprogramme zu entwickeln.
Gartner empfiehlt CISOs, ein Gleichgewicht anzustreben, mit dem das Beschaffungswesen, Sicherheitsarchitekten, Sicherheitsingenieure und andere Beteiligte zufrieden sind. Das helfe, die richtige Sicherheitslage im Unternehmen aufrecht zu erhalten. Um dies zu erreichen, sollten CISOs außerdem die zentralen Sicherheitskontrollen validieren und sich auf eine Architektur konzentrieren, die die Portabilität von Daten verbessert.
Ein Beispiel dafür ist eine Zero-Trust-Architektur. Ein Zero-Trust-Ansatz sorgt dafür, dass alle Datenbewegungen überprüft und authentifiziert werden. Erst dann erfolgt die Übertragung zwischen Systemen. Zudem minieren Ende-zu-Ende-Verschlüsselungen Risiken beim Datentransfer und granulare Zugriffskontrollen sorgen für Compliance mit Regulierungen.
Bedrohungsmodellierung und organisatorische Technologietreiber können ebenfalls zur Bewertung erweiterter Anforderungen verwendet werden. Moderne Lösungen arbeiten dafür mit KI. Denn durch KI-gestützte Mustererkennung lassen sich Sicherheitsrisiken besser vorhersagen. Außerdem können auf Basis von Bedrohungsanalysen dynamische Sicherheitsrichtlinien eingeführt und durchgesetzt werden.

5. Sicherheitskultur als Teil der Unternehmensstrategie

Eine weitere Empfehlung von Gartner sind Security Behaviour and Culture Programs (SBCPs). Die strategischen Maßnahmen innerhalb solcher Programme, zielen darauf ab, ein starkes Sicherheitsbewusstsein innerhalb einer Organisation zu schaffen und sicherheitskon-

Laut Gartner ist Burnout bei CISOs und Sicherheitsteams ein Hauptproblem für die Branche.

formes Verhalten nachhaltig zu fördern. Laut Gartner ist GenAI einer der größten Treiber für den Wandel in diesen Programmen. Unternehmen, die die Technologie mit einer integrierten plattformbasierten Architektur in SBCPs kombinieren, werden bis 2026 zu 40 Prozent weniger von Mitarbeitern verursachte Cybersicherheitsvorfälle erleben.

Solche Security-Awareness-Programme sind derzeit sehr beliebt, da zunehmend erkannt wird, dass sowohl gutes als auch schlechtes menschliches Verhalten entscheidende Komponenten der Cybersicherheit sind. Daher sind kultur- und verhaltensorientierte Aktivitäten zu einem wichtigen Ansatz geworden, um das Verständnis und die Verantwortung für Cyberrisiken auf menschlicher Ebene zu verbessern. Dies spiegele eine strategische Verschiebung hin zur Einbettung der Sicherheit in die Unternehmenskultur wider.

6. Burnout in der Cybersicherheit

Laut Gartner ist Burnout bei CISOs und Sicherheitsteams ein Hauptproblem für die Branche, die bereits von einem systemischen Fachkräftemangel betroffen ist. Die hohen Erwartungen, Verantwortung und die ständige Erreichbarkeit seien nur ein Teil der Gründe für das hohe Stresslevel der Betroffenen.

Weitere Gründe für den allgegenwärtigen Stress seien die Anforderungen, die mit der Absicherung hochkomplexer Organisationen in ständig wechselnden Bedrohungs-, Regulierungs- und Geschäftsumgebungen verbunden sind. Das wird den Analysten zufolge durch begrenzte Autorität und fehlende Unterstützung durch die Führungsebene und wenig Ressourcen verschlimmert. Unternehmen, Abteilungsleiter und CISOs sollte achtsam gegenüber Anzeichen für zu hohen Stress und Burnout sein und darauf reagieren. □

KOBIL mPower: Neue Enterprise-Plattform konsolidiert Identität, Kommunikation, Dokumente und Apps in einem zentralen Hub

KOBIL, führender Anbieter von Sicherheits- und Identitätsmanagement-Lösungen, stellt zur it-sa (7. – 9.10.2025) KOBIL mPower vor. Die Enterprise-Plattform zentralisiert digitale Unternehmensprozesse in einem einzigen Hub: Identität, Kommunikation, Genehmigungen, Dokumente, Applikationen sowie sicheres On- und Offboarding. Mitarbeiter, Dienstleister und Partner haben einfachen und hochsicheren Zugriff darauf. Unternehmen profitieren von mehr Effizienz und Produktivität. Die Lösung ist flexibel skalierbar, Cloud- und hybridfähig sowie konform mit DSGVO, eIDAS und DORA.


Bild: KOBIL Gruppe

„mPower gibt Unternehmen ein Tool an die Hand, um Ordnung in ihre digitalen Prozesse zu bringen sowie Risiken zu minimieren – bei voller Einhaltung regulatorischer Vorgaben."
Ismet Koyun, CEO und Gründer, KOBIL Gruppe

KOBIL mPower: Alles in einem am digitalen Arbeitsplatz

Viele Unternehmen arbeiten mit verschiedensten Tools für Identität, Kommunikation, Signaturen oder Onboarding. Das ist nicht effizient und bringt Sicherheits- und Compliance-Risiken mit sich. KOBIL mPower liefert die Antwort – mit einer einzigen Plattform, die alles in einem bereitstellt:

- **Ein Login** statt verschiedene Tools – Passwordless by Design.
- **Onboarding** in Minuten statt Tagen – effizient und reibungslos.
- Automatisiertes Offboarding – keine vergessenen „Zombie-Accounts".
- **Audit-Trail** und **Compliance by Design** – automatische Erfüllung regulatorischer Vorgaben wie DSGVO, eIDAS und DORA.
- **Digitale Signaturen** und Genehmigungen mit einem Klick – rechtskonform, revisionssicher und eIDAS-ready.
- **Integrierte Kommunikation** mit eigener Chat-Technologie bietet sichere, verschlüsselte und auditierbare Kanäle – nahtlos integriert.

- **Einheitliches Identitäts- und Zugriffsmanagement** – mit Banking-Level-Security, Gerätebindung und multifaktorbasierter Authentifizierung.
- **Offenes Ökosystem** – API-first mit Integrationen zu SAP, Salesforce, ServiceNow und weiteren Plattformen.
- **Low-Code** – für schnelle Anpassungen und die Entwicklung eigener Business-Apps ohne aufwendige Programmierung.

Tiefe Orchestrierung – Cloud-basiert und hybrid nutzbar

KOBIL mPower konsolidiert sämtliche Tools an zentraler Stelle und orchestriert Abhängigkeiten, Rollen und Policies über alle Ebenen hinweg: von Benutzer- und Geräteidentitäten bis zu Genehmigungen, Dokumenten und Kommunikationskanälen. Dadurch lassen sich komplexe Enterprise-Prozesse zentral und regelkonform steuern.
Die Architektur von mPower ist Cloud-native und lässt sich auch in hybriden Umgebungen nutzen. Unternehmen erhalten End-to-End-Transparenz, Zugriffskontrolle und volle Auditierbarkeit.
Als offene, API-first Plattform lässt sich KOBIL mPower flexibel in bestehende IT-Landschaften integrieren. Sie dient als Backend für den gesamten digitalen Lifecycle.

Sicherheit als DNA

mPower wurde in Deutschland entwickelt und folgt höchsten Sicherheitsstandards. Seit mehr als 30 Jahren ist KOBIL ein führender Anbieter von Sicherheits- und Identitätslösungen. Über 100 Millionen Anwender weltweit vertrauen auf KOBIL-Technologie. Mit der Secure SuperApp-Plattform ermöglicht KOBIL Städten, Behörden, Unternehmen und Startups, eigene digitale Ökosysteme sicher und skalierbar aufzubauen – innerhalb weniger Tage. Die Plattform ist als CityApp mit „Istanbul Senin“ und „MyCity Worms“ erfolgreich im Einsatz.

KOBIL auf der it-sa: Halle 9 / Stand 9-346 (bei TeleTrusT) ■

Über die KOBIL Gruppe
Die KOBIL Gruppe ist Weltmarktführer für digitale Identitäts- und mobile Sicherheitslösungen. Gegründet 1986 von Ismet Koyun, entwickelt KOBIL innovative Lösungen für Anwendungsschutz, Benutzerauthentifizierung, Transaktionsautorisierung und mehr. Es ist das einzige Unternehmen auf der Welt, das mit seinen Technologien ein durchgängiges Identitäts- und mobiles Sicherheitsmanagement auf allen Plattformen und Kommunikationskanälen ermöglicht. KOBIL hat Pionierarbeit im Bereich Datensicherheit geleistet und ist Visionär hinsichtlich zukunftsweisender Sicherheitstechnologien. Weltweit vertrauen mehr als 1.000 Unternehmen auf KOBIL, darunter die deutsche Regierung, Airbus, DATEV, Raiffeisen Bank, Commerzbank, Erste Group, ING, Migros Bank, Mastercard oder Siemens.
KOBIL beschäftigt über 500 Mitarbeiter.
Der Hauptsitz ist in Worms.
Weitere Informationen unter www.kobil.com

In acht Schritten zum Security-Awareness-Programm

Zu den größten Sicherheitsrisiken für Unternehmen zählen laut BSI ungeschulte Mitarbeiter. Deshalb sollten Führungskräfte das Bewusstsein für IT-Sicherheit vorleben und ein Awareness-Programm entwickeln, das auf verschiedene Zielgruppen eingeht.

Von Jürgen Paukner, Security-Insider

Mit der Publikationsreihe „Management Blitzlicht“ will das Bundesamt für Sicherheit in der Informationstechnik (BSI) die deutschen Chefetagen über aktuelle Themen der Cybersicherheit informieren und somit ihre Awareness stärken. In der Ausgabe vom Dezember 2024

Bild: stardadw007 – stock.adobe.com / KI-generiert

„Awareness stärken – Risiken minimieren" geht es um den Sicherheitsfaktor Mensch.

Security Awareness ist Chefsache

Als eine der größten Schwachstellen in der Informationssicherheit bezeichnet das BSI den Menschen. Grund dafür sind Social-Engineering-Angriffe. Besonders ungeschultes Personal stelle eine Herausforderung dar, die das Management jedoch selbst bewältigen könne. Als Werkzeug empfiehlt das Bundesamt der Chefetage effektive Trainings sowie das richtige Wissen. Unternehmen sollen ihre Teams als wesentlichen Bestandteil der Sicherheitsstrategie integrieren und sie in die Gesamtstrategie des Unternehmens einbeziehen.

Dazu gehört die offene Kommunikation über die Relevanz von Sicherheitsmaßnahmen auf verschiedenen Ebenen sowie die Verantwortung jedes Einzelnen – auch über die IT-Abteilung hinaus. „Investieren Sie langfristig in die Sicherheit Ihres gesamten Unternehmens, indem Sie kontinuierlich das Informationssicherheitsbewusstsein Ihrer Mitarbeitenden schärfen. Der Sicherheitsfaktor Mensch spielt eine wichtige Rolle bei der Abwehr von Cyberangriffen. Geschultes Personal und eine sensibilisierte Belegschaft sind genauso relevant wie technische Maßnahmen. Informationssicherheit betrifft alle Ebenen des Unternehmens, von der Geschäftsführung bis zu den Mitarbeitenden in jeder Abteilung", heißt es im Management Blitzlicht.

Cyber-Awareness-Programm in acht Schritten

Führungskräfte sollten dem BSI zufolge die Initiative ergreifen und IT-Sicherheit vorleben. Dazu gehöre es, sich strikt an die eigenen Sicherheitsmaßnahmen zu halten, was zudem die Motivation der Mitarbeitenden erhöhe. Die European Union Agency for Cybersecurity (ENISA) hat acht Schritte definiert, die Unternehmen helfen sollen, ein eigenes Awareness-Programm zu entwickeln:

1. Sensibilisierungsziele ermitteln
2. Finanzielle Mittel sicherstellen
3. Personelle Ressourcen sicherstellen
4. Zielgruppen identifizieren
5. Passende Methoden für die Zielgruppen wählen
6. Zeitplan erstellen
7. Mit der Durchführung starten
8. Programm evaluieren und überarbeiten

Um das Bewusstsein für Cybersicherheit im Unternehmen zu verankern, empfiehlt das BSI:

- Kontinuierliche Fortbildung, wobei die Inhalte der Trainings und Schulungen variieren können. Sie sollten jedoch regelmäßig wiederholt werden. Außerdem seien Informationen, die in kleinen Paketen vermittelt werden, oft effektiver als umfangreiche.
- Gamification, Infotainment und Simulationen seien eine gute Möglichkeit, die verschiedenen Zielgruppen effektiv anzusprechen. Dies motiviere die Mitarbeitenden und mache die Inhalte spannender. Unternehmen sollten zudem einen Bezug zum Arbeitsalltag herstellen und konkrete Tipps und Vorgaben für die gewünschte Vorgehensweise geben.
- Transparente Kommunikation ist das A und O. Das BSI empfiehlt, Regeln und deren Wichtigkeit immer wieder zu kommunizieren. Sicherheitsvorfälle und erfolgte Maßnahmen sollten intern ebenfalls transparent bekannt gemacht werden. Dazu gehöre auch, einen Weg für die Mitarbeitenden einzurichten, über den sie Vorfälle oder einen Verdacht unkompliziert und schnell melden können.
- Eine positive Fehlerkultur ist laut BSI entscheidend, damit sich die Mitarbeitenden bei einem möglichen Cybersicherheitsvorfall an die Chefetage wenden und diesen zeitig melden. Denn: Aus Fehlern lassen sich wertvolle Erfahrungen gewinnen. □

Deutschen Angestellten fehlt das Bewusstsein für Cyberangriffe

„Wir sind kein interessantes Ziel für Angreifer"– diese Meinung vertreten 44 Prozent der Arbeitnehmer in deutschen Klein- und Mittelständischen Unternehmen. Doch die Gefahr eines Cyberangriffs besteht auch dort.

Von Ira Zahorsky, IT-BUSINESS

Mehr als die Hälfte der Belegschaft von kleinen und mittelständischen Unternehmen (KMU) schätzen ihre Firma als uninteressantes Ziel für Cyberkriminelle ein. Zu diesem Ergebnis kommt die aktuelle Studie „Cybersicherheit in Zahlen" von G DATA CyberDefense, Statista und Brand eins. Ihnen gaben im März und April 2024 mehr als 5.000 Beschäftigte im Alter von 16 bis 70 Jahren aus Unternehmen aller Branchen in Deutschland Auskunft. Sie berichteten über ihr Wissen, ihre Einschätzungen und Erfahrungen im Umgang mit IT.

Gefahrenbewusstsein wächst mit Unternehmensgröße

Je größer das Unternehmen ist, desto eher wird es von Mitarbeitern als potenzielles Ziel für Cyberangriffe wahrgenommen. Dies ist die zentrale Erkenntnis der Befragung. In Firmen mit 250 bis 999 Beschäftigten hält G DATA zufolge gut die Hälfte der Befragten ihren Arbeitgeber für ein potenzielles Angriffsziel. In großen Unternehmen mit mehr als 1.000 Mitarbeitern sei das Bewusstsein für das Angriffsrisiko bei fast 70 Prozent der Beschäftigten vorhanden. Laut den Studienautoren liege das an den regulierten Prozessen und verpflichtenden Sicherheitsmaßnahmen, über die große Konzerne oft verfügen. Doch diese Fehleinschätzung über die Korrelation zwischen Unternehmensgröße und der Wahrscheinlichkeit einer Cyberattacke könne im schlimmsten Fall das Risiko eines Angriffs für KMU erhöhen. Laut der Bitkom-Studie Wirtschaftsschutz 2024 sind KMU eher von Phishing als von komplexen Angriffskampagnen betroffen. Denn Unaufmerksamkeit und geringes Bewusstsein über potenzielle Gefahren erleichtern Kriminellen den Diebstahl von Firmendaten.

G DATA warnt Unternehmen deshalb davor, seine Mitarbeiter bei der Sicherheitsstrategie außen vor zu lassen. Eine wirksame IT-Sicherheitsstrategie berücksichtige neben technischen Schutzmaßnahmen auch die Mitarbeiter. Informationssicherheit sei eine Teamaufgabe. Alle Beschäftigten sollen potenzielle Gefahren kennen und verantwortungsvoll handeln können.

Schaden durch Cybercrime weiterhin hoch

Aus der Umfrage wird klar: Den Arbeitnehmern fehlt das Bewusstsein für potenzielle

Bild: Jss – stock.adobe.com / KI-generiert

Cyberangriffe. Dabei zeigt die „Cybersicherheit in Zahlen"-Studie auch, dass die Gefahr allgegenwärtig ist. 36 Prozent der Befragten Angestellten in IT- und EDV-Unternehmen haben in den vergangen zwei Jahren einen Cyberangriff erlebt. Bei IT-Security-Firmen sind es sogar 46 Prozent.

Aktuelle Berichte und Analysen verschiedener Institutionen verdeutlichen die Gefahr durch Cyberangriffe. Laut dem Bundeslagebild Cybercrime 2024 des Bundeskriminalamts (BKA) wurden im Jahr 2024 in Deutschland insgesamt 131.391 Fälle von Cyberkriminalität registriert. Bei weiteren 201.877 Straftaten handelt es sich um sogenannte Auslandstaten, die vom Ausland oder einem unbekannten Ort aus verübt wurden. Zudem schätzt der Digitalverband Bitkom den wirtschaftlichen Schaden durch Cyberangriffe in Deutschland für das Jahr 2024 auf 178,6 Milliarden Euro. Diese Zahlen verdeutlichen die anhaltende Relevanz von Cyberkriminalität. Um die Belegschaft für die Gefahren zu sensibilisieren, können Unternehmen regelmäßige Mitarbeiterschulungen durchführen. Dadurch lernen die Mitarbeiter Gefahren zu erkennen und entwickeln ein Sicherheitsbewusstsein.

Risikobewusstsein stärken

„Angreifer wählen ihre Ziele nicht nach Branche oder Größe, sondern nach Schwachstellen aus", erläutert Andreas Lüning, Vorstand und Mitgründer G DATA CyberDefense. „Dazu zählen verwundbare Strukturen, mangelhaft gesicherte Systeme und unaufmerksame Mitarbeitende. In jedem Unternehmen ist eine Sicherheitsstrategie sinnvoll, die das Risikobewusstsein des gesamten Teams stärkt." □

Was Datenschutzbehörden für die KI-Aufsicht planen

Bei der nationalen Umsetzung der KI-Verordnung der EU soll die Bundesnetzagentur die Marktaufsicht in Deutschland übernehmen, nicht aber die Datenschutzaufsichtsbehörden. Das bedeutet aber nicht, dass die Datenschutzbehörden bei KI-Projekten nicht mehr involviert werden müssen. Eine Vielzahl an KI-Initiativen der Datenschutzaufsicht unterstreicht dies.

Von Dipl.-Phys. Oliver Schonschek

Bild: chiew – stock.adobe.com

Die nationale Aufsicht bei Fragen über Künstliche Intelligenz ist aufgrund der sektoralen Zuständigkeiten und der föderalen Aufteilung komplex, so der Deutsche Bundestag. Gemeint ist damit, dass der Umgang mit KI nicht nur in den einzelnen Bundesländern, sondern auch für alle möglichen Branchen kontrolliert und überwacht werden muss.

Die KI-VO (KI-Verordnung) sieht bereits in einigen Fällen die sektorspezifische Zuständigkeit der Datenschutzbehörden als Marktüberwachungsbehörden vor. Die Datenschutzaufsichtsbehörden erklärten sich bereit, die Aufgabe der nationalen Marktüberwachung für KI-Systeme zu übernehmen. Als Argumente nannten sie die bestehenden Zuständigkeiten nach der DSGVO (Datenschutz-Grundverordnung der EU), eine langjährige Expertise im digitalen Grundrechtsschutz und etablierte, kooperative Aufsichts- sowie Abstimmungsmechanismen.

Aus Sicht der deutschen Wirtschaft sprechen aber einige Argumente dafür, die Bundesnetzagentur (BNetzA) mit der Aufgabe der nationalen KI-Aufsicht zu betrauen, wie die Deutsche Industrie- und Handelskammer erklärte. Die BNetzA könne an bisherige Erfahrungen anknüpfen, als zentrale Ansprechbehörde fungieren und damit eine bundesweit einheitliche Auslegung gewährleisten. In der Vergangenheit hätte sie dies bereits mit der Aufsicht über Unternehmen in anderen Bereichen unter Beweis gestellt, unter anderem in der Telekommunikation sowie im Strommarkt.

Inzwischen hat sich die Bundesregierung für eine deutsche KI-Aufsicht durch die Bundesnetzagentur entschieden. Doch die Datenschutzaufsichtsbehörden sind damit nicht „aus dem Spiel".

Zahlreiche KI-Initiativen der Datenschutzbehörden

„Das Verhältnis von Künstlicher Intelligenz zum Datenschutz ist ein Schwerpunkt meiner Behörde. Schon 2019 haben wir in unserer Hambacher Erklärung als deutsche Datenschutzaufsichtsbehörden eine humanistische und damit grundrechtsschützende Ausrichtung von KI als Standard gefordert", erklärt Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz.

Wie sehr die Datenschutzaufsicht mit dem Thema KI in Verbindung bleibt, zeigen umfangreiche Initiativen dieser Aufsichtsbehörden rund um Künstliche Intelligenz. Das sollte auch nicht verwundern, denn KI-Systeme verarbeiten in vielen Fällen personenbezogene Daten, zudem haben die Datenschutzaufsichtsbehörden aus der KI-Verordnung heraus definierte Aufgaben bei der Marktüberwachung bei KI, in den besonders grundrechtsrelevanten Bereichen der Strafverfolgung, Migration, Integration und Wahlen.

„Auch für Künstliche Intelligenz gilt das Datenschutzrecht und wir beschäftigen uns bereits gegenwärtig mit der Technologie, ihrer Anwendung durch Verwaltung und Wirtschaft sowie ihrer Fortentwicklung", so Prof. Kugelmann. „Zugleich geht es darum, die Entwicklung im Rahmen des Datenschutzrechts in die Richtung einer menschenzentrierten und grundrechtsschonenden Nutzung von Systemen Künstlicher Intelligenz zu lenken."

Beispiele für Beratung und Überwachung bei KI

Tatsächlich sind die Datenschutzaufsichtsbehörden sehr aktiv im Bereich der Beratung und Überwachung von KI, wie diese Beispiele zeigen:

- Mit einem Themenschwerpunkt zu KI & Datenschutz bietet das Bayerische Landesamt für Datenschutzaufsicht Unternehmen erste Orientierung und Hilfestellungen für den datenschutzgerechten Einsatz von KI-Technologien. Dazu der Präsident des Landesamts ⇨

Michael Will: „Gerade kleine und mittlere Unternehmen brauchen mehr als akademische Leuchtturmprojekte, um ihren passenden Zugang zum Zukunftsthema KI zu finden. Die neuen Informationsangebote des Landesamts bieten deshalb einen Lotsendienst durch die Klippen neuer Begriffe, Funktionen und Anforderungen, damit der digitale Alltag in Unternehmen auch mit KI gelingt."

- Der Landesbeauftragte für den Datenschutz (LfD) Niedersachsen begleitet als Projektpartner das Forschungsprojekt CRAI zur Entwicklung vertrauenswürdiger KI-Anwendungen für den Mittelstand. Im Rahmen des Projekts entsteht in Niedersachsen ein Reallabor, in dem praxisnahe Lösungen für den Einsatz vertrauenswürdiger, auf Künstlicher Intelligenz basierter Geschäftsmodelle in mittelständischen Unternehmen entwickelt werden.
- Ein vom Landesbeauftragten für den Datenschutz (LfD) Niedersachsen, Denis Lehmkemper, einberufener Expertenkreis zu Künstlicher Intelligenz hat seine Arbeit aufgenommen. Ziel des Expertenkreises ist es, Rahmenbedingungen für den datenschutzkonformen Einsatz Künstlicher Intelligenz in der Wirtschaft wie auch in der niedersächsischen Verwaltung zu formulieren. Es sollen technische und rechtliche Gestaltungsvorschläge für einen datenschutzfreundlichen KI-Einsatz

Bild: tadamichi – stock.adobe.com

Das Training von Large Language Models mit personenbezogenen Daten muss datenschutzkonform erfolgen.

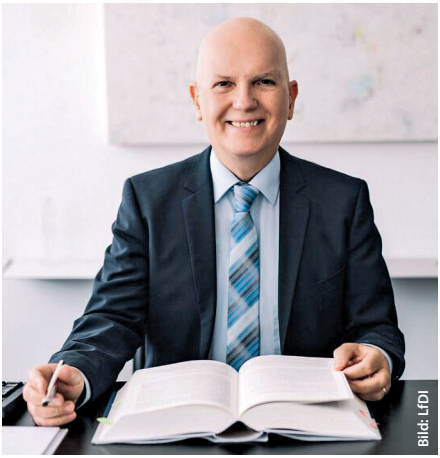
erarbeitet werden, um diese technische Innovation zu fördern.

- Forschende der Universität Bayreuth schaffen in Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Rheinland-Pfalz die Grundlage für digitale Experimentierumgebungen. In diesen können Unternehmen und Behörden künftig die Datenschutzkonformität ihrer Anwendungen testen. Das Projekt wird vom Bundesministerium für Bildung und Forschung (BMBF) gefördert. Obwohl das europäische Recht für den Bereich der Künstlichen Intelligenz die Einrichtung von „KI-Reallaboren" bereits verbindlich vorgibt, ist noch weitgehend offen, wie eine Sandbox unter deutschen Regularien realisiert werden kann. „Unser Projekt ist ein wichtiger Schritt in Richtung sicherer und innovativer digitaler Anwendungen in Deutschland. Wir stellen damit eine Balance zwischen dem Schutz sensibler Daten und der Förderung von Innovationen her, indem wir eine Umgebung schaffen, in der Unternehmen neue Technologien und Lösungen testen können, ohne die Privatsphäre der Nutzenden zu gefährden", erläutert Prof. Dr. Christoph Krönke vom Lehrstuhl Öffentliches Recht I der Universität Bayreuth.

KI-VO: Auch Datenschutzbehörden werden sie umsetzen

Offensichtlich sollten KI-Projekte auch immer den Datenschutz im Blick behalten, so wie der Datenschutz die KI im Fokus hat und haben wird. Bei der Strategieklausur der Datenschutzaufsichtsbehörden in Speyer erklärten diese, dass es ihre Aufgabe sei, Behörden und Unternehmen, die KI einsetzen, mit ihrer Expertise für den Schutz personenbezogener Daten eng und praxisorientiert zu begleiten. Dies beginne bereits mit dem Training von generativen KI-Modellen, die ganz offensichtlich das Kernelement der meisten in der Praxis eingesetzten KI-Systeme bilden werden. Wer ihre Funktionsbedingungen rechtlich und technisch genauer analysiert, werde feststellen, dass schon hier in den allermeisten Fällen eine Verarbeitung personenbezogener Daten nicht auszuschließen ist. Für die Nutzung von LLMs (Large Language Models) zum Beispiel gibt der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) diese zentralen Hinweise: Die bloße Speicherung eines LLMs stellt keine Verarbeitung im Sinne der DSGVO dar. Mangels Speicherung personenbezogener Daten im LLM können die Betroffenenrechte der DSGVO nicht das Modell selbst zum Gegenstand haben. Aber das Training von LLMs mit personenbezogenen Daten muss datenschutzkonform erfolgen.

Der Datenschutz bei KI ist und bleibt also ein zentrales Thema und damit bleiben die Datenschutzbehörden auch Teil der KI-Aufsicht. □



„Künstliche Intelligenz und Datenschutz gehören zusammen", Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz.

Wie mit KI der Identitätsdiebstahl noch bedrohlicher wird

Künstliche Intelligenz (KI) kann den Schutz digitaler Identitäten verbessern, ist aber gleichzeitig auch ein Werkzeug in den Händen der Internetkriminellen, die Zugangsdaten ausspähen und Identitäten stehlen wollen. Die Bedeutung sicherer, digitaler Identitäten nimmt durch die neue Bedrohungslage weiter zu. Unternehmen und Behörden sollten wissen, wie KI zum erhöhten Risiko für digitale Identitäten beitragen kann.

Von Dipl.-Phys. Oliver Schonschek

Bild: Andrea Danti – stock.adobe.com

Untersuchungen wie die Studie „Wirtschaftsschutz 2024“ des Digitalverbands Bitkom machen sehr deutlich, was Cyberkriminelle bei ihren digitalen Attacken erbeuten wollen: Demnach waren 74 Prozent der Unternehmen vom digitalen Ausspähen von Geschäftsdaten „betroffen“ oder „vermutlich betroffen“, ein Plus von vier Prozentpunkten im Vergleich zum Vorjahr. Die von Datendiebstahl betroffenen Unternehmen berichten aber nicht nur, dass Kundendaten (62 Prozent, plus sechs Prozentpunkte) gestohlen werden, sondern auch Zugangsdaten oder Passwörter (35 Prozent, plus zwölf Prozentpunkte).

Betrachtet man die vorherrschenden Arten der Cyberangriffe, berichten Unternehmen insbesondere von Schäden durch Ransomware (31 Prozent), dahinter folgen aber gleich die Phishing-Attacken (26 Prozent) und die Angriffe auf Passwörter (24 Prozent) und damit der Diebstahl digitaler Identitäten. Das ist nicht verwunderlich, denn mit gestohlenen oder gefälschten Identitäten versuchen die Internetkriminellen an ihre Datenbeute zu gelangen. Dabei kommen auch neue Technologien wie KI zum Einsatz.

KI wird zum wichtigen Werkzeug der Identitätsdiebe

Im Jahr 2024 waren Cyberattacken unter Einsatz von Verfahren mit Künstlicher Intelligenz zwar noch nicht so weit verbreitet, ergab die Bitkom-Umfrage: Schäden durch neue Angriffsmethoden wie Deep Fakes und Robo Calls (je drei Prozent), die vor allem durch die Verbreitung von Künstlicher Intelligenz einfacher werden, waren eher selten.

Das sollte aber nicht dazu führen, dass die Risiken durch KI-basierte Cyberattacken unterschätzt werden. So erklärte das BSI (Bundesamt für Sicherheit in der Informationstechnik) in der Untersuchung „Chancen und Risiken generativer KI-Sprachmodelle für Industrie und Behörden“: KI ermöglicht es Angreifenden mit geringsten Fremdsprachenkenntnissen, qualitativ hochwertige Phishing-Nachrichten zu erstellen. Herkömmliche Methoden zur Erkennung betrügerischer Nachrichten wie die Prüfung auf Rechtschreibfehler und unkonventionellen Sprachgebrauch reichen zur Erkennung von Phishing-Angriffen damit nicht mehr aus. Zudem erklärte BSI-Präsidentin Claudia Plattner: „Immer häufiger spielen dabei auch Inhalte eine Rolle, die mit Hilfe von KI manipuliert oder komplett gefälscht wurden. Deswegen müssen wir dafür sorgen, dass Texte, Bilder und Videos mit technischen Werkzeugen auf ihre Authentizität hin überprüft werden können!“ ⮑

Das BSI warnt vor KI-basierten Attacken

Das BSI gibt auch Beispiele, wie man sich eine KI-Unterstützung bei Cyberangriffen auf Identitäten und Daten vorstellen kann: Demnach macht Künstliche Intelligenz es leichter, Videos zu manipulieren oder die Stimmen anderer am Telefon zu imitieren (Deepfakes). So können sich Betrügerinnen und Betrüger zum Beispiel als enge Kontakte einer Person ausgeben, eine Notlage fingieren und Geldzahlungen anfordern.

Doch es gibt noch mehr kriminelle Möglichkeiten: KI-Anwendungen erfassen große Datenmengen, auf die es auch Cyberkriminelle abgesehen haben, so das BSI weiter. Denkbar sei es, dass Cyberkriminelle Anwendungen so manipulieren, dass sie nicht mehr oder anders als vorgesehen reagieren – beispielsweise gezielt nach sensiblen Daten fragen. Postadresse, Passwörter oder Kreditkarteninformationen könnten so in falsche Hände geraten.

Phishing und Daten-Leaks gehören damit zu den größten Bedrohungen und können durch bösartige KI-Nutzung noch kritischer werden. Dazu BSI-Präsidentin Claudia Plattner: „Eine Achillesferse ist dabei die Authentisierung". Passwortbasierte Authentisierungsverfahren seien nicht ausreichend resistent gegen Phishing und Daten-Leaks gewappnet. Das BSI empfiehlt daher dringend den Einsatz einer Zwei-Faktor-Authentisierung (2FA), welche die Online-Konten zusätzlich absichert. Besonders vielversprechend sei die passwortlose Authentisierung.

Europol berichtet von KI-basierter Kriminalität

Das BSI ist mit den Warnungen nicht allein. Die Europäische Polizeibehörde Europol berichtet von Veränderungen bei der organisierten Kriminalität und nennt dabei explizit die Gefahren durch KI: Künstliche Intelligenz verändert demnach die Landschaft der organisierten Kriminalität grundlegend. Kriminelle nutzen neue Technologien zeitnah und verwenden sie sowohl als Katalysator für Kriminalität als auch zur Steigerung der Effizienz, betont Europol.

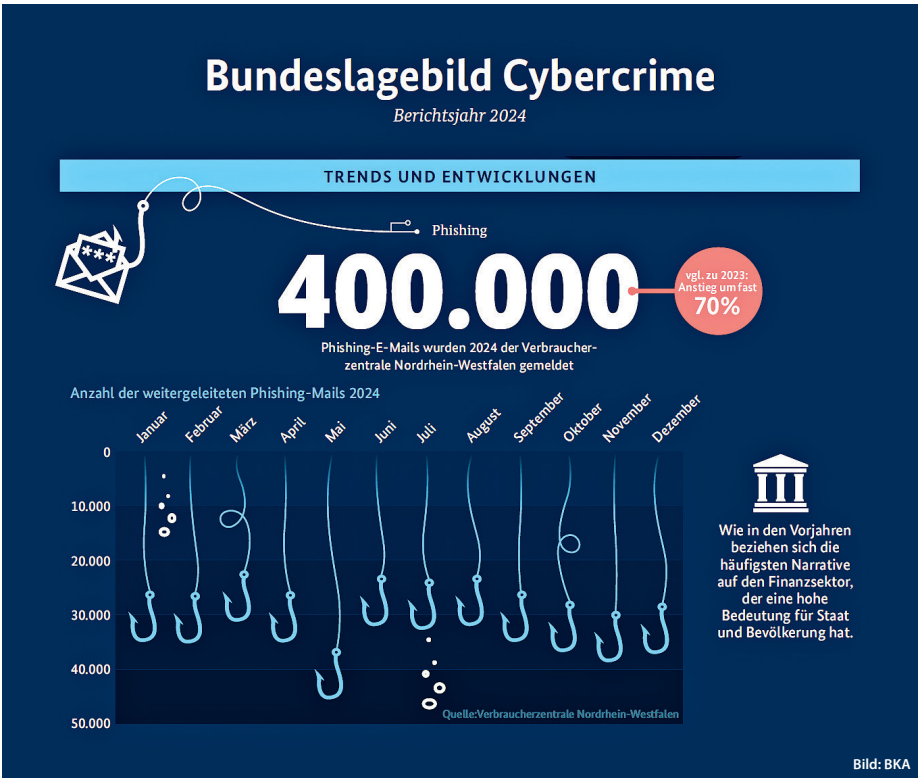
Dieselben Eigenschaften, die KI revolutionär machen – Zugänglichkeit, Anpassungsfähigkeit und Raffinesse – machen sie auch zu einem mächtigen Werkzeug für kriminelle Netzwerke. Diese Technologien automatisieren und erweitern kriminelle Aktivitäten, machen sie skalierbarer und schwerer zu erkennen, warnt die Polizeibehörde.

Der Europol-Bericht „EU-SOCTA 2025" hebt unter anderem die Risiken durch Online-Betrugssysteme hervor, die zunehmend durch KI-gestütztes Social Engineering und den Zugriff auf riesige Datenmengen, einschließlich gestohlener persönlicher Informationen, vorangetrieben werden.

BKA-Lagebericht Cybercrime nennt ebenfalls KI-basiertes Phishing

Auch das Bundeskriminalamt (BKA) sieht eine steigende Gefahr durch KI, wenn es zum Beispiel um Phishing-Attacken geht. Zu den zentralen Erkenntnissen des „Bundeslagebilds Cybercrime 2024" gehört: Phishing-Mails werden durch den Einsatz von Künstlicher Intelligenz sprachlich gesehen professioneller und persönlicher. Dadurch steigt das Risiko, dass die Empfänger sie nicht als schadhafte Phishing-Mail erkennen.

Das BKA macht deutlich: Die stetigen Fortentwicklungen im Bereich der Künstlichen Intelligenz kamen 2024 bereits zum Tragen. Seit Veröffentlichung des ersten ChatGPT-Modells im November 2023 wurden inzwischen zahlreiche generative KI-Modelle (weiter-) entwickelt, die nicht nur Wort und Schrift, sondern auch Bild, Ton und Video generieren und verarbeiten können. Viele kriminelle Akteure ergänzen bereits ihr bisheriges Repertoire durch generative KI.



Das Bundeslagebild Cybercrime 2024 des BKA beschreibt die Risiken durch Phishing und betont dabei die Verschärfung der Lage durch KI-Einsatz auf Seiten der Angreifenden.

Im Bereich Cybercrime im engeren Sinne sind davon vorwiegend die Phänomene Phishing und Malware-Entwicklung betroffen, so das BKA. Da KI-Modelle für jegliche Bedürfnisse kontinuierlich weiterentwickelt werden, ist für das Jahr 2025 eine weitere Verschärfung KI-unterstützer Straftaten zu erwarten. Dabei gilt gerade für den Bereich Cybercrime im engeren Sinne: Auch wenn KI bestehende Modi Operandi bislang nicht revolutioniert hat, kann sie Cyberangriffe nicht nur professioneller gestalten, sondern durch Automatisierung auch schneller ein breiteres Ausmaß und folglich eine höhere Kritikalität erreichen, warnt das Bundeskriminalamt.

Identitätsschutz muss sich gegen KI-Risiken rüsten

Offensichtlich muss der Schutz digitaler Identitäten auch wegen der KI-Risiken weiter optimiert werden. Dazu gehört ein verbesserter Phishing-Schutz mit einer Zwei-Faktor-Authentifizierung, die ohne Passwörter auskommt und Phishing-resistent ist. □

Impressum

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21, 86157 Augsburg
Tel. 0821/2177-0, Fax 0821/2177-150
eMail it-business@vogel.de
Internet www.it-business.de

Geschäftsführer:
Tobias Teske, Günter Schürger

IT-BUSINESS

Redaktion: Sylvia Lösel – Chefredakteurin (verantwortlich für redaktionelle Inhalte), Heidi Schuster – CvD/ltd. Redakteurin, Natalie Forell

Co-Publisher: Lilli Kos (verantwortlich für den Anzeigenteil)

Account Management:
Besa Agaj (International Accounts), David Holliday, Stephanie Steen

SECURITY-INSIDER

Redaktion: Peter Schmitz – Chefredakteur (verantwortlich für redaktionelle Inhalte), Jürgen Paukner – CvD, Melanie Staudacher

Anzeigendisposition: Denise Falloni, Mihaela Mikolic

Grafik & Layout: Carin Böhm (Titel), Jürgen Paukner, Johannes Rath, Udo Scherlin, Gaby Weihmayer

EBV: Carin Böhm, Gaby Weihmayer

Anzeigen-Layout: Johannes Rath

Druck: deVega Medien GmbH, Anwaltinger Straße 10, 86156 Augsburg

Vogel IT-Medien, Augsburg, ist eine 100-prozentige Tochtergesellschaft der **Vogel Communications Group**, Würzburg, einem der führenden deutschen Fachinformationsanbieter mit 100+ Fachzeitschriften, 100+ Webportalen, 100+ Business-Events sowie zahlreichen mobilen Angeboten und internationalen Aktivitäten. Seit 1991 gibt Vogel IT-Medien Fachmedien für Entscheider heraus, die mit der Produktion, der Beschaffung oder dem Einsatz von Informationstechnologie beruflich befasst sind. Dabei bietet der Verlag neben Print- und Online-Medien auch ein breites Veranstaltungsportfolio an.

Die wichtigsten Angebote des Verlages sind **IT-BUSINESS, Vogel IT-Akademie, eGovernment, Healthcare Digital, BigData-Insider, CloudComputing-Insider, DataCenter-Insider, IP-Insider, Security-Insider** und **Storage-Insider**.

Inserenten

Bundesverband IT-Sicherheit e.V. (TeleTrusT)	Berlin	https://www.teletrust.de/	U3
G DATA Software AG	Bochum	https://www.gdata.de	18, U2
KOBIL GmbH	Worms	https://www.kobil.com/en/	44
INFODAS GmbH	Köln	https://www.infodas.com	28
NCP engineering GmbH	Nürnberg	https://www.ncp-e.com/de/	14
sayTEC AG	München	https://www.saytec.eu	38
secunet Security Networks AG	Essen	https://www.secunet.com	8
SEPPmail AG	Brunntal bei München	https://www.seppmail.com/de/	22
TDT AG	Essenbach	https://tdt.de	32
Vogel IT-Akademie	Augsburg	https://www.vogelitakademie.de	5

TeleTrusT
Pioneers in IT security.

Bundesverband IT-Sicherheit e.V.
IT Security Association Germany

www.teletrust.de

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

www.teletrust.de/itsmig

Die Verwendung des markenrechtlich geschützten TeleTrusT-Vertrauenszeichens "IT Security made in Germany" ("ITSMIG") wird interessierten Verbandsmitgliedern durch TeleTrusT auf Antrag und Konformitätserklärung zu den nachstehenden Kriterien zeitlich befristet gestattet.

1. **Der Unternehmenshauptsitz muss in Deutschland sein.**
2. **Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.**
3. **Die angebotenen Produkte dürfen keine versteckten Zugänge enthalten (keine "Backdoors").**
4. **Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in Deutschland stattfinden.**
5. **Das Unternehmen muss sich verpflichten, den Anforderungen des Datenschutzrechtes zu genügen.**

Besuchen Sie TeleTrusT auf der it-sa in Halle 9 / Stand 9-346.