OKTOBER **2026**

ISSN 1864-0907 • 7,- €

IT-BUSINESS

IT Security

made in Germany



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

VOGEL IT MEDIEN



Managed Extended Detection and Response (MXDR)

24/7-Expertenschutz aus Deutschland

Erweitern Sie Ihren Managed Service: Unsere Experten erkennen und stoppen Cyber-Angriffe für Ihre Kunden – bevor diese zum Ausnahmezustand führen. Rund um die Uhr. Komplett entwickelt, gehostet und betreut in Deutschland. Für mehr CyberVertrauen.

Jetzt kostenlos testen

G DATA CyberDefense | TRUST IN GERMAN SICHERHEIT

IT-Sicherheit als Grundlage digitaler Souveränität



Dr. Holger Mühlbauer
Geschäftsführer
Bundesverband
IT-Sicherheit e.V.
(TeleTrusT)

Bild: TeleTrusT

Wie souverän sind wir digital, wenn zentrale Technologien, Daten und Infrastrukturen von wenigen Anbietern abhängen? Diese Frage wird immer wichtiger. Cloud-Dienste, mobile Geräte und Künstliche Intelligenz gehören längst zu unserem Arbeitsalltag. Sie machen vieles einfacher und effizienter, schaffen aber zugleich neue Abhängigkeiten und Angriffsflächen.

Digitale Souveränität bedeutet nicht, jede Technologie selbst zu entwickeln. Entscheidend ist, Abhängigkeiten zu kennen, Risiken einschätzen zu können und dort Alternativen zu haben, wo es kritisch wird. IT-Sicherheit ist dabei ein zentrales Kriterium.

Auch die europäischen Vorgaben setzen neue Maßstäbe. Der Cyber Resilience Act verpflichtet Hersteller, Sicherheit von Anfang an mitzudenken und ihre Produkte über den gesamten Lebenszyklus hinweg sicher zu halten. Security by Design und ein verlässlicher Umgang mit Schwachstellen werden damit zu festen Bestandteilen der Produktentwicklung. Entscheidend ist, dass daraus nicht nur neue Pflichten entstehen, sondern mehr Sicherheit in der Praxis.

Gleichzeitig verändert sich die Bedrohungslage. Quantencomputer könnten künftig Verschlüsselungsverfahren gefährden, die heute als sicher gelten. Bei mobilen Geräten sind die Risiken schon heute greifbar: Sie ermöglichen den Zugang zu Unternehmenssystemen und sensiblen Daten. Sicherheitskonzepte müssen deshalb mit der technischen Entwicklung Schritt halten.

Auch die Frage nach Daten und Identitäten gewinnt an Bedeutung. Bei Cloud-Diensten geht es längst nicht mehr nur um den Speicherort, sondern auch um Kontrolle und Abhängigkeiten. Gleichzeitig reichen Passwörter als alleiniger Schutz immer weniger aus. Sichere digitale Identitäten und starke Authentifizierung werden zum wichtigen Bestandteil moderner IT-Sicherheit.

Mit Künstlicher Intelligenz kommen weitere Herausforderungen hinzu. Hohe Rechenleistung, sensible Daten und neue Angriffsmöglichkeiten treffen aufeinander. Sicherheit muss deshalb bereits bei der Infrastruktur beginnen, auf der KI betrieben wird.

Diese Publikation nimmt aktuelle Entwicklungen in den Blick und zeigt, wie eng Technologie, Regulierung und IT-Sicherheit miteinander verbunden sind. Sie ordnet ein, wo sich Risiken verändern, welche Fragen sich daraus ergeben und welche Lösungen bereits heute möglich sind.

"IT Security made in Germany" steht dabei für einen Anspruch: Sicherheit und Innovation miteinander zu verbinden und damit die Grundlage für eine digitale Zukunft zu schaffen, in der Europa handlungsfähig und souverän bleibt. □

IT SECURITY MADE IN GERMANY

Die Initiative: Vertrauen hat einen Namen 6

IT-SICHERHEIT UND GESETZGEBUNG

Cyber Resilience Act: EU-Kommission veröffentlicht CRA-Leitfaden 10

Stellungnahme von TeleTrusT: BMI veröffentlicht Referentenentwurf zur Umsetzung des CRA 16

Folgen einer Zentralisierung im Datenschutz: Praxis-Check: Wie kann die neue Datenschutzaufsicht aussehen? 20

DATENSICHERHEIT UND CLOUD

r-tec Cyber Security Lagebericht: Externe Admins, interner Kontrollverlust 25

Bitkom Cloud Report 2026 deckt Souveränitätslücke auf: Cloud-Abhängigkeit als KRITIS-Risiko – Revival der Datensicherung vor Ort 30

SICHERHEIT DIGITALER IDENTITÄTEN

Identity Access Management: Darum profitiert der Channel 38

Digitale Identität für KI-Agenten: Gibt es da nicht auch was von eIDAS 2.0? 42

APP-ENTWICKLUNG UND QUANTEN-KRYPTOGRAFIE

App-Entwicklung unter Zeitdruck gefährdet die Sicherheit: Warum mobile Apps zum gefährlichen Einfallstor werden 46

Quantencomputer in fünf bis zehn Jahren breit verfügbar: Post-Quanten-Kryptografie wird zur Pflicht 54

REDAKTION

Editorial 3

Impressum / Inserenten 58

Titel: alexp / KI-generiert

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.

Trust Seal
www.teletrust.de/itsmig

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. 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.

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.

Die Verwendung des markenrechtlich geschütz ten TeleTrusT Vertrauenszeichens IT ecurit made in German wird interessierten An bietern durch TeleTrusT auf Antrag und bei rfüllung der nachstehenden Kriterien zeitlich befristet gestattet:

Der nternehmenshauptsitz muss in Deutschland sein

Das nternehmen muss vertrauenswürdige IT icherheitslösungen anbieten

Die angebotenen Produkte dürfen keine ver steckten ugänge ackdoors enthalten

Die IT icherheitsforschung und entwick lung des nternehmens muss in Deutsch land stattfinden.

5. Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Daten schutzrechtes zu genügen

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

TRÄGER DES VERTRAUENSZEICHENS (STAND 16.09.2026)

- 8com GmbH & Co. KG
- Accellence Technologies GmbH
- AceBIT GmbH
- achelos GmbH
- Achtwerk GmbH & Co. KG
- ACT DIGITAL Deutschland GmbH
- ads-tec Industrial IT GmbH
- agilimo Consulting GmbH
- AirID GmbH
- AI-Z GmbH
- Alphasolid IT GmbH
- Alpha Strike Labs GmbH
- AMPEG GmbH
- ANMATHO AG
- Anqa IT-Security GmbH
- Antago GmbH
- APRO Computer & Dienst-leistung GmbH
- APT GmbH
- ASOFTNET
- arcitects IT Security GmbH
- arnautdigital
- Athereon GRC GmbH
- ATIS systems GmbH
- AUCONET Solutions GmbH
- AUTHADA GmbH
- authenton GmbH
- AWARE7 GmbH
- axilaris GmbH
- Bare.ID GmbH
- BAYOOSOFT GmbH
- Bechtle GmbH & Co. KG
- Biteno GmbH
- blueteam GmbH
- Bosch CyberCompare
- Build38 GmbH
- Bundesdruckerei GmbH
- BRIGHTCYTE GmbH
- BvL.com GmbH
- CBA - Cybersecurity and Business Advisory GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- CERTIX IT-Security GmbH
- COGNITUM Software Team GmbH
- COMback Holding GmbH
- comcrypto GmbH

Fortsetzung auf der nächsten eite

TRÄGER DES VERTRAUENSZEICHENS "IT SECURITY MADE IN GERMANY"

- comforte AG
- comtime GmbH
- Condition-ALPHA Digital Broadcast Technology Consulting
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- Cybersense GmbH
- CycleSEC 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
- DFN-CERT Services GmbH
- Digital Recovery PHD GmbH
- digitronic computer-systeme GmbH
- digit solutions GmbH
- Dirk Losse Consulting
- ditis Systeme Niederlas-sung der JMV GmbH & Co.
- DriveLock SE
- D-Trust GmbH
- DTS Systeme GmbH
- eCom Service IT GmbH
- ecsec GmbH
- EgoMind GmbH
- enclaive GmbH
- EncryptoBox GmbH
- Enginsight GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- essentry GmbH
- evolutionQ GmbH
- Exploit Labs GmbH
- eyeDsec Information Security GmbH
- FAST LTA GmbH
- floragunn GmbH
- FP Digital Business Solutions GmbH
- FB Pro GmbH
- FZI Forschungszentrum Informatik
- Garancy AG
- GBS Europa GmbH
- G DATA CyberDefense AG
- Generation Secure GmbH
- genua GmbH
- gescheit.IT GmbH
- glacier ac GmbH
- GORISCON GmbH
- HDPnet GmbH
- HiScout GmbH
- HK2 Rechtsanwälte
- Host-On Service Provider GmbH
- i2solutions GmbH
- idgard GmbH
- if(is) - Institut für Internet-Sicherheit
- Infineon Technologies AG
- INFODAS GmbH
- Inlab Networks GmbH
- INNOSYSTEC GmbH
- innovaphone AG
- Inovetra GmbH
- Insentis GmbH
- INSYS icom GmbH
- intarsys GmbH
- intelliCard Labs GmbH
- iseco consulting GmbH
- isits AG International School of IT Security
- ISL Internet Sicherheits-lösungen GmbH
- ITConcepts PSO GmbH
- ITSG GmbH
- itWatch GmbH
- KaitoSec GmbH
- keepbit IT-SOLUTIONS GmbH
- keyONE GmbH
- KOBIL GmbH
- Kobra Infosec GmbH
- Kopiaconsulting GmbH
- Kroll Strategieberatung GmbH
- limes datentechnik® gmbh
- Linogate GmbH
- loyyal UG
- LocateRisk UG
- MACONIA 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
- MTG AG
- MTRIX GmbH
- Mühlbauer ID Services GmbH
- NCP engineering GmbH
- ndaal Gesellschaft für Sicherheit in der Informati-onstechnik mbH & Co KG
- NetComProtect
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- Nexis GRC GmbH
- Nextron Systems GmbH

(STAND 16.09.2026)

- nicos GmbH
- Nimbus Technologie-beratung GmbH
- OctoGate IT Security Systems GmbH
- ondeso GmbH
- ONEKEY GmbH
- oneconsult Germany AG
- OTARIS Interactive Services GmbH
- O&O Software GmbH
- P3KI GmbH
- pen.sec AG
- Pentaris Security GmbH
- Pently GmbH
- PFALZKOM GmbH
- PNL Technology GmbH
- PORTFORMANCE GmbH
- PRESENSE Technologies GmbH
- procilon GmbH
- ProLog GmbH
- PSW GROUP GmbH & Co. KG
- QGroup GmbH
- RapidResponse GmbH
- real-cis GmbH
- RedMimicry GmbH
- Reiner Kartengeräte GmbH und Co. KG
- Relution GmbH
- Robin Data GmbH
- Rohde & Schwarz Cybersecurity GmbH
- Rohde & Schwarz Networks and Cyber-security GmbH
- r-tec IT Security GmbH
- SAMA PARTNERS Business Solutions GmbH
- sayTEC AG
- SCHUTZWERK GmbH

Trust Seal
www.teletrust.de/itsmig

- Schwarz Cyber Techno-logies GmbH & Co. KG
- Secorvo Security Consulting GmbH
- secrypt GmbH
- SECUDOS GmbH
- SECUINFRA GmbH
- Seculution GmbH
- secunet Security Networks AG
- Secure Service Provision GmbH
- Securepoint GmbH
- Secuvise GmbH
- secuvera GmbH
- SEPPmail - Deutschland GmbH
- SerNet GmbH
- signotec GmbH
- Spike Reply GmbH
- SRC Security Research & Consulting GmbH
- Star Finanz GmbH
- Steganos Software GmbH
- suresecure GmbH
- SVA System Vertrieb Alexander GmbH
- syracom AG
- TDT AG

- TE-SYSTEMS GmbH
- Tech-Prax GmbH
- telent GmbH
- TG alpha GmbH
- Deutsche Cyberkom GmbH
- TÜV Informationstechnik GmbH
- TÜV Rheinland i-sec GmbH
- TÜV SÜD Akademie GmbH
- TWINSOFT biometrics GmbH & Co. KG
- Unosecur GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- VisionmaxX GmbH
- VMRay GmbH
- VORNAC GmbH
- water IT Security GmbH
- whitemacs GmbH
- XignSys GmbH
- XnetSolutions KG
- YARIX GmbH
- zeroBS GmbH
- Zertificon Solutions GmbH

Schluss mit Passwortschutz.
Sie haben die Kontrolle.

Passwörter allein reichen heute nicht mehr aus, um digitale Zugänge zuverlässig zu schützen. Mit **REINER SCT Login** sichern Sie die Windows-Anmeldung Ihrer Mitarbeitenden mit einer modernen Multi-Faktor-Authentifizierung und schaffen eine zusätzliche Schutzebene gegen unbefugte Zugriffe.

Passwörter allein reichen heute nicht mehr aus, um digitale Zugänge zuverlässig zu schützen. Mit **REINER SCT Login** sichern Sie die Windows-Anmeldung Ihrer Mitarbeitenden mit einer modernen Multi-Faktor-Authentifizierung und schaffen eine zusätzliche Schutzebene gegen unbefugte Zugriffe.

Statt sich ausschließlich auf ein Passwort zu verlassen, wird die Identität des Benutzers durch einen zusätzlichen Faktor abgesichert.

Dabei unterstützt REINER SCT Login eine **phishing-resistente Anmeldung** und trägt dazu bei, dass gestohlene oder abgegriffene Zugangsdaten allein nicht ausreichen, um auf geschützte Systeme zuzugreifen.

Besonders praktisch für Unternehmen: Die Anmeldesicherheit lässt sich **zentral verwalten**. So können Authentifizierungsverfahren und Zugriffsrechte strukturiert organisiert und an die Anforderungen Ihrer IT angepasst





werden. Mitarbeitende erhalten eine komfortable Möglichkeit, sich sicher an Windows-Arbeitsplätzen anzumelden – ohne dass Sicherheit zum Hindernis im Arbeitsalltag wird.

REINER SCT Login eignet sich damit für Unternehmen, die ihre klassische Passwortanmeldung um eine zeitgemäße Multi-Faktor-Authentifizierung ergänzen und ihre IT-Zugänge besser absichern möchten.

Mehr Sicherheit bei der Anmeldung. Mehr Kontrolle für die IT.

Entdecken Sie REINER SCT Login und erfahren Sie, wie Sie die Windows-Anmeldung in Ihrem Unternehmen sicherer und moderner gestalten können.

REINER SCT Login –
sichere Windows-Anmeldung mit Multi-Faktor-Authentifizierung.



EU-Kommission veröffentlicht CRA-Leitfaden

Um Unternehmen bei der praktischen Umsetzung des Cyberresilienz-gesetzes zu unterstützen, hat die EU-Kommission einen Leitfaden veröffentlicht. Für Kleinstunternehmen und KMU sollen zahlreiche Beispiele die Einhaltung erleichtern.

Von Ira Zahorski, IT-BUSINESS

Im Gesetzestext zum Cyber Resilience Act (CRA) wurde die EU-Kommission verpflichtet, einen Leitfaden zu erstellen, der die fristgerechte und klare Umsetzung erleichtern soll. Der Leitfaden wurde am 27. Juli 2026 veröffentlicht, ist aber rechtlich nicht bindend

Er kann Behörden und Unternehmen jedoch als Orientierungsgrundlage dienen und soll vor allem Kleinstunternehmen und KMU mit praktischen Beispielen, Diagrammen und Ent scheidungsbäumen zur ompliance Prüfung unterstützen

BERICHTERSTATTUNGSPFLICHT

Die erste Pflicht des Cyber Resilience Act (CRA), nämlich die Berichterstattungspflicht, gilt be reits ab 11. September 2026. Ab diesem Zeit punkt müssen ersteller von Produkten mit digitalen Elementen (Hardware und Software), aktiv ausgenutzte Schwachstellen und schwer



Bild: Dall-E / KI-generiert

wiegende icherheitsvorfälle innerhalb stren ger Fristen an Behörden melden. Routinefehler und gewöhnliche Patches fallen nicht darunter und verbleiben im täglichen chwachstellen management

Auch wenn das genaue Format und Verfahren für Meldungen und die harmonisierten or men die das chwachstellenmanagement un terstützen, voraussichtlich erst kurz vor eginn der Verpflichtung vorliegen werden, empfiehlt die Kommission, bereits etzt interne rken nungs und Meldeprozesse aufzubauen

1. **Führen Sie eine genaue SBOM** (Software Bill of Materials und halten ie diese aktuell, wenn sich Versionen ändern
2. **Kontinuierliche Überwachung:** Gleichen ie Ihre Komponenten mit bekannten chwach stellenquellen ab, damit eine aktiv ausge nutzte chwachstelle innerhalb von tunden und nicht Wochen erkannt wird
3. **Legen Sie den Prozess im Voraus fest:** Wer entscheidet, ob eine Meldung fällig ist? Wer verfasst sie? Wer reicht sie ein?
4. **Lückenlose Dokumentation:** Die Konformi tätsmatri ist das zentrale achweisdoku ment. Sie verknüpft die Meldung mit den übergeordneten chwachstellenmanage mentpflichten gemäß Anhang I des CRA, in den sie eingebettet ist.

Für die ersten beiden Tipps stellt die Kom mission online einen chwachstellenanal sator zur Verfügung https://www.cyberresilienceact.eu/de/analysis.html Dieser gleicht ede Kompo nente mit der National Vulnerability Database VD und der Vulnerabilit Database VD ab, kennzeichnet nd of Life Komponenten und ⇨

WAS IST DIE BERICHTERSTATTUNGSPFLICHT NACH DEM CRA?

Hersteller von Produkten mit digitalen Elementen (Hardware und Software) müssen ab dem 11. September 2026 sowohl aktiv ausgenutzte Schwachstellen als auch schwerwiegende Sicherheitsvorfälle melden, sobald sie davon Kenntnis erlangen. Die Meldepflicht ist damit eine fortlaufende, aktive Verpflichtung. Der Meldeprozess ist in drei Fristen unterteilt:

- **Frühwarnung:** Innerhalb von 24 Stunden muss eine erste Meldung erfolgen, dass ein Vorfall oder eine ausgenutzte Schwachstelle vorliegt.
- **Ausführliche Meldung:** Innerhalb von 72 Stunden müssen detailliertere Informationen zum Sachverhalt und eine erste Bewertung des Risikos gemeldet werden.
- **Abschlussbericht:** Spätestens 14 Tage nach Entdeckung einer Schwachstelle bzw. nach 1 Monat bei einem Vorfall muss der finale Bericht nach Bereitstellung einer Korrekturmaßnahme oder Behebung vorliegen.

Die Meldung muss an das zuständige nationale CSIRT (Computer Security Incident Response Team) des EU-Landes, in dem das Unternehmen seine Hauptniederlassung hat – in Deutschland: Bundesamt für Sicherheit in der Informationstechnik (BSI) bzw. CERT-Bund – übermittelt werden. Außerdem muss die Schwachstelle bzw. der Vorfall an die ENISA (Agentur der Europäischen Union für Cybersicherheit) gemeldet werden. Beides erfolgt über die zentrale CRA Single Reporting Platform (SRP). Stand heute ist die Plattform noch im Aufbau. Bis zum Inkrafttreten der Meldepflichten soll sie betriebsbereit sein. Bei Nichtbeachtung drohen hohe Bußgelder und der Verlust des Marktzugangs im EU-Binnenmarkt.

⇨ erstellt einen Konformitätsbericht, den erstel ler ihrer technischen Dokumentation beifügen können. Für die Konformitätsmatrix gibt es eine kostenlose Checkliste für Hersteller (https:// www.cyberresilienceact.eu/de/compliance-matrix. html

WAS ZÄHLT ALS PRODUKT?

Laut EU-Kommission gab es die meisten Fragen dazu, was genau als „Produkt" zählt. Daher beschäftigt sich auch der größte Teil des Leit fadens damit. Artikel 3(1) der EU-Verordnung (EU) 2024/2847 definiert ein Produkt mit digitalen Elementen als Software- oder Hard wareprodukt (einschließlich seiner Datenfern verarbeitung), dessen Nutzung eine direkte oder indirekte Datenverbindung einschließt. Eine Software, die auf dem Gerät des Nutzers ausgeführt wird, beispielsweise eine herunter geladene App, zählt dazu. Software, auf die nur über einen Browser aus der Ferne zugegriffen wird, nicht. Web-Apps und Websites fallen nur dann in den Anwendungsbereich, wenn sie als Datenfernverarbeitung gelten, die eine Produktfunktion unterstützt. Das bloße Teilen von Open-Source-Code in einem öffentlichen Repository stellt in der Regel kein „Inverkehr bringen" dar.

Hersteller können im CRA Fast Check prüfen, ob ihr Produkt in den CRA-Anwendungsbereich fällt und in welche Klasse es einzuordnen ist (https://www.cyberresilienceact.eu/de/fast-check. html

OPEN-SOURCE-SOFTWARE

Bei Open-Source-Software ist ausschlagge bend, ob sie im Rahmen einer kommerziellen Tätigkeit entwickelt wird und ob sie „in Verkehr gebracht" wird. Dazu zählt:

- Erhebung eines Preises
- Monetarisierung verbundener Dienste
- Verlangen personenbezogener Daten
- kostenpflichtiger Support
- Spenden
- Finanzierungsvereinbarungen
- gemeinnützige Strukturen
- Integration von FOSS (Free and Open-Source Software) durch andere Hersteller

WESENTLICHE ÄNDERUNGEN

Laut CRA gilt ein Produkt als wesentlich geän dert, wenn eine Änderung sein Cybersicher heits Risikoniveau in einer Weise verändert, die der Hersteller in seiner Risikobewertung noch nicht berücksichtigt hatte. Sicherheits-updates zählen in der Regel nicht dazu. Maß geblich sei die Auswirkung der Änderung auf das Cybersicherheitsrisikoprofil wie beispiels weise neue Bedrohungsvektoren, neue An griffsszenarien oder eine veränderte Eintritts wahrscheinlichkeit oder Auswirkung, nicht der Umfang der Änderung.

Wurde ein Produkt wesentlich geändert, gilt es als neu in Verkehr gebracht. Nimmt jemand anderes als der ursprüngliche Hersteller die Änderung vor, übernimmt diese Person die Herstellerpflichten für den geänderten Teil. Ein neues Inverkehrbringen verpflichtet den Her steller gesetzlich, die Konformität dieses Pro dukts nachzuweisen. Der Nachweis besteht aus der EU-Konformitätserklärung und der techni schen Dokumentation. Bei Erfüllung erhält das Produkt die CE-Kennzeichnung.

UNTERSTÜTZUNGSZEITRAUM

Fünf Jahre hat die EU als Untergrenze für den Zeitraum angesetzt, für den ein Produkt voraussichtlich in Gebrauch ist, es sei denn, das Produkt wird voraussichtlich kürzer genutzt. In diesem sogenannten Unterstützungszeitraum, gerechnet ab dem Zeitpunkt des Inverkehr bringens, müssen Schwachstellen behandelt werden

Das Enddatum der Nutzung ist zum Zeitpunkt des Kaufs anzugeben. Soweit technisch mach bar sind Nutzer bei Ablauf zu benachrichtigen.

Können Nutzer eine Software kostenlos und ohne zusätzliche Kosten aktualisieren, darf der Hersteller die Schwachstellen nur in der jeweils aktuellsten Version beheben.

Sollte das Produkt wesentlich verändert wor den sein, muss der Unterstützungszeitraum neu bewertet werden. Eine automatische Ver längerung oder Erneuerung schließt der Ge setzgeber aus.

Die EU-Kommission stellt einen Planer zur Verfügung, mit dem der Unterstützungszeit raum berechnet werden kann (https://www.cyberresilienceact.eu/de/support-planner.html).

PRODUKTKLASSEN: STANDARD, WICHTIG, KRITISCH

Produkte werden in Standard, Wichtig Klasse I, Wichtig Klasse II und Kritisch unterteilt. Dabei ist die Kernfunktion das entscheidende Krite rium; die Hauptmerkmale des Produkts, ohne die es seinen vorgesehenen Zweck nicht erfül len würde. Fällt ein Produkt in mehrere Katego rien, gilt die strengere Klasse.

S an ar Wird das Produkt weder in Anhang III noch in Anhang IV des Cyber Resilience Act genannt, gilt es als Standardprodukt und kann nach Modul A kontrolliert werden. Das heißt, der Hersteller darf die gesetzliche Kon formität (z. B. für die CE-Kennzeichnung) in Eigenverantwortung prüfen und erklären.

Wichtig Klasse I: Hierzu zählen Produkte, deren Schwachstelle viele andere Systeme beeinträchtigen kann. Sie sind in Anhang III, erste Gruppe, aufgelistet. Wenn eine europä ische Norm die CRA-Anforderungen abdeckt und der Hersteller sie vollständig anwendet, erklärt er die Konformität selbst. Ohne Norm prüft eine unabhängige, offiziell zugelassene und überwachte Prüforganisation die techni sche Dokumentation und Fertigungsprozesse.

Wichtig Klasse II: Ebenfalls in Anhang III, aber in der zweiten Gruppe, finden sich Produkte, die kritischer sind als Klasse I. Eine Schwach stelle im Produkt würde ganze kritische Infra strukturen oder viele nachgelagerte Systeme gefährden. Hier muss die Konformität immer über eine notifizierte Stelle erfolgen. Die Ver fügbarkeit der zuständigen Stellen können Hersteller im EU-Register NANDO tagesaktu ell prüfen.

Kritisch: In Anhang IV sind hochkritische Pro dukte gelistet, deren Ausfall kritische Dienste wie Energie- oder Wasserversorgung beein trächtigen würden.

Der Produktklassen-Check soll Herstellern die Einordnung erleichtern (https://www.cyberresilienceact.eu/de/classification.html).

DATENFERNVERARBEITUNG

Lösungen zur Datenfernverarbeitung sind nur dann Teil eines Produkts mit digitalen Ele menten, wenn sie für die Ausübung der Pro duktfunktionen erforderlich sind. Im Leitfaden findet sich ein Test, der die Grenze zwischen Produkt und Dienstleistung aufzeigt. □

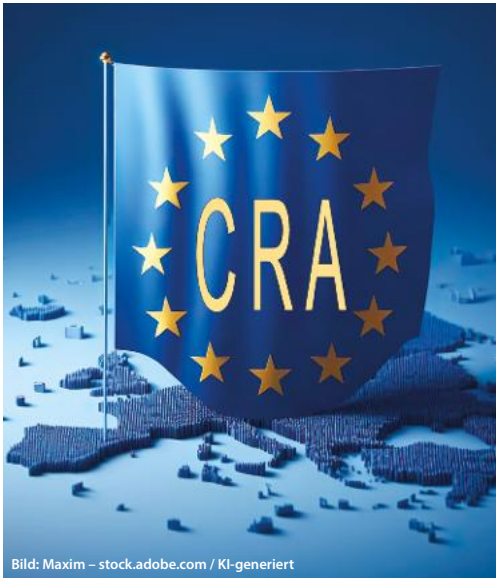


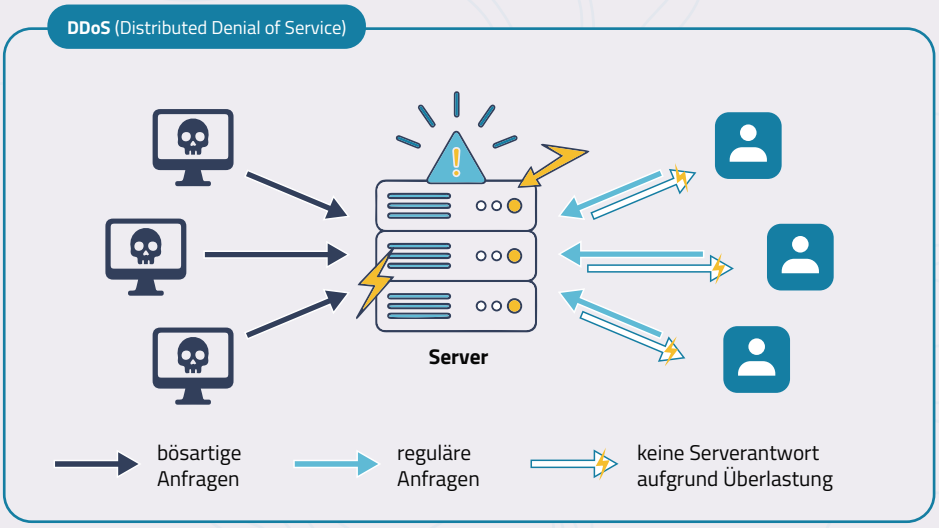
Bild: Maxim – stock.adobe.com / KI-generiert

PFALZKOM

Wenn die digitale Lebensader stillsteht

DDoS-Angriffe zielen auf das, was Unternehmen heute am dringendsten brauchen: **Verfügbarkeit**.

Websites, Kundenportale, APIs oder geschäftskritische Anwendungen können innerhalb kürzester Zeit durch eine Flut manipulierter Anfragen lahmgelegt werden. Klassische Firewalls reichen insbesondere bei komplexen Angriffen auf Anwendungsebene oft nicht mehr aus.



PFALZKOM DDoS Schutz erkennt schädlichen Datenverkehr und wehrt ihn automatisiert ab, während legitime Anfragen weiterhin ihr Ziel erreichen.

Als Security-as-a-Service lässt sich die Lösung ohne zusätzliche Hardware in bestehende IT-Infrastrukturen integrieren – vom Mittelstand bis zu KRITIS-Unternehmen.

Hier mehr erfahren

Digitale Souveränität beginnt mit Vertrauen

Unternehmen teilen immer größere Datenmengen mit Partnern und Cloud-Diensten oder nutzen sie für KI-Anwendungen und -Modelle. Damit wächst auch die Frage, **wer auf welche Daten zugreifen darf und wie sich das zuverlässig kontrollieren lässt.** Denn digitale Souveränität bedeutet nicht nur, Daten nutzen und teilen zu können, sondern auch dabei die Kontrolle zu behalten.

PFALZKOM

Gaia-X schafft dafür einen offenen und interoperablen Vertrauensrahmen für den souveränen Austausch von Daten. Eine zentrale Rolle übernehmen die Gaia-X Digital Clearing Houses (GXDCH). Sie prüfen Identitäten, Dienste und Infrastrukturen und ermöglichen damit eine sichere, digitale Zusammenarbeit.

PFALZKOM ist eines von derzeit nur drei akkreditierten Gaia-X Digital Clearing Houses in Deutschland. Damit sorgt das Unternehmen dafür, dass Identitäten und Zugriffsberechtigungen zuverlässig überprüft werden können.

Als neutrale Vertrauensinstanz prüft und bestätigt PFALZKOM die digitalen Identitäten von Organisationen, Personen und Maschinen, die an Datenräumen teilnehmen. Technologien wie **Decentralized Identifiers (DIDs)** und **Verifiable Credentials** ermöglichen dabei überprüfbare digitale Identitäten. Vereinfacht gesagt funktionieren sie wie digitale Reisepässe und fälschungssichere Nachweise: Nur wer eindeutig identifiziert und berechtigt ist, erhält Zugang zu Daten und Diensten.

Für Unternehmen stellt sich neben der Frage nach Zugriffsrechten eine weitere: **Wo liegen ihre Daten und über welche Infrastruktur werden sie verarbeitet?**

PFALZKOM verbindet seine Rolle im europäischen Gaia-X-Ökosystem deshalb mit eigener Infrastruktur. Das Unternehmen betreibt eigene Rechenzentren in der Metropolregion Rhein-Neckar und ein leistungsfähiges Glasfasernetz. Damit schafft PFALZKOM auch auf infrastruktureller Ebene die Voraussetzungen dafür, Daten im europäischen Rechts- und Wirtschaftsraum selbstbestimmt zu verarbeiten.

Wer digitale Souveränität will, muss deshalb beides im Blick haben: den kontrollierten Zugang zu Daten und die Infrastruktur, über die sie verarbeitet werden. ■

BMI veröffentlicht Referentenentwurf zur Umsetzung des CRA

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) kritisiert den aktuellen BMI-Entwurf zur Umsetzung des Cyber Resilience Act und fordert Nachbesserungen und eine klare Finanzierung. Dies sind die wichtigsten Punkte des Entwurfs.

Von Jürgen Paukner



Bild: UGoC stock.adobe.com / KI-generiert

Am 18. März 2026 hat das Bundesministerium des Innern (BMI) einen Gesetzesentwurf zur Durchführung der Verordnung (EU) 2024/2847 veröffentlicht. Das ist die offizielle Bezeichnung für den Cyber Resilience Act (CRA), der am 10. Dezember 2024 in Kraft trat. Während die EU-Verordnung unmittelbar in allen Mitgliedsstaaten gilt, gibt es einige Umsetzungsfristen, die den betroffenen Unternehmen Zeit geben, die Anforderungen umzusetzen. Mit dem Referentenentwurf kommt Deutschland seiner Pflicht nach, bestimmte nationale Regelungen zu treffen. Dazu gehören zum Beispiel die Benennung von Zuständigkeiten sowie Durchsetzungsbefugnissen.

DAS BEINHALTET DER BMI-REFERENTENENTWURF ZUM CRA

Der Referentenentwurf sieht einige Änderungen am Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG) vor, um den Cyber Resilience Act umzusetzen. Die wichtigsten Punkte des Referentenentwurfs sind:

Das I wird die zentrale Marktüberwachungsbehörde und notifizierende Behörde für Konformitätsbewertungsstellen Au er dem übernimmt das undesamt zusätzlich formal Aufgaben als IRT wie die ntgegennahme und earbeitung von Meldungen zu aktiv ausgenutzten Schwachstellen und si cherheitsrelevanten Vorfällen

- Der Entwurf legt fest, dass das BSI die notifizierende Behörde für Konformitätsbewertungsstellen wird. Die notifizierende Behörde prüft, ob eine Prüfstelle fachlich geeignet ist, und meldet sie bei der Kommission, da mit die Stelle offizielle Prüfbescheinigungen ausstellen darf In Ausnahmefällen kann das I selbst ewertungen vornehmen, wenn dies aus öffentlichem Interesse nötig ist.
- Das BSI soll betroffene Wirtschaftsakteure durch ensibilisierungs und chulungsmanahmen unterstützen und ein Reallabor für berresilienz einrichten und betreiben Dazu richtet das I eine eschwerdestelle ein, bei der Verbraucher inweise auf mögliche Verstö e einreichen können Der nt wurf prognostiziert einen dauerhaften Personalmehrbedarf beim I von insgesamt Planstellen bis 2029 und einmalige Kosten von etwa 10 Millionen Euro für das Reallabor. Für Verstö e gegen die Verordnung werden die Vorschriften des Gesetzes über Ordnungswidrigkeiten entsprechend angewendet, und die uständigkeiten für u geldverfahren werden national geregelt.

TELETRUST EMPFINDET ENTWURF ALS UNZUREICHEND

Wenige Wochen nach der Veröffentlichung des Referentenentwurfs hat TeleTrusT eine tellungnahme formuliert war greife der ntwurf die CRA-Regelungen im Grundsatz auf, bleibe jedoch in zentralen Punkten hinter den praktischen und rechtlichen Anforderungen zurück Die vorgesehene Aufgabenbündelung beim I ist nur dann tragfähig, wenn dessen personelle, technische und organisatorische Ausstattung verlässlich und dauerhaft abgesichert wird Daran fehlt es bislang , hei t es in der tellungnahme

Als besonders kritisch sieht der Verband die zu weit gefasste Ausnahmeregelung für die Notifizierung von Konformitätsbewertungsstellen ohne Akkreditierung, die unzureichend konkretisierten Unterstützungsleistungen für Wirtschaftsakteure sowie die unklare Ausgestaltung des Reallabors für berresilienz In allen drei Bereichen bestehe die Gefahr, dass der Entwurf formale Strukturen schaffe, ohne deren praktische Wirksamkeit belastbar sicher zustellen

Daher halte der TeleTrusT eine deutliche ach schärfung des ntwurfs für erforderlich ot wendig seien insbesondere eine verlässliche Finanzierung und Ausstattung des BSI und der deutschen Akkreditierungsstelle, enge und klare Voraussetzungen für Ausnahmen von der akkreditierungsbasierten Notifizierung, ein substantiell ausgebautes und praxisnahes Unterstützungskonzept für nternehmen sowie transparente und nachvollziehbare Regelungen zum Reallabor □

UMSETZUNGSFRISTEN DES CRA

Mit Inkrafttreten des CRA am 10. Dezember 2024 läuft eine Frist von drei Jahren. Ab dem 11. September 2026 gilt die Meldepflicht für aktiv ausgenutzte Schwachstellen und schwere Vorfälle. Ab 11. Dezember 2027 müssen alle CRA-Anforderungen erfüllt werden. In speziellen Fällen gibt es noch Übergangsfristen, die über dieses Datum hinausgehen. Darauf sollten Unternehmen sich aber besser nicht verlassen und bis zu den genannten Stichtagen ihre Prozesse und Produkte auf Vordermann gebracht haben.

Warum VPN und Zero Trust keine Gegensätze sind

Seit 40 Jahren steht NCP für hochsichere Kommunikation und technologische Weiterentwicklung. Mit unserem neuen Produkt gehen wir jetzt den nächsten Schritt: Wir verbinden moderne Zero Trust-Architekturen mit unserer bewährten VPN- und Remote Access-Technologie und schaffen damit eine souveräne deutsche Lösung für den sicheren Zugriff auf Anwendungen. Dabei verfolgen wir keinen radikalen Bruch mit bestehenden Technologien, sondern setzen auf deren gezielte Weiterentwicklung.

Die Diskussion um Zero Trust wird häufig mit der Frage verbunden, ob klassische VPN-Konzepte künftig ersetzt werden müssen. Diese Betrachtung greift zu kurz. Entscheidend ist nicht allein, wie eine Verbindung technisch hergestellt wird, sondern wie Zugriffe auf Anwendungen und Daten kontrolliert und abgesichert werden. VPN und Zero Trust sind deshalb keine Gegensätze, sondern können sich sinnvoll ergänzen.

Zero Trust bedeutet: Vertrauen wird nicht automatisch gewährt. Jeder Zugriff wird anhand von Identität, Kontext, Gerätezustand und Sicherheitsrichtlinien geprüft. Denn klassische Unternehmensgrenzen verschwimmen zunehmend – Mitarbeitende arbeiten flexibel, während Anwendungen in unterschiedlichen Umgebungen betrieben werden. Nutzer erhalten dabei nur Zugriff auf die Anwendungen, die sie tatsächlich benötigen.

ZERO TRUST ERSETZT VPN NICHT AUTOMATISCH

Zero Trust wird häufig als Gegenmodell zum VPN dargestellt. Bei einem klassischen VPN wird nach erfolgreicher Authentifizierung häufig ein Zugang zum gesamten Unternehmensnetzwerk hergestellt. Zero Trust verschiebt den Fokus dagegen hin zum gezielten Zugriff auf einzelne Anwendungen.

Das bedeutet jedoch nicht, dass bestehende VPN-Strukturen überflüssig werden. Gerade in gewachsenen IT-Landschaften sind VPN-Verbindungen weiterhin sinnvoll. Unternehmen können vorhandene Remote Access-Infrastrukturen als Ausgangspunkt



Bild: NCP

nutzen und schrittweise um Zero Trust-Mechanismen ergänzen.

WO ZERO TRUST DURCHGESETZT WIRD

Eine Zugriffsentscheidung allein schützt noch keine Anwendung. Sie muss technisch durchgesetzt werden. Hier kommen Enforcement-Komponenten ins Spiel.

Der Policy Decision Point (PDP) entscheidet, wer unter welchen Bedingungen auf eine bestimmte Anwendung zugreifen darf. Der Policy Enforcement Point (PEP) setzt diese Entscheidung technisch um. Er kann beispielsweise am Endpunkt, an einem Gateway oder unmittelbar vor einer Anwendung angesiedelt sein.

Entscheidend ist das Zusammenspiel: Eine erfolgreiche Authentifizierung bedeutet nicht automatisch uneingeschränkten Zugriff. Stattdessen wird anhand von Identität, Gerätezustand, Kontext und Sicherheitsrichtlinien entschieden, auf welche Anwendung tatsächlich zugegriffen werden darf.

VPN BEKOMMT EINE NEUE ROLLE

VPN kann weiterhin Bestandteil einer modernen Sicherheitsarchitektur sein. Es stellt eine geschützte Verbindung her, während Zero Trust den Zugriff regelt. Bestehende VPN-Gateways oder -Clients können mit weiteren Komponenten einer Zero Trust-Architektur zusammenspielen. Der VPN-Tunnel ist dann nicht zwangsläufig der Zugang zum gesamten Unternehmensnetzwerk, sondern kann Teil einer umfassenderen Zugriffskontrolle sein.

40 JAHRE ERFAHRUNG, BEREIT FÜR DIE ZUKUNFT

Mit unserem neuen Produkt bieten wir eine souveräne deutsche Zero Trust-Lösung, die moderne Zero Trust-Architekturen mit unserer bewährten VPN- und Remote Access-Technologie verbindet. Zugriffe werden dabei nicht pauschal gewährt, sondern abhängig von Identität, Berechtigungen und Risiko gezielt auf Anwendungen gesteuert.

Die vollständig softwarebasierte Lösung lässt sich On-Premises, in der Private Cloud, hybrid oder in der Cloud betreiben. Unternehmen können damit ihre bestehende Infrastruktur schrittweise migrieren und in die Zero Trust-Architektur überführen, ohne ihre Systeme zu einem festen Zeitpunkt vollständig ersetzen zu müssen. ■

Praxis-Check: Wie kann die neue Datenschutzaufsicht aussehen?

Auf politischer Ebene wird über eine Bündelung oder Zentralisierung der Datenschutzaufsicht in Deutschland diskutiert. Doch was hätte die Wirtschaft von solch einer Bündelung? Ein Praxis-Check zur laufenden Diskussion.

Von Dipl.-Phys. Oliver Schonschek

Weniger Bürokratie, beschleunigte Verfahren und effizientere staatliche Strukturen: Das ist das Ziel der Föderalen Modernisierungsagenda von Bund und Ländern. Dazu gehört auch eine Vereinfachung im Datenschutzrecht. Die Agenda besagt unter anderem: „Der Bund wird in Abstimmung mit den Ländern die Datenschutzaufsicht für den nichtöffentlichen Bereich bis spätestens 31.12.2027 reformieren und dabei gegebenenfalls auch die Aufgabenverteilung im Föderalstaat neu justieren."

Ziel ist demnach die Sicherstellung der einheitlichen Rechtsauslegung und -anwendung sowie eine Erhöhung der Effizienz im Zusammenspiel der Aufsichtsbehörden. Hierzu können insbesondere die Bündelung von Kompetenzen bei der Bundesdatenschutzbeauftragten (BfDI) oder Aufsichtsbehörden der Länder (beispielsweise durch Zuständigkeitskonzentration und/oder One-Stop-Shop-Regelungen), eine bessere Einbindung der DSK (Datenschutzkonferenz) und/oder die Einführung eines Kohärenzverfahrens unter Nutzung der Möglichkeiten des Art. 87 Abs. 3 GG auf Bundesebene oder im Wege von Staatsverträgen zwischen den Ländern gehören. Der Bund prüft zudem die Aufhebung der Pflicht zur Bestellung eines Landes datenschutzbeauftragten.

PLANUNGEN BETREFFEN DEN NICHTÖFFENTLICHEN BEREICH

Wenn über eine Bündelung oder Zentralisierung der Datenschutzaufsicht diskutiert wird, geht es um den nichtöffentlichen Bereich, also insbesondere um die Wirtschaft. Wie zum Beispiel die Wissenschaftlichen Dienste des Deutschen Bundestages erklärt haben, ist im öffentlichen Sektor eine vollständige Zentralisierung der Datenschutzaufsicht auf Bundesebene nicht möglich: Soweit Sachgebiete betroffen sind, für die das Grundgesetz den Ländern die Gesetzgebungskompetenz zuweist, fehlt dem Bund die Zuständigkeit für eine Regelung der Datenschutzaufsicht.

Anders sehen die Wissenschaftlichen Dienste es für den nichtöffentlichen Bereich: „Soweit die Aufsicht über die Verarbeitung personenbezogener Daten im privaten Sektor betroffen ist, begegnet eine Zentralisierung auf Bundesebene auch im Hinblick auf die innerstaatliche Kompetenzordnung des Grundgesetzes keine durchgreifenden rechtlichen Bedenken".

⇨

it-sa 2026
Messe Nürnberg
27.–29. Oktober
Halle 9 | Stand 424
Besuchen Sie uns!

genua.



Sicherheit, die Freiraum schafft.

VS-NfD-Kommunikation mobil, barrierefrei und leistungsstark.
Mit flexiblen, skalierbaren und BSI-zugelassenen Lösungen.
Made in Germany. Für Ihre digitale Souveränität.

Teil der Bundesdruckerei-Gruppe
bdr.

genua.de/
beh-sicher-mobil


Bild: ImageFlow – stock.adobe.com

ERWARTUNGEN DER WIRTSCHAFT AN EINE DATENSCHUTZAUFSICHT

mfragen wie die des Digitalverbands itkom zeigen regelmä ig, dass die nternehmen in Deutschland klare rwartungen an eine Auf sicht für den Datenschutz haben Prozent der nternehmen haben ilfestellungen der Aufsichtsbehörden genutzt oder angefragt Prozent Mit den ilfestellungen zu frieden waren zuletzt nur Prozent, so der itkom

ei einer anderen itkom mfrage berichten Prozent der befragten nternehmen von einer mangelnden eratung durch Aufsichts behörden, Prozent wünschen sich eine verpflichtende praxisnähere Beratung durch die Aufsichtsbehörden Die nternehmen plä dieren mit knapper Mehrheit dafür, die Daten schutzaufsicht auf undesebene zu zentralisie ren Prozent befürworten den Vorschlag, Prozent sind dagegen

Die Datenschutzaufsicht von RW wertet sol che mfragen so, dass die nternehmen die Aufsichtsbehörden für den Datenschutz brau chen, denn von den Datenschutzaufsichtsbe hörden wünscht sich eine deutliche Mehrzahl von Prozent mehr ilfestellung Dazu die Landesbeauftragte für Datenschutz und Infor mationsfreiheit in NRW, Bettina Gayk: „Der Wunsch ist verständlich Wir beraten bereits intensiv Aber angesichts der massiven unah me von eschwerden wegen Datenschutzver stö en, die in RW im vergangenen ahr um Prozent angewachsen sind, sto en unsere Kapazitäten leider an ihre Grenzen. Hier be nötige ich die Unterstützung von Landtag und Regierung, damit ich die hohe eschwerdelast und die Erwartung der Wirtschaft bedienen kann hne zusätzliches Personal ist das nicht leistbar

Mit lick auf die geplante ündelung der Auf sicht weist Bettina Gayk darauf hin, dass die itkom mfrage auch berlegungen der un desregierung konterkariert, die Datenschutz aufsicht über die nternehmen bei einer un desbehörde zu zentralisieren o sähen gerade einmal neun Prozent der efragten keine ach teile, sollten die Pläne Wirklichkeit werden ur Prozent glaubten daran, dass die nt scheidungsprozesse in einer undesbehörde schneller gehen, während dagegen Prozent Sorge hätten, die Nähe zu ihrer Aufsichtsbehör

it-sa 2026
Messe Nürnberg
27.–29. Oktober
Halle 9 | Stand 424
Besuchen Sie uns!

genua.



Geheimschutz to go.

Flexible, skalierbare Lösungen für VS-NfD-konformes mobiles Arbeiten. Einfach, barrierefrei und gesetzeskonform. Made in Germany. Für Ihre digitale Souveränität.

Teil der Bundesdruckerei-Gruppe
bdr.

genua.de/
sicher-mobil-gbi

de im Land und damit eine direkte Ansprech partnerin oder einen direkten Ansprechpart ner zu verlieren

STARKER WUNSCH NACH MEHR BERATUNG UND UNTERSTÜTZUNG

Wenn man die rwartungen und Wünsche aus der Wirtschaft betrachtet und erfüllen möch te, stellt sich die Frage, wie dies eine zentrale Datenschutzbehörde leisten kann, auch wenn die Bundesbeauftragte für die Bündelung der Aufsicht zur Verfügung steht.

Die Landesdatenschutzbehörden haben eige ne Vorschläge zur Modernisierung von Daten schutz und Aufsichtspraxis in den „Stuttgarter Impulsen“ eingebracht. Dort regen auch sie eine Veränderung der Aufsichtsstruktur an.

Der Landesbeauftragte für den Datenschutz in Rheinland-Pfalz, Prof. Dr. Dieter Kugelmann, stellt klar: „Auch die Datenschutzaufsichtsbe hörden der Länder treten für einen moder nen und zukunftsgewandten Datenschutz ein. Dieser lässt sich hervorragend im föderalen Rahmen verwirklichen Ausgangspunkt sei die konkrete Betrachtung der Realität in der Aufsicht. Davon ausgehend könnten zukunfts



Bild: sh99 – stock.adobe.com

feste Strukturen entwickelt werden, die im Gegensatz zu anderen öffentlich geäußerten Vorschlägen keine verfassungsrechtlichen oder europarechtlichen Risiken bergen würden.

Die Landesdatenschützer verweisen insbeson dere darauf, dass die Aufsichtsbehörden der Länder über detaillierte Kenntnisse regionaler wirtschaftlicher und gesellschaftlicher Struk turen sowie über gewachsene Netzwerke zu Unternehmen, insbesondere zu KMU, sowie Verbänden und Verwaltungen verfügen. Eine föderal gegliederte Datenschutzaufsicht er möglicht demnach passgenaue Beratung und praktikable Lösungen unter Einbeziehung lokaler esonderheiten und heterogener e dürfnisse.

Die Datenschutzbeauftragten der Länder warnen: „Zentralisierung mag Effizienz und Einheitlichkeit versprechen, sie birgt aber die Gefahr, regionale und wirtschaftliche Expertise aus den Ländern zu verdrängen. Die föderale Aufsichtsstruktur garantiert eine Datenschutz aufsicht mit Umsicht, die regionale Besonder heiten angemessen berücksichtigt.“

Wenn also die Wirtschaft nach mehr Beratung und Unterstützung durch die Datenschutzauf sicht verlangt, bedeutet dies einen Bedarf an passender Kompetenz, Erreichbarkeit und Per sonalstärke. Ob eine zentrale Behörde auf Bun desebene das leisten kann, sollte hinterfragt werden. Das zeigen auch die Umfragen unter den nternehmen, die zwar die Datenschutz aufsichtsbehörden in verschiedenen Punkten kritisieren, grundsätzlich aber mehr Unterstüt zung und eratung wollen

Eine neue Datenschutzaufsichtsstruktur mit Kompetenz-Clustern, zum Beispiel in Bereichen wie Künstliche Intelligenz, Plattformökonomie, Cloud-Infrastrukturen oder Wissenschaft und Forschung, könnte hier der richtige Weg sein. Statt Bündelung der Aufsicht wäre der Weg dann eine Spezialisierung der Aufsicht, bei gleichzeitiger Erreichbarkeit in der Fläche. □

Externe Admins, interner Kontrollverlust

Ein gekündigter IT-Dienstleister, ein leer wirkender Tenant, 50.000 neue Gastkonten – der vielleicht unbequemste Befund aus dem r-tec Lagebericht 2025 ist so simpel wie brisant: Viele Unternehmen schützen sich gegen Angreifer von außen und übersehen Risiken mit Schlüsselgewalt im eigenen Ökosystem.

Von Dr. Stefan Rummenhöller, r-tec IT Security

Wer glaubt, das eigene Unternehmen sei zu unauffällig für echte Angreifer, hat bisher nur Glück gehabt. Cyberkriminelle treffen nicht nach Branche oder Größe, sie treffen nach Gelegenheit. Lead Cybersecurity Expert Rüdiger Trost von WithSecure warnt im r-tec Cyber Security Lagebericht 2025 treffend, „[...] dass Unternehmen in Deutschland weiterhin im Fokus von Cyberkriminellen aus der ganzen Welt stehen. Wie groß ein Unternehmen ist oder in welcher Branche es agiert, spielt keine Rolle – jedes Netzwerk kann ein lohnendes Ziel sein“. Gleichzeitig wird es operativ enger. Mehr Systeme, mehr Abhängigkeiten, mehr Cloud. Und am Ende oft ein simples Problem: Rechte bleiben zu lange, zu breit, zu unkontrolliert.

EIN TENANT, DER PLÖTZLICH LEER WIRKT

Denn nicht jeder Sicherheitsvorfall beginnt mit Phishing, Malware oder einer Zero-Day-Sicherheitslücke. Manchmal beginnt er mit einer Kündigung. Genau das zeigt einer der eindrücklichsten Fälle aus dem Lagebericht: Am ⮑



Bild: sahanaj – stock.adobe.com

Tag nach einer konfliktbehafteten Trennung von einem IT-Dienstleister fiel einer Organisation auf, dass ihr Microsoft-Entra-Tenant auffällige Veränderungen zeigte. Produktive Benutzer und Betriebsdaten fehlten. Parallel war die Umgebung mit rund 50.000 Gastbenutzern geflutet. Auf Wunsch der Cyberversicherung wurde r-tec hinzugezogen.

Die Cloud-Forensik ergab einen sauberen Ablauf: Login über ein Konto aus dem Dienstleisterkontext, Registrierung einer Enterprise Application, Anlage eines weiteren Global Admin. Danach folgten Löschungen von Benutzern und Postfächern. Anschließend setzte eine automatisierte Erzeugung zufällig benannter Gastkonten ein. Die aktivierten Entra- und M365-Logging-Einstellungen ermöglichten eine weitgehend lückenlose Rekonstruktion, die Attribution blieb offen. Der Fall zeigt deutlich: Wenn Governance- und Offboarding-Prozesse nicht belastbar sind, können privilegierte Cloud-Berechtigungen schnell zu einem vollständigen Kontrollverlust führen.

WARUM DIENSTLEISTERZUGÄNGE EIN EIGENER RISIKOTYP SIND

Damit ist nicht gemeint, dass alle externen Admins böse Absichten haben. Doch sie stellen eine eigene Risikoklasse dar. Dienstleister brauchen weitreichende Rechte, tiefes Umgebungswissen und oft operative Freiheit. Diese Kombination macht sie unverzichtbar und zugleich hochkritisch. Bei Zeitdruck, Kommunikationslücken oder auch Streit entstehen potenzielle Risiken, die Unternehmen unbedingt auf dem Radar haben sollten.

Der r-tec Lagebericht 2025 formuliert es unmissverständlich: „Dienstleisterkonten sind Hochrisiko-Identitäten und müssen, wie eigene Assets behandelt werden. [...] Offboarding muss technisch durchgesetzt werden und darf nicht von Tickets oder Goodwill abhängen." Für einen Kontrollverlust wie im Beispielfall braucht es kein spektakuläres Angriffswerkzeug. Es reichen wenige privilegierte Aktionen zur falschen Zeit mit den richtigen Rechten. Genau deshalb liegt der Wert dieses Falls nicht allein in seiner Dramatik, sondern in seiner Nüchternheit. Er zeigt, wie schnell Governance-Versäumnisse zu einem operativen Ausnahmezustand werden. Multi-Faktor-Authentisierung (MFA) allein genügt hier nicht. Denn erfolgreiche MFA kann auch bedeuten, dass ein legitimer Pfad missbraucht wurde. Was daraus folgt, ist unbequem: Kritische Admin-Aktionen sind Hochrisiko-Vorgänge und müssen auch als solche betrachtet werden. Dafür braucht es klare Auslöser für Alarmierung, verbindliche Playbooks und eine definierte Reaktion – nicht erst in der Nachbereitung, sondern unmittelbar bei der Ausführung.

123 KRITISCHE VORFÄLLE ZEIGEN EINE ANGESPANNTE SICHERHEITSLAGE

Der Fall mit dem gekündigten Dienstleister ist kein Einzelfall, sondern ein Brennglas für eine insgesamt härtere Lage. r-tec hat im Cyber Security Lagebericht Erkenntnisse aus 123 besonders kritischen Cybersicherheitsvorfällen zusammengeführt. Insgesamt ist die Zahl der Sicherheitsvorfälle gegenüber dem Vorjahr um 53,8 Prozent angestiegen. Parallel dazu wurden über zweimal so viele Geräte im EDR-Monitoring erfasst wie im Jahr zuvor, von 24.330 auf 60.000. Das tägliche SIEM-Logvolumen wuchs um 97,5 Prozent. Schon diese drei Zahlen erzählen eine klare Geschichte: mehr Fläche, mehr Signale, mehr Druck, mehr Komplexität. Hinzu kommt der reale Aufwand in der Reaktion. Das r-tec CERT verzeichnete 2.505 Stunden Vorfallsaufwand im Jahr 2025, davon 1.643 Stunden bei Nicht-Servicekunden und 862 Stunden bei Servicekunden. Die längste Bearbeitungsdauer lag bei 450 Stunden für Nicht-Servicekunden und bei 46 Stunden für

ervicekunden Auch das ist mehr als eine Kennzahlensammlung s ist ein inweis darauf, wie teuer fehlende Vorbereitung in der Pra is wird. Wer im Ernstfall erst Zuständigkeiten, Kommunikationswege und technische Grund lagen sortieren muss, verliert nicht nur Zeit, sondern vor allem die hance, einen Vorfall früh klein zu halten

READINESS IST KEIN ZUSATZ, SONDERN DIE EIGENTLICHE SICHERHEITSFRAGE

Der Lagebericht 2025 bündelt Einsätze aus dem ber Defense enter, verdichtet sie in kura tierte Fälle und leitet praxisrelevante Learnings ab. Ziel ist, Organisationen zu helfen, Wider standsfähigkeit aufzubauen, bevor der nächste Vorfall den Alltag übernimmt Dazu beschreibt der ericht keine abstrakten Trends, sondern reale Einsatzmuster. Das Spektrum reicht von Ransomware über Malvertising und ClickFix bis zu OT-Vorfällen, Supply-Chain-Fragen und Business-E-Mail-Compromise. Auffällig ist da bei, dass nicht nur technische chwachstellen eine Rolle spielen. Betriebliche Brüche wie unklare Zuständigkeiten, fehlende Playbooks, lückenhafte Transparenz oder ungenügend gesteuerte Identitäten sind ein grundlegendes Problem

Gute Sicherheitsarbeit beginnt nicht im Mo ment des Angriffs. Sie beginnt vorher: bei kla ren Rollen, belastbarem Offboarding, sauber getrennten Admin-Konten, regelmäßigen Re views privilegierter Identitäten, vollständigen Audit-Logs und getesteten Reaktionspfaden. Unternehmen, die diese Grundlagen nicht gesetzt haben, werden im Ernstfall nicht nur langsamer: Sie verlieren zuerst Übersicht und dann Kontrolle Auch reichen einzelne, silo artig betriebene Security-Lösungen längst nicht mehr aus chutz wird erst dann wirksam, wenn mehrere Ebenen als Gesamtsystem zu sammenspielen.

PRAXISWISSEN AUS REALEN SICHERHEITSVORFÄLLEN NUTZEN

Daher steht auch der Vorfall rund um den Miss brauch privilegierter Zugänge exemplarisch für das, was der ericht in seiner ganzen reite zeigt: Sicherheitsvorfälle entstehen heute sel ten nur durch eine einzelne technische Schwä che ie entstehen dort, wo Rechte, Prozesse, Transparenz und Reaktionsfähigkeit nicht sau ber zusammenspielen.

Zudem bietet der Lagebericht viele weitere Er kenntnisse zur aktuellen bersicherheitslage und einen Mehrwert, der in vielen Diskussio nen oft zu kurz kommt: echte Einsatzpraxis, klar verdichtet und direkt anschlussfähig für bessere Entscheidungen in Prävention, Detek tion und Reaktion. Denn wer aus realen Vor fällen lernt, muss den nächsten nicht erst erle ben, um ins andeln zu kommen □



Bild: r-tec

ÜBER DEN AUTOR

Dr. Stefan Rummenhöller gründete r-tec vor rund drei Jahrzehnten und entwickelte das Unternehmen zu einem Anbieter für Cybersecurity in Deutschland. Am 31. Juli 2026 übergab er die Geschäftsführung und verließ den Wuppertaler IT-Sicherheitsspezialisten.

Mehr Umsatz für den Channel mit IT-Sicherheit „Made in Germany“

Cybersecurity ist für Systemhäuser und Managed Service Provider ein wichtiges Geschäftsfeld. Doch nicht jeder Partner kann oder will dafür ein eigenes Security Operations Center aufbauen und rund um die Uhr betreiben. G DATA CyberDefense setzt daher auf ein flexibles Modell: Mit XDR und MXDR erhalten Systemhäuser und MSPs den Service „Angriffserkennung und Reaktion“ aus Deutschland. Sie entscheiden dabei selbst, wie viel sie bei ihren Kunden selbst leisten.

G DATA CyberDefense

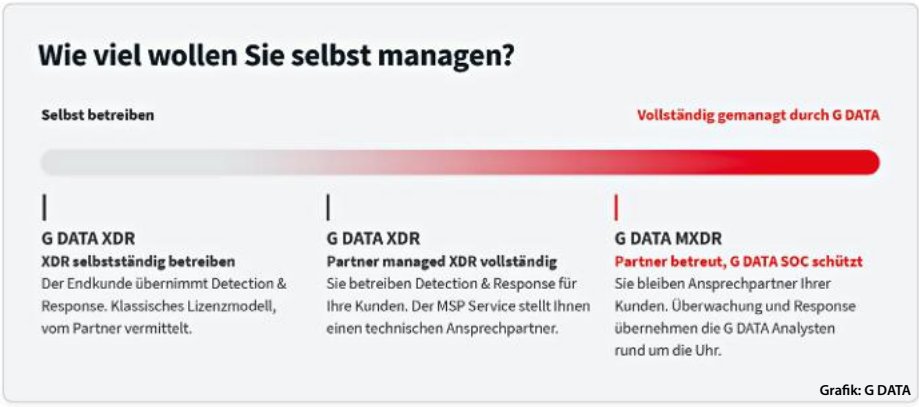
Angesichts einer komplexen und verschärften Bedrohungslage sind Unternehmen darauf angewiesen, Cyberangriffe frühzeitig zu entdecken und im Ernstfall sofort richtig zu reagieren. Für Systemhäuser, Reseller und MSPs eröffnet das neue Geschäftsmöglichkeiten: Sie können ihr Portfolio um Detection-and-Response-Services erweitern und ihre Kunden umfassend und effektiv absichern. G DATA CyberDefense bietet dafür mit XDR und Managed XDR (MXDR) zwei aufeinander aufbauende Modelle an. Der Partner entscheidet dabei selbst, welche Aufgaben er übernimmt und wo er auf Unterstützung zurückgreift.

XDR: SECURITY SELBST MANAGEN

G DATA XDR (Extended Detection and Response) richtet sich an Partner und Kunden, die Angriffserkennung und Reaktion selbst leisten. Neben dem klassischen Lizenzmodell für Endkunden gibt es eine speziell auf Managed Service Provider zugeschnittene Variante: MSPs verwalten die IT-Sicherheit ihrer Kunden zentral und integrieren Security-Leistungen in ihr eigenes Serviceportfolio. Dabei bleiben sie technisch nicht auf sich allein gestellt. Zum Angebot gehört der persönliche Service, der beim Einsatz der Lösung unterstützt. Das erleichtert insbesondere Dienstleistern die Arbeit, die ihr Security-Geschäft ausbauen und gleichzeitig auf die Expertise des Herstellers zurückgreifen möchten.

MXDR: MANAGED SECURITY OHNE EIGENES SOC

Wer seinen Kunden Managed Security anbietet, aber weder die personellen Ressourcen noch eine eigene 24/7-Bereitschaft aufbauen kann, setzt auf G DATA Managed Extended Detection and Response (MXDR). Bei der vollständig gemanagten Variante



Grafik: G DATA

überwacht das Analystenteam des Cyber-Defense-Spezialisten die Systeme rund um die Uhr, bewertet verdächtige Aktivitäten und reagiert umgehend im Angriffsfall.

Partner bieten mit G DATA MXDR umfassende Managed-Security-Leistungen an, ohne selbst ein Security Operations Center (SOC) zu betreiben und dauerhaft Security-Spezialisten für Schichtdienste vorzuhalten. Gleichzeitig entstehen neue Möglichkeiten für wiederkehrende Umsätze und langfristige Kundenbeziehungen.

G DATA XDR und G DATA MXDR sind dabei kein „entweder oder“: Ein Partner kann beispielsweise mit XDR starten, eigene Detection-and-Response-Kompetenzen aufbauen und später auf MXDR wechseln. Damit entsteht ein Wachstumsmodell, das sich flexibel an Geschäftsmodell, Ressourcen und Security-Know-how des Systemhauses anpasst.

„MADE IN GERMANY“ ALS TÜRÖFFNER

Neben Technik und Service ist für Unternehmen entscheidend, wem sie ihre Security-Infrastruktur und sensible Daten anvertrauen. Hier ist „IT-Sicherheit Made in Germany“ das Verkaufsargument: G DATA entwickelt seine Security-Technologien in Deutschland. Auch das Analysten- und das Service-Team sind am Bochumer Unternehmenssitz angesiedelt. Datenschutz und DSGVO-Konformität gehören damit ebenso zum Angebot wie technologische Expertise.

Gerade bei mittelständischen Unternehmen und öffentlichen Auftraggebern ist dies ein wichtiger Türöffner. Für den Channel verbindet G DATA damit technische Leistungsfähigkeit mit einem Vertrauens- und Souveränitätsargument. Systemhäuser und MSPs bieten Detection und Response aus Deutschland an und bestimmen dabei ihr Geschäftsmodell: von XDR in Eigenregie bis zum vollständig gemanagten MXDR-Service. „IT-Sicherheit Made in Germany“ wird somit zur Grundlage für neue Security-Services, wiederkehrende Umsätze und langfristiges Wachstum im Channel. ■

Erfahren Sie mehr über G DATA MXDR unter: www.gdata.de/mxdr

Cloud-Abhängigkeit als KRITIS-Risiko – Revival der Datensicherung vor Ort

Der „Bitkom Cloud Report 2026" zeigt eine wachsende Kluft zwischen Cloud-Nutzung und Souveränitätsanspruch. Für KRITIS-Betreiber verschärfen neue gesetzliche Vorgaben den Druck, Datenkontrolle, Resilienz und unabhängige Backup-Strategien jenseits der Public Cloud neu zu denken.

Von Roland Stritt, FAST LTA

Eine aktuelle Bitkom-Befragung von 603 Un ternehmen bringt es auf den Punkt: 85 Prozent der deutschen nternehmen halten Deutsch land für zu abhängig von loud Anbietern 95 Prozent nennen Vertrauen in IT-Sicherheit, Datenschutz und ompliance als Must have Kriterium bei der Providerwahl nd Prozent fordern Schutz vor unbefugtem Zugriff, auch durch den loud Anbieter selbst Diese ig nale treffen auf eine konkrete regulatorische Realität: Das KRITIS-Dachgesetz verpflichtet Betreiber kritischer Infrastrukturen zu Risiko



Bild: prehistorik – stock.adobe.com

analysen, dokumentierten Resilienz-Plänen und nachweisbaren Schutzmaßnahmen. Wer Backup, Archivierung und Notfallwiederherstellung bislang als nachrangig behandelt hat, steht unter Erklärungsdruck.

Für CIOs und CISOs in kritischen Infrastrukturen stellt sich damit eine Frage, die der Bitkom Cloud Report 2026 schärfer formuliert als jede Compliance-Broschüre: Wie souverän ist Ihre Infrastruktur wirklich?

Das KRITIS-Dachgesetz setzt die EU-CER-Richtlinie in deutsches Recht um und erweitert den Schutzrahmen für kritische Anlagen. Der Fokus liegt auf physischer Resilienz: Zugangskontrollen, Krisenreaktionspläne, Schutz vor physischen Angriffen und Sabotage. Das Gesetz verpflichtet Betreiber unter anderem zu...

- redundanten Systemen für Daten und Betrieb,
- Meldepflichten bei Vorfällen gegenüber dem BBK (binnen 24 Stunden),
- Risikoanalysen und dokumentierten Resilienzplänen,
- nachweisbarer Resilienz gegenüber physischen und digitalen Bedrohungen.

Ergänzend dazu greift NIS-2 mit Anforderungen an die IT-Sicherheit, darunter Maßnahmen zur Angriffserkennung. Beide Regelwerke wirken für KRITIS-Betreiber parallel und verstärken sich gegenseitig.

IT-SICHERHEIT ALLEIN REICHT NICHT

Der Cloud-Report von Bitkom Research berichtet: 75 Prozent der Cloud-nutzenden Unternehmen geben an, mit der Cloud primär die IT-Sicherheit erhöhen zu wollen. Das ist eine deutliche Steigerung um 18 Prozentpunkte gegenüber 2024. Der Impuls ist verständlich, die Umsetzung birgt jedoch einen strukturellen Widerspruch, den der Report selbst benennt.

Bei der Auswahl von Cloud-Providern nennen 87 Prozent der Unternehmen den Schutz vor unbefugtem Zugriff des Cloud-Anbieters selbst als Must-have-Kriterium. Wer also die Sicherheit erhöhen will, indem er Daten in die Cloud verlagert, erwartet gleichzeitig, dass der Anbieter keinen unkontrollierten Zugriff auf diese Daten hat. Das ist ein Ziel, das viele Public-Cloud-Verträge strukturell nicht erfüllen können.

DIE SOUVERÄNITÄTSLÜCKE: WUNSCH UND REALITÄT KLAFFEN WEIT AUSEINANDER

71 Prozent der befragten Unternehmen nutzen aktuell Cloud-Dienste von Anbietern aus den USA. Bevorzugen würden diesen Ansatz nur acht Prozent. Umgekehrt: 91 Prozent würden deutsche Cloud-Anbieter bevorzugen, tatsächlich genutzt werden sie von 53 Prozent.

Diese Lücke ist kein Nischenproblem. 85 Prozent der Unternehmen halten Deutschland für zu abhängig von US-Anbietern. 80 Prozent fordern deutsche oder europäische Hyperscaler. Und 64 Prozent der Cloud-Nutzer sagen, die aktuelle US-Politik zwingt sie, ihre Cloud-Strategie zu überdenken (im Vorjahr waren es 50 Prozent).

Für KRITIS-Betreiber kommt eine weitere Dimension hinzu: Gemäß KRITIS-DachG und NIS-2 müssen Sicherheitsmaßnahmen nachweisbar wirksam und souverän kontrollierbar sein. Die Frage, ob ein US-Anbieter im Zweifelsfall weisungsgebunden gegenüber US-Behörden agiert, ist keine theoretische.

LOCK-IN ALS OPERATIVES RISIKO

Das größte Hindernis beim Cloud-Provider-Wechsel sind Lock-in-Effekte: 59 Prozent der Unternehmen nennen sie als zentrale Wechselbarriere, verursacht durch schwierige Datenexporte, Migrationskomplexität oder proprietäre Formate. 45 Prozent nennen zu hohen personellen Aufwand und Anwendungskomplexität, 28 Prozent sehen ein zu hohes Risiko.

⇨

VS-Fitness als Eintrittskarte in den Verteidigungsmarkt

Steigende Verteidigungsbudgets und beschleunigte Beschaffungsprogramme öffnen den Markt für deutlich mehr Unternehmen als noch vor wenigen Jahren. Bundeswehr und Generalunternehmer vergeben Aufträge heute tiefer in die Lieferkette hinein. Damit ergeben sich neue Chancen für Zulieferer, Softwarehäuser und Technologieanbieter. Wer an entsprechenden Projekten teilnehmen will, muss jedoch mehr mitbringen als technische Leistungsfähigkeit. Der sichere Umgang mit Verschlusssachen wird zunehmend zur Voraussetzung.

infodas
connect more. be secure.

NEUE CHANCEN, NEUE ANFORDERUNGEN

Bundeswehr und Generalunternehmer binden heute verstärkt Tier-1- und Tier-2-Lieferanten ein. Darunter fallen längst nicht nur klassische Wehrtechnikunternehmen. Auch Maschinenbau, Sensorik und Elektronik, Automotive, Software, KI und Defense-Tech stoßen auf Ausschreibungen, die den Umgang mit Verschlusssachen voraussetzen. KRITIS-Betreiber und BOS (Behörden und Organisationen mit Sicherheitsaufgaben) sehen sich vergleichbaren Anforderungen gegenüber. Für viele Anbieter bedeutet das erstmals, Informationen des Grades VS-NfD (VS nur für den Dienstgebrauch) rechtssicher verarbeiten zu müssen. Fehlt diese Fähigkeit, scheitert die Teilnahme bereits an formalen Anforderungen.

GEHEIMSCHUTZ FOLGT EIGENEN REGELN

Viele Organisationen kennen Informationssicherheit aus ISO-Normen und Auditverfahren. Im Geheimschutz gelten jedoch andere Grundlagen. Maßgeblich sind u. a. das Sicherheitsüberprüfungsgesetz, die Verschlusssachenanweisung und das Geheimschutzhandbuch. Als Ansprechpartner fungiert zudem eine zuständige Behörde statt einer klassischen Zertifizierungsstelle. Parallel treffen viele Unternehmen Anforderungen aus NIS2, CRA und Geheimschutz. Wer diese Themen getrennt bearbeitet, schafft doppelte Prozesse und redundante Dokumentation.

ZEIT WIRD ZUM KRITISCHEN FAKTOR

Behördliche Verfahren, organisatorische Veränderungen und Sicherheitsüberprüfungen benötigen Vorlauf. Gleichzeitig deckt die klassische IT-Security-Beratung dieses Spezialgebiet nur begrenzt ab. Wer erst mit einer konkreten Ausschreibung beginnt, gerät deshalb schnell unter Zeitdruck.

VON DER ANALYSE ZUR VS-FÄHIGEN ORGANISATION

Ein Readiness Assessment von infodas zeigt, wo organisatorische und technische Lücken bestehen. Daraus entsteht eine priorisierte Roadmap mit konkreten Maßnahmen.

Die Beratung bezieht auch die technische Umsetzung ein. Ziel ist eine VS-konforme IT, die dem jeweiligen Schutzbedarf entspricht. Je nach Schutzbedarf erfordert das separierte Umgebungen, zugelassene IT-Systeme und kontrollierte Übergänge zwischen Sicherheitsdomänen. Cross-Domain Solutions ermöglichen dabei den kontrollierten Austausch sensibler Informationen.


Bild: infodas

BESTEHENDE STRUKTUREN WEITER NUTZEN

infodas verbindet produktneutrale Beratung mit langjähriger Erfahrung aus Projekten bei Bund, Ländern und Streitkräften. Als BSI-zertifizierter IT-Sicherheitsdienstleister betrachtet infodas organisatorische und technische Anforderungen gemeinsam. Vorhandene ISMS-Strukturen lassen sich gezielt weiter nutzen. Das reduziert Parallelprozesse und vermeidet Investitionen in Lösungen, die später keine Zulassung erhalten.

EIN TYPISCHER ANWENDUNGSFALL AUS DER PRAXIS

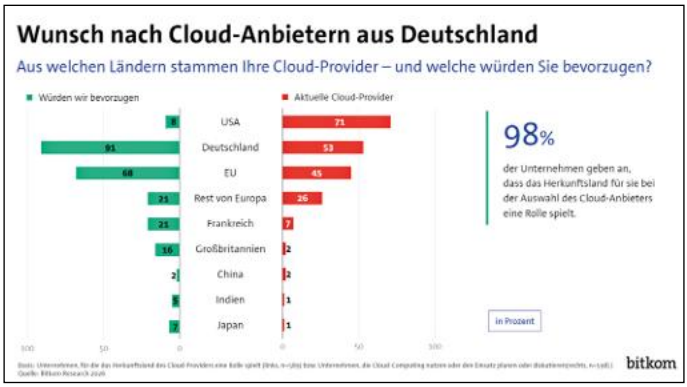
Wie VS-Fitness konkret aussehen kann, zeigt das Beispiel eines mittelständischen Elektronikzulieferers. Für einen Tier-1-Partner soll der Zulieferer eine Baugruppe entwickeln. Voraussetzung ist VS-NfD-Fähigkeit bereits in der Angebotsphase. Das Unternehmen ist nach ISO 27001 zertifiziert, verfügt aber weder über eine Geheimschutzorganisation noch über getrennte Entwicklungsumgebungen.

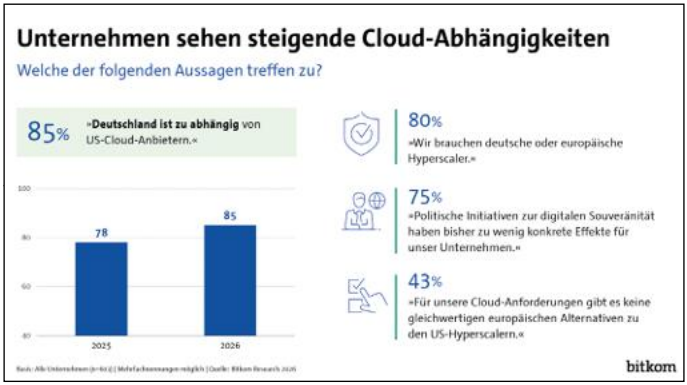
Das Assessment identifiziert Lücken bei Rollen, personellem Geheimschutz und IT-Trennung. Die Umsetzung umfasst eine dedizierte VS-NfD-Umgebung, einen kontrollierten Datenaustausch über ein zugelassenes Gateway sowie die notwendige Dokumentation auf Basis bestehender ISMS-Prozesse. So erreicht der Zulieferer die Angebotsfähigkeit, ohne die gesamte IT-Landschaft neu aufzubauen.

VS-FITNESS WIRD ZUM MARKTZUGANGSKRITERIUM

VS-Fitness ist eine Unternehmensfähigkeit. Wer die organisatorischen, personellen und technischen Grundlagen frühzeitig schafft, reagiert schneller auf Ausschreibungen, vermeidet formale Hürden und verschafft sich damit einen Vorsprung in einem Markt, der auf sicherheitsgeprüfte Partner angewiesen ist.

Mehr zum Thema: https://www.infodas.com/de/loesungen/geheimschutz/ ■





Grafiken: Bitkom Research

➥ Für KRITI etreiber ist ein solches Lock in nicht nur ein wirtschaftliches Problem. Es ist ein Resilienzproblem. Wer bei einem Ausfall oder einer regulatorischen nderung nicht handlungsfähig wechseln kann, hat keine echte Infrastruktursouveränität.

CLOUD-KOSTEN: KALKULATION WIRD SCHWIERIGER

64 Prozent der Cloud-nutzenden Unterneh men berichten, dass ihre Betriebskosten 2025 gestiegen sind. Für 2026 erwarten 54 Prozent erneut steigende Ausgaben. Der Report hält fest: „Schwer kalkulierbare Kosten können ein Grund dafür sein, dass Un ternehmen nicht sämtliche IT-Anwendungen in die Cloud verlagern."

Für KRITIS-Betreiber mit Haushalts- und Planungs pflichten ist Kalkulierbarkeit kein Nice-to-have. Sie ist eine Anforderung.

WAS EIN CLOUD-AUSFALL KOSTET

Bitkom Research hat gefragt, wie lange Unternehmen ohne Cloud-Zugang über haupt arbeitsfähig bleiben. Das Ergebnis: Knapp die Hälf te der Unternehmen käme irgendwann zum Stillstand, ein kleiner Teil sofort.

Das ist keine Worst-case-Spekulation. 28 Prozent der Cloud-Nutzer hatten in den vergangenen zwölf Monaten bereits einen gravierenden Ausfall erlebt. Was das be deutet, lässt sich beziffern: Branchenstudien (Gartner, ITIC) setzen IT-Ausfallkosten für mittelgroße und große Unternehmen bei mehreren hunderttausend Euro pro Stunde an. 41 Prozent der Großunternehmen berichten laut ITIC von Verlusten zwischen einer und fünf Millionen Euro pro Ausfallstunde. Für KRITIS-Betreiber kommen Meldepflichten, Behörden verfahren und Reputationsschäden hinzu, die in keiner Stundenkalkulation auftauchen.

Bemerkenswert ist, was Unternehmen daraus gezogen haben: Drei Viertel sichern wichtige Daten bereits außerhalb der Cloud. Zwei Drittel haben Notfall- und Wiederanlaufpläne. Mehr als die Hälfte kann einen lokalen Notbetrieb starten. Das ist kein Argument gegen die Cloud.

Es ist ein Argument dafür, dass kritische Daten und Betriebsfähigkeit nicht ausschließlich von ihr abhängen dürfen. Für KRITIS-Betreiber ist das keine Empfehlung, sondern regulatorische Grundlage: Das KRITIS-DachG fordert genau diese Redundanz und Wiederherstellungsfähigkeit, unabhängig vom Primärsystem.

WAS DAS FÜR DIE INFRASTRUKTUR BEDEUTET

Der Cloud-Report beschreibt ein Spannungsfeld, das sich nicht durch einen weiteren Cloud-Vertrag auflösen lässt. Die Antwort liegt in einer Infrastrukturentscheidung: Was muss vollständig unter Ihrer Kontrolle bleiben? Für Datensicherung, Langzeitarchivierung und Notfallwiederherstellung gibt es eine klare Antwort: On-Premises, unveränderlich, ohne externe Abhängigkeit. Im Fokus stehen dabei drei Begriffe:

er S rage bezeichnet eine Speicherarchitektur, bei der Daten ohne Ausnahme integer, vollständig und wiederherstellbar gespeichert werden. Das setzt voraus: keine stillen Bit-Fehler, nachweisliche Integrität, definierte Recovery-Zeiten und kein Single Point of Failure. Es ist kein Marketing-Begriff. Es ist eine Eigenschaft, die sich in der Infrastruktur entweder nachweisen lässt oder nicht.

ir a bezeichnet die physische oder logische Trennung eines Speichersystems vom Netzwerk und vom Internet. Ein echter Air-Gap verhindert, dass Ransomware, Malware oder unbefugte Zugriffe das Backup-Ziel erreichen. Er ist die wirksamste bekannte Maßnahme gegen Backup-Verschlüsselung durch Ransomware, vorausgesetzt er ist strukturell verankert und nicht nur konfigurierbar.

O M ri e On e ea Man bezeichnet unveränderliche Datenspeicherung: Einmal geschrieben, kann ein Datensatz nicht überschrieben, gelöscht oder manipuliert werden. Für KRITIS-Betreiber ist WORM eine Voraussetzung für revisionssichere Archivierung nach NIS-2, DORA, BSI-Grundschutz und branchenspezifischen Anforderungen wie § 291a SGB V (Gesundheitswesen) oder den Anforderungen der BaFin (Finanzsektor).

DATENSOUVERÄNITÄT, KOSTENKLARHEIT UND ANBIETER-UNABHÄNGIGKEIT

Der „Bitkom Cloud Report 2026“ liefert keine neuen Argumente gegen die Cloud. Er liefert belastbare Zahlen dafür, dass Datensouveränität, Kostenklarheit und Anbieterunabhängigkeit für deutsche Unternehmen und KRITIS-Betreiber zunehmend strategische Priorität haben. Wunsch und Wirklichkeit liegen dabei noch weit auseinander.

Das KRITIS-Dachgesetz ist in Kraft, die NIS-2-Meldepflicht steht an. Die Frage ist nicht, ob deutsche Unternehmen auf Cloud verzichten müssen. Die Frage ist, ob ihre Backup- und Archivierungsinfrastruktur den Anforderungen an Souveränität, Unveränderlichkeit und nachweisliche Resilienz standhält. □



Bild: FAST LTA

ÜBER DEN AUTOR

Roland Stritt ist CRO bei FAST LTA in München.

Continuous Compliance: Wenn Sicherheit verlässlich wirkt

Was eine Tür mit einem Zugriffsrecht gemeinsam hat

Eine Tür, die sich nicht öffnet, obwohl sie sollte, ist lästig. Eine Tür, die sich öffnet, obwohl das längst nicht mehr so sein sollte, birgt ein Risiko. Dasselbe gilt digital: Zugriff nur, solange er benötigt wird.

BAYOOSOFT

Physisch drückt sich das über Zonenkonzepte aus, digital über Rollen und Berechtigungen. Der Zugriff bleibt oft bestehen, selbst wenn das Projekt abgeschlossen ist, die Kollegin die Abteilung gewechselt hat oder ein ehemaliger Mitarbeiter das Unternehmen verlassen hat.

Solche Rechte werden selten aktiv entzogen, insbesondere wenn sie kopiert wurden, um Zeit zu sparen. Über die Jahre hinweg sammeln sich Berechtigungen an, die niemand mehr benötigt. Sicherheitsfachleute bezeichnen diesen Fall als Access Creep.

Seit Inkrafttreten des NIS-2-Umsetzungsgesetzes ist dieser Umgang mit Berechtigungen nicht mehr ausreichend: Sicherheitsvorkehrungen müssen nicht nur vorhanden sein, sondern auch nachweislich wirken. Laut Anhang zu NIS-2, Punkt 11.1, sind Konzepte für die logische und physische Kontrolle des Zugangs erforderlich. Betroffene müssen sich innerhalb weniger Monate beim BSI registrieren und Sicherheitsvorfälle innerhalb von 24 Stunden melden. Wer das versäumt, riskiert nicht nur Bußgelder, sondern auch das Vertrauen von Kunden und Partnern.

VOM PRÜFEN ZUM DAUERHAFTEN WIRKEN

Hier kommt das Konzept der Continuous Compliance ins Spiel: Statt einmal jährlich zu prüfen, werden Berechtigungen dauerhaft implementiert, kontrolliert, angepasst und dokumentiert. Sowohl beim physischen Zutritt als auch beim digitalen. Bei Projektende oder Abteilungswechsel werden nicht mehr benötigte Rechte automatisch entzogen. So werden Anforderungen nicht nur formuliert, sondern fortlaufend überwacht und bei Abweichungen automatisch korrigiert.

WENN RECHTE SICH SELBST KORRIGIEREN

Was wäre, wenn solche Lücken gar nicht erst entstehen? GRC-Tools bilden Risiken und Anforderungen zuverlässig ab, bleiben



aber meist auf der Management-Ebene. Sind aber Änderungen am operativen Prozess erforderlich, finden diese losgelöst vom Anforderungsmapping statt und die Verbindung zwischen Anforderung und Realität reißt ab.

Das ist die Idee von Compliance Execution: Governance, Identity und Security setzen Anforderungen um und halten sie dauerhaft konsistent.

Auf der Governance-Ebene beginnt das: Eine eQMS-nahe Lösung wie BAYOOSOFT Themis verlinkt Anforderungen, Prozesse, Risiken und Nachweise in einer gemeinsamen Datenbasis (Single Source of Truth) statt sie in mehreren Kopien parallel zu pflegen. Ändert sich ein verlinkter Baustein, zum Beispiel die zugrundeliegende Anforderung oder der konkrete Prozess, erkennt die integrierte Impact-Based Requalification, welche Abhängigkeiten ebenfalls überprüft werden müssen, und schickt sie zurück in den Review-Status.

Auf der Identity-Ebene setzt sich das fort: Genau das Muster aus dem Eingangsbeispiel wird im Access Manager durch das Zusammenspiel aus Rollenprofilen, automatisierten Start- und Enddaten und periodischen Access Reviews verhindert. Zusammengehalten wird es durch Reconciliation & Auto-Remediation: Diese führt eine kontinuierliche Überprüfung der Berechtigungen im Vergleich zum Soll-Zustand durch und nimmt automatische Korrekturen von Abweichungen vor.

Auf der Security-Ebene schließt sich der Kreis: Gpg4o schützt die vertraulichste Kommunikation per E-Mail Ende-zu-Ende.

FAZIT: ZUTRITT GEWÄHREN IST DIE LEICHTE ÜBUNG

Regulatorische Anforderungen lassen sich so nicht nur im Audit belegen, sondern sind fortlaufend gesichert. Der alte Laufwerkszugriff der Kollegin, der Account des ehemaligen Mitarbeiters und die unverschlüsselte E-Mail kurz vor Feierabend: Genau solche Dinge soll Continuous Compliance verhindern, bevor sie entstehen. Entscheidend ist nicht, ob eine Tür einmal überprüft wurde, sondern dass sie nicht unbeabsichtigt für Angreifer offensteht. ■

Identity Access Management: Darum profitiert der Channel

Passwörter auf Zetteln, vergessene Zugänge ehemaliger Mitarbeiter, täglich 119 neue Schwachstellen. Die aktuelle Sicherheitslage verzeiht keine veralteten Konzepte dieser Art. Der wachsende IAM-Markt bringt dem Channel jetzt neue Geschäftschancen.

Von Natalie Forell, IT-BUSINESS

Durchschnittlich 119 neue Schwachstellen täglich: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zeichnet ein besorgniserregendes Bild der deutschen IT-Sicherheitslage im Lagebericht 2025. Bei fast jeder zehnten Anfrage an das BSI-Service-Center geht es um Account-Missbrauch und Identitätsdiebstahl (9,5 %). Der zweithäufigste Grund, warum ein Unternehmen beim Bundesamt um Hilfe anfragt, sind Phishing-Angriffe.

Dabei wissen Unternehmen laut dem BSI-Lagebericht durchaus, was sie zu tun haben. Im Schnitt kennen sie die grundlegenden Schutzmaßnahmen: sichere Passwörter, Zwei-Faktor-Authentifizierung (2FA), Passwortmanager im Browser, passwortloses Anmelden und eigenständiger Passwortmanager. Zu den häufigsten umgesetzten Maßnahmen zählen sichere Passwörter (54 %), 2FA (44 %) und der Passwortmanager im Browser (29 %). Ob es nun die geopolitische oder regulatorische Lage ist: Viele Unternehmen warten auf den letzten Moment, der sie zu neuen Maßnahmen zwingt. Elmar Eperiesi-Beck, CEO der deutschen IAM-Plattform Bare.ID, rät, „sich frühzeitig mit der Einhaltung solcher Vorgaben zu befassen, um dann nicht in Zeitdruck zu geraten“. Ein wichtiger Punkt ist also frühzeitige Resilienz.



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

ES FEHLT DIE UMSETZUNG

Die Kluft zwischen Wissen und Umsetzung ist groß und kann vielen Unternehmen zukünftig zum Verhängnis werden. Dienstleister haben jetzt die Möglichkeit, neben Beratung auch direkt bei der Umsetzung zu unterstützen. Dazu gehört auch, die Technik auf dem aktuellen Stand zu halten. Ein Beispiel: Der Handwerker von nebenan speichert die Kundendaten in der Cloud und geht damit einen Schritt in Richtung Modernisierung. Beim Thema Sicherheit endet es aber. Jeder Mitarbeiter hat eigene Passwör

ter, die auf Zetteln notiert sind; die Zugänge der ehemaligen Mitarbeiter sind nicht geschlossen, und der Azubi hat die gleiche Dateneinsicht wie der Geschäftsführer.
Verschärft wird das Problem durch KI. Kriminelle nutzen Künstliche Intelligenz, um gestohlene Passwörter systematisch zu testen, schwache Zugangsdaten zu knacken oder mit gefälschten Stimmen Mitarbeiter zu täuschen. Was früher Wochen dauerte, schaffen KI-Tools heute in Stunden.

GEOPOLITIK BEEINFLUSST IT-SICHERHEIT

Eine Antwort darauf ist Identity Access Management (IAM). Diese Systeme wissen nicht nur, wer sich anmeldet, sondern prüfen bei Anmeldungen kontinuierlich, ob das Verhalten normal ist. Die verschärfte Bedrohungslage, sowohl durch Cyberangriffe als auch durch geopolitische Spannungen, führt dazu, dass Unternehmen ihre Software-Strategie überdenken, erklärt Eperiesi-Beck. „Wir erhalten täglich Berichte über Entwicklungen in den USA, Russland oder anderen Regionen. Dadurch entsteht eine neue, deutlich komplexere Bedrohungslage. Das führt zwangsläufig dazu, dass Unternehmen ihre bestehenden Softwarelösungen kritisch überprüfen und neu bewerten."
In diesem Kontext gewinnt das Thema „Digitale Souveränität" bei Technologieentscheidungen zunehmend an Bedeutung. Wichtig ist dabei jedoch eine klare Definition, da sie die Grundlage für eine glaubwürdige und nachhaltige Umsetzung bildet. Eperiesi-Beck sieht hier eine problematische Entwicklung: „Wir beobachten aktuell ein Sovereignty-Washing, bei dem digitale Souveränität eher ein Marketingversprechen als eine tatsächliche Umsetzung ist. Für mich beginnt echte Digitale Souveränität mit einer klaren Definition zweier Mindestanforderungen: eine vollständig deutschen Lieferkette und kein Vendor-Lock-in."

MODERNE ZUGANGSKONTROLLEN SIND GEFRAGT

Die Auseinandersetzung mit diesen Fragen führt in vielen Organisationen zu einer ernüchternden Erkenntnis über die bestehende IT-Landschaft. „Viele Unternehmen verfügen noch über veraltete Identity-Access-Management-Systeme", so der Experte. Beispielsweise wurde das Active Directory von Microsoft eingeführt und „über die Jahre hinweg einfach weiterbetrieben und mitgeführt". Dabei fehle es oft an Übersicht und Kontrolle. Moderne IAM-Systeme sollen helfen, mit dem Chaos aufzuräumen. Sie erkennen automatisch ungewöhnliche Anmeldungen, dokumentieren alle Berechtigungen transparent, und statt Passwörtern auf Zettel gibt es Single Sign-On (SSO). „Häufig wird angenommen, dass zusätzliche Sicherheitsmaßnahmen Unternehmen schaden. Tatsächlich ist jedoch das Gegenteil der Fall. Wie die Vergangenheit zeigt, stellen sie einen erheblichen Wettbewerbsvorteil dar."
Hinzu kommt ein weiterer struktureller Wandel: Unternehmen müssen heute weit mehr Identitäten verwalten als nur die ihrer eigenen Mitarbeitenden. „Die meisten Kunden beginnen mit Business-to-Employee-Szenarien, also der klassischen Mitarbeiter-Authentifizierung. Dieses Modell lässt sich anschließend auf Lieferanten oder Endkunden ausweiten."

PROJEKTE FÜR JEDE UNTERNEHMENSGRÖSSE

Identitätsmanagement gibt es für jede Unternehmensgröße und jedes Budget. Die Lösungen reichen von Microsoft Entra ID bis zu europäischen Alternativen wie Bare.ID. Für IT-Dienstleister bedeutet das neue Geschäftschancen, wobei Projekte hier von Drei-Tages-Migrationen bis hin zu Systemen mit Millionen Nutzern reichen können. Der Markt wächst – und mit ihm die Chancen für Dienstleister, Kunden bei der Digitalisierung zu unterstützen. □

Die Meldepflicht scheitert selten am Prozess

Ein kommunaler Versorger bemerkt an einem Donnerstagmorgen, dass ein Server in der Leittechnik ungewöhnlich viel Verkehr nach außen erzeugt. Ab diesem Moment läuft eine Frist. § 32 BSIG verlangt binnen 24 Stunden eine frühe Erstmeldung an die gemeinsame Meldestelle von BSI und BBK. Lückenhaft darf sie sein. Nach 72 Stunden wird es jedoch ernst. Dann erwartet der Gesetzgeber eine erste Bewertung samt Schweregrad und möglichen Auswirkungen, einen Monat später dann noch eine Abschlussmeldung.

An dieser zweiten Stufe zeigt sich, ob ein Betreiber wirklich meldefähig ist. „Wir wurden angegriffen“ hält die Frist ein, erfüllt sie allerdings nicht. Ohne Angaben dazu, welche Systeme betroffen waren und ob Daten das Netz verlassen haben, bleibt die Meldung formal fristgerecht, inhaltlich hingegen leer. Das hat Folgen, denn spätestens im Nachweisverfahren nach § 39 BSIG muss derselbe Betreiber erklären, warum seine Angaben so dünn ausfielen.

Der Grund liegt fast nie im Meldeprozess. Er liegt in den Daten. In gewachsenen OT-Umgebungen arbeiten Komponenten ohne verwertbare Protokollierung. Was protokolliert wird, verändert ein Angreifer mit Administrationsrechten nachträglich. Netzbasierte Erkennung hält das BSI deshalb für besonders relevant, weil eine mitgelesene Kopie des Datenverkehrs schwerer zu manipulieren ist als der Eintrag auf dem betroffenen System.

Am dünnsten ist die Datenlage dort, wo keine Leitstelle steht. In seiner Empfehlung CS 153 vom März 2025 hält das BSI fest, dass dezentrale Anlagen wie Umspannwerke oft unzureichend in das zentrale Monitoring eingebunden sind. Für Pumpwerke und Übergabestationen gilt derselbe Befund. Im Ernstfall beginnt dort die Rekonstruktion des Vorfalls, ohne dass Material vorliegt.

DIE AUFSICHT RÜCKT NÄHER AN DEN BETRIEB

Betreiber kritischer Anlagen setzen seit Mai 2023 Systeme zur Angriffserkennung ein, heute verankert in § 31 BSIG. Die Orientierungshilfe des BSI führt die Protokollierung darin als eigenen Anforderungsbereich, noch vor der eigentlichen Erkennung. Der dort erreichte Umsetzungsgrad wandert in den Nachweis an die Aufsicht. Seit der BSIG-Novelle wird dieser Nachweis alle drei Jahre statt wie bisher alle zwei fällig. Zwischen zwei externen Prüfungen liegt also ein Jahr mehr Eigenverantwortung.

Der Regierungsentwurf eines Gesetzes zur Stärkung der Cybersicherheit, seit Juni im

Bundestag in Beratung, geht noch weiter. Für kritische Anlagen ist eine automatisierte Ausleitung von Verfügbarkeitsindikatoren und von Informationen aus der Angriffserkennung an das BSI vorgesehen. Ausgeleitet werden kann allerdings nur, was vorher irgendwo erfasst wurde.

ERKENNUNG IM SCHALTSCHRANK STATT IM RECHENZENTRUM

An diesem Punkt setzt die Zusammenarbeit von consistec und ADS-TEC Industrial IT an. Das in Saarbrücken entwickelte Angriffserkennungssystem caplon© liest den Netzwerkverkehr passiv mit und meldet Abweichungen vom eingelernten Normalbild, ohne auf den Prozess zurückzuwirken. Seit der Partnerschaft läuft es als Docker-Container direkt auf den Industrial Router Firewalls der IRF-Serie, die ADS-TEC in Nürtingen entwickelt und die ohnehin im Schaltschrank sitzen. Ein Außenstandort bekommt damit eine Erfassung, ohne dass dafür ein eigenes Gerät samt Klimatisierung Platz finden muss. Für die Melde- und Nachweisführung verschiebt das die Ausgangslage. Aufgezeichnet wird dann auch an Stationen, die bisher nur ihren Betriebszustand an die Leitstelle gemeldet haben. Die Bewertung nach 72 Stunden stützt sich damit auf Verkehrsdaten. Der Umsetzungsgrad im Nachweis bildet über die Zentrale hinaus auch den verteilten Bestand ab.

Dass die Sensorik an solchen Standorten selbst zum Angriffsziel werden kann, gab für consistec bei der Partnerwahl den Ausschlag. ADS-TEC entwickelt die Firmware seiner Geräte selbst. Eingerichtet wird eine solche Erfassung im laufenden Betrieb, samt ausreichend Zeit für den Abgleich mit der Anlagendokumentation. Nach dem Alarm steht diese Zeit nicht mehr zur Verfügung. ■



Simon Göggel, Produktmanager bei ADS-TEC Industrial IT



Dr.-Ing. Thomas Sinnwell, geschäftsführender Gesellschafter bei consistec

Digitale Identität für KI-Agenten: Gibt es da nicht auch was von eIDAS 2.0?

Mit der EUDI-Wallet bekommt Europa eine Antwort auf eine sehr alte Frage: Wer bist du, und kannst du das beweisen? Bürgerinnen und Bürger, Behörden, Unternehmen – für sie alle schafft eIDAS 2.0 einen verlässlichen Rahmen für digitale Identität und Vertrauensdienste. Aber was geschieht, wenn nicht mehr der Mensch selbst handelt, sondern eine Software in seinem Auftrag?

Von Dr. André Kudra, TeleTrusT

KI-Agenten, die Bestellungen auslösen, Ver träge vorbereiten, Zugriffe anfordern oder mit anderen stemen verhandeln, sind keine u kunftsmusik mehr, sondern laufende Pilotpro jekte im B2B-Umfeld. Ein Beispiel: Ein Einkaufs-agent eines mittelständischen Unternehmens erkennt einen drohenden Lagerengpass, sucht automatisiert einen Lieferanten in einem ande ren EU-Land, handelt Konditionen aus und löst die Bestellung selbstständig aus. Klingt nach sinnvoller Automatisierung – wirft aber sofort die Frage auf: Handelt hier tatsächlich befugt jemand im Namen des Unternehmens?

eIDAS 2.0 und die EUDI-Wallet sind dafür kon zipiert, dass eine natürliche oder juristische Person sich selbst gegenüber Dritten ausweisen und Berechtigungen nachweisen kann. Das ist die richtige Antwort auf die richtige Frage – so lange am anderen Ende ein Mensch sitzt, der eine Wallet bedient. Sobald jedoch ein Agent selbstständig im Namen eines Auftraggebers handelt, verschiebt sich das Problem: Es geht nicht mehr nur darum, wer eine Person ist, son dern darum, wer in ihrem Namen handeln darf.

DREI FRAGEN, DIE SICH BEI JEDEM KI-AGENTEN NEU STELLEN

Wer sich dem Thema strukturiert nähert, lan det regelmä ig bei drei Fragen

Identität: Welcher Agent handelt hier eigent lich – und ist das eindeutig feststellbar? Inner halb einer einzelnen technischen Domäne lässt sich das mit etablierten IdP-/IAM-Lösungen heute meist gut lösen. Domänenübergreifend, etwa zwischen den stemen von nterneh men und Lieferant, entstehen erste Discovery-tandards sie klären aber nur, welcher Agent sich meldet, nicht, ob ihm zu trauen ist. Diese Frage lässt sich nicht auf der Identitätsebene beantworten: Vertrauen entsteht erst darüber, wer für einen Agenten bürgt und ihn autorisiert hat.

Mandat: Wer hat diesen Agenten wozu autori siert? Diese Frage zerfällt in mehrere Teilprob leme: die technische Berechtigung im jeweili gen System, die Kette der Delegation (hat der Mensch den Agenten beauftragt – oder der Agent einen weiteren Agenten , den Wider ruf einer einmal erteilten Berechtigung – und,

besonders anspruchsvoll, die grenzüberschrei tend rechtswirksame Bevollmächtigung. Durfte der inkaufsagent im eispiel tatsächlich einen Vertrag mit indungswirkung in einem anderen Rechtsraum eingehen? in technisch sauber si gniertes Token ist nicht automatisch ein Man dat, das vor Gericht in einer anderen Rechts ordnung Bestand hat. Welches technische Format sich durchsetzt, ist dabei offen – ob Verifiable Credentials, signierte Verträge oder andere strukturierte b ekte, wie sie etwa im mfeld von ahlungsprotokollen wie AP dis kutiert werden.

a h ei ier lohnt eine weitere nterschei dung. Zum einen die Durchsetzung zur Laufzeit: Darf dieser Agent jetzt, in diesem Moment, diese eine Aktion ausführen? Zum anderen die nachträgliche Beweiswerterhaltung: Kann Monate oder Jahre später noch belastbar re konstruiert werden, dass die Aktion damals befugt war? Im eIDAS-Rahmen existieren mit qualifizierten Zeitstempeln und etablierten Verfahren zur eweiswerterhaltung bereits belastbare austeine für genau diese Art von Langzeit-Nachweis – auf Agenten-Handlungen angewandt werden sie bislang aber kaum.

Marktbeobachtungen der vergangenen Mona te zeichnen ein konsistentes Bild: Identität lässt sich innerhalb einer Domäne bereits gut abbil den, an einzelnen Stellen auch das technische Mandat. Die grenzüberschreitend rechtswirk same Mandatskette dagegen bleibt in nahezu allen betrachteten Ansätzen unadressiert.

WARUM DAS JETZT ZÄHLT, NICHT ERST MORGEN

Der Impuls kommt dabei nicht in erster Linie aus der Regulierung. Unternehmen setzen KI-Agenten bereits heute in Einkauf, Beschaffung und internen Prozessen pilothaft ein – die praktischen Fragen nach Identität, Mandat und Nachweis entstehen also aus der Adoption he raus, zumal die EU die verbindlichen Pflichten für Hochrisiko-KI-Systeme selbst gerade auf 2027 beziehungsweise 2028 verschoben hat. Das verschafft der Branche Zeit, tragfähige Ant worten zu entwickeln, bevor der regulatorische Druck steigt – Zeit, die genutzt werden sollte.

EIN THEMA FÜR DEN FACHLICHEN AUSTAUSCH

Genau hier setzt TeleTrusT an: In den Arbeits gremien zu Digitaler Identität und Vertrauens diensten sowie in der TeleTrusT-AG „Cyber-Nation“ wird die Frage, wie sich Identität und Mandat für autonome Systeme sauber ab bilden lassen, bereits diskutiert. In bester „IT Security made in Germany“-Manier bringen sich TeleTrusT-Mitglieder mit passenden Bau steinen aus ihrem Portfolio ein und tauschen sich darüber aus, wie sich diese zu belastbaren Antworten zusammenfügen lassen. Wer sich in diese Diskussion einbringen möchte, ist herz lich eingeladen und kann sich an die Geschäfts stelle des Verbandes in Berlin wenden. □



Bild: TeleTrusT

ÜBER DEN AUTOR

Dr. André Kudra ist TeleTrusT-Vorstand mit Fokus auf Digitale Identität und Digitale Souveränität, CIO esatus AG.

Was kostet Sie Ihre Microsoft-Abhängigkeit?

Microsoft ist für viele Unternehmen unverzichtbar. Doch wer Daten, Zusammenarbeit und Sicherheitsfunktionen immer enger an einen Anbieter bindet, macht auch seine Handlungsfähigkeit von dessen Plattform- und Cloud-Strategie abhängig. Wie viel Wahlfreiheit wollen Sie behalten?

Informationssicherheit wird zum Geschäftsfaktor

Kunden und Lieferketten stellen konkrete Anforderungen an den Schutz sensibler Informationen. Standards wie ISO 27001, TISAX oder BSI IT-Grundschutz greifen Schutzbedarf und Klassifizierung ausdrücklich auf. Wer nicht nachvollziehbar darlegen kann, wie vertrauliche Informationen erkannt und geschützt werden, riskiert Rückfragen in Audits oder Nachteile in Ausschreibungen.

Der öffentliche Sektor zeigt, wie konkret der Umbau bereits ist: Schleswig-Holstein hat LibreOffice zum verbindlichen Standard für die Landesverwaltung gemacht und Exchange/Outlook durch Open-Source-Lösungen ersetzt. Ziel ist mehr digitale Souveränität und weniger Herstellerabhängigkeit.

Wenn Komfort zur Abhängigkeit wird

Office- und Collaboration-Plattformen bündeln immer mehr Funktionen: Dokumentenerstellung, Kommunikation, Speicherung, Klassifizierung, Schutzmechanismen und zunehmend KI. Das ist komfortabel – erschwert aber den späteren Wechsel.

Wer Klassifizierung und Sicherheitsrichtlinien eng an eine Plattform koppelt, bindet einen Teil seiner Informationssicherheitsarchitektur an denselben Hersteller. Die Managementfrage lautet deshalb nicht „Microsoft oder kein Microsoft?“, sondern: Welche Entscheidungen können Sie morgen noch selbst treffen?

Unternehmen, die Abhängigkeiten reduzieren, alternative Office-Umgebungen prüfen oder sensible Bereiche außerhalb großer Cloud-Plattformen betreiben wollen, brauchen Sicherheitsmechanismen, die diesen Handlungsspielraum erhalten.

Was ist Informationsklassifizierung?

Informationsklassifizierung ordnet Informationen nach ihrem Schutzbedarf ein – etwa als „öffentlich“, „intern“, „vertraulich“ oder „streng vertraulich“. Daraus entstehen Regeln: Wer darf eine Information sehen? Darf sie das Unternehmen verlassen? Muss sie verschlüsselt werden? So werden organisatorische Vorgaben zu technischen Schutzmaßnahmen.

M&H IT-Security

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

Die Klassifizierung gehört zum Dokument – nicht zur Office-Suite

Eine Einstufung wie „vertraulich“ beschreibt den Schutzbedarf einer Information. Dieser ändert sich nicht mit der Office-Strategie.

Genau hier setzt NovaPath an: Die Software klassifiziert Office-Dokumente, PDFs und E-Mails. Die gesetzten Klassifizierungsmetadaten verbleiben im Dokument und sind unabhängig von Microsoft Office. Damit muss ein Wechsel der Arbeitsumgebung nicht bedeuten, dass vorhandene Klassifizierungsinformationen verloren gehen.

Die Sicherheitsrichtlinie gehört dem Unternehmen – nicht dem Hersteller der Office-Anwendung.

Classified by NovaPath

Souverän ist, wer entscheiden kann

Digitale Souveränität bedeutet nicht, auf Cloud-Dienste oder amerikanische Technologie zu verzichten. Sie bedeutet, Alternativen zu besitzen. Unternehmen sollten selbst entscheiden können, wo sensible Informationen verarbeitet werden, welche Systeme dafür eingesetzt werden und wann ein Plattformwechsel sinnvoll ist.

Deutsche und europäische Lösungen wie NovaPath können dabei Wahlfreiheit schaffen: lokal betreibbar, unter eigener Kontrolle und auf die Anforderungen des Unternehmens anpassbar.



Informationsklassifizierung Made in Germany

NovaPath ist eine in Deutschland von der M&H IT-Security GmbH entwickelte Software für technische Informationsklassifizierung. Sie kann vollständig On-Premises betrieben werden; Datenhoheit, Klassifizierungslogik und Konfiguration verbleiben beim Kunden.

Individuelle Klassifizierungsregeln · On-Premises · DLP & Verschlüsselung · Made in Germany

Sie reduzieren Microsoft-Abhängigkeiten oder prüfen alternative Office-Strategien? Sprechen Sie mit uns über Ihre Klassifizierungsstrategie.

novapath.de **mh-it-security.de**

Warum mobile Apps zum gefährlichen Einfallstor werden

App-Entwicklung unter Zeitdruck lässt Sicherheit zur Nebensache werden. Mobile Apps werden so zum Einfallstor für Cyberangriffe, die Kundendaten, Unternehmensidentitäten und Geschäftsprozesse gefährden. Wer jetzt nicht auf automatisierte Sicherheit setzt, riskiert Vertrauen, Reputation und regulatorische Strafen.

Von Ismet Koyun, KOBIL

Vom praktischen Helfer zum zentralen Zu gangspunkt für digitale Dienste Mobile An wendungen haben sich zum unverzichtbaren estandteil unserer digitalen Infrastruktur entwickelt Immer mehr ervices laufen wie selbstverständlich über mobile ndgeräte, vom



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

anking über den nline andel bis hin zu ealth und digitalen ehördengängen Gleichzeitig verlagern Unternehmen auch in terne Geschäftsprozesse zunehmend auf mo bile Plattformen.

Das Problem: Je bedeutender die App-Nutzung wird, desto mehr wächst das Risiko. Smartphones sind einer der häufigsten Angriffspunk te für Cyberkriminelle. Laut dem Mobile Secu rity Index 2025 von Verizon berichten weltweit 85 Prozent der Unternehmen, dass mobile Angriffe zugenommen haben. Die größte Be drohung sind demnach Mobile-Phishing-Me thoden, zum Beispiel über SMS („Smishing“) oder als Voice-Phishing („Vishing“). Künstliche Intelligenz sorgt dafür, dass die Attacken im mer ausgefeilter werden und kaum noch von echten Anfragen zu unterscheiden sind. Weite re Bedrohungsszenarien reichen von Reverse Engineering über Code Injection bis zu Manipu lation auf gerooteten Geräten.

Mobile Apps enthalten hochsensible Nutzerda ten und fungieren zunehmend als Schnittstel len zu Unternehmenssystemen. Ein erfolgrei cher Angriff kann damit schnell zum Einfallstor für weitreichende Sicherheitsvorfälle werden. App-Sicherheit ist deshalb längst ein geschäfts kritischer Faktor. Es geht nicht nur um Daten schutz, sondern um den Schutz der digitalen Identität, der Business-Logik und letztlich um die Widerstandsfähigkeit der gesamten digita len Infrastruktur.

AGILITÄT VERSUS SICHERHEIT?

Bei der App-Entwicklung arbeiten Teams oft un ter enormem Zeitdruck. Das Thema Sicherheit wird daher oft ans Ende des Entwicklungspro zesses verschoben – oder sogar erst nach dem Go-Live angegangen. Das Problem sind die feh lenden Ressourcen. Klassische Sicherheitsinte gration über ein Software Development Kit be deutet erheblichen zusätzlichen Aufwand und tiefes Security-Fachwissen. Doch Sicherheits experten sind auf dem Arbeitsmarkt schwer zu finden. Gleichzeitig steigen die regulatorischen Anforderungen, etwa durch DSGVO, ISO 27001 und HIPAA. Unternehmen müssen nachweisen, dass sie die Daten und Identitäten ihrer Nutzer aktiv schützen. Besonders Startups stehen vor einem Dilemma: Sie müssen schnell skalie ren, haben aber weder finanzielle Mittel noch Kapazitäten für eigene Security-Engineers. Auf Sicherheit können sie aber nicht verzichten – zu groß sind die Risiken eines Sicherheitsvor falls in der Wachstumsphase.

FOKUS AUF SECURITY-AS-A-SERVICE

Das Problem lässt sich nicht lösen, solange Unternehmen Sicherheit als nachträgliches Add-on betrachten. Vollständigen App-Schutz bieten nur Sicherheitskonzepte, die von vorn herein um die Themen IT Security, Datenschutz und sicheres Identitätsmanagement gebaut wurden. Wenn App-Entwickler das nicht selbst leisten können, brauchen sie externe Unter stützung – etwa in Form von Security-as-a-Ser vice (SECaaS). Der zentrale Vorteil: Sicherheit wird aus der Komplexität des Codes heraus gelöst und als eigenständige, automatisierte Dienstleistung bereitgestellt

Idealerweise folgen SECaaS-Lösungen einem Zero-Code-Ansatz. Sie sind also ohne Program mierung direkt einsatzbereit und können vor handene App-Binärdateien sofort schützen. Die Datei wird dabei analysiert und anschlie ßend automatisch gehärtet. Refactoring, Re build und zusätzlicher Entwicklungsaufwand sind nicht notwendig.

So können Entwickler, Unternehmen und Start-ups ihre mobilen Anwendungen schnell und sicher bereitstellen. Dieser Ansatz demokrati siert selbst hochentwickelte Sicherheitstech nologie. Sicherheit wird für Organisationen jeder Größe zu einer On-Demand-Ressource, vergleichbar mit Cloud-Diensten.

⇨

Europas digitale Souveränität beginnt beim Router

TDT AG – Sichere Netzwerktechnologie aus Deutschland – Made in Germany

Die TDT AG entwickelt, produziert und supportet professionelle Router, Gateways und Firewalls für Unternehmen und KRITISAnwender. Als „High Security Data Company" steht TDT für souveräne, hochsichere und langfristig wartbare Netzwerklösungen auf Basis von Open-Source-Technologien. TDT ist seit 2017 Silver Member der Linux Foundation und nach ISO 27001 auf Basis des BSI IT-Grundschutzes zertifiziert.

Wir wissen heute um die Risiken kritischer digitaler Infrastrukturen. Wir diskutieren über Cloud, Halbleiter und Technologielieferketten. Doch ein entscheidender Baustein bleibt dabei häufig im blinden Fleck: der Router.

Als digitale Zentrale von Haus und Unternehmen transportiert er mehr als 90 Prozent des Datenverkehrs. Er ist der digitale Hausschlüssel – und damit ein zentraler Baustein unserer digitalen Souveränität. Die entscheidende Frage lautet deshalb: **Wem vertrauen wir diesen Schlüssel an?**

Vier führende europäische Netzwerktechnologie-Unternehmen – devolo, FRITZ!, LANCOM und TDT AG – haben deshalb SAFENet gegründet: die **Sovereignty Alliance for European Network Technology**.

Unser Ziel ist klar: **Europa muss die Kontrolle über seine Netze und seine digitale Infrastruktur behalten.** Gemeinsam wollen wir Politik, Wirtschaft und Gesellschaft dafür sensibilisieren, dass Router und Netzwerktechnologie eine strategische Schlüsselrolle für die technologische Souveränität Europas spielen. Denn digitale Souveränität bedeutet nicht nur, Daten und Anwendungen zu kontrollieren – sie beginnt bei der Technologie, die diese Daten sicher und zuverlässig transportiert.



Bild: TDT AG / KI-generiert

TDT® | Your experts in TELE COMMUNICATION

Die Zahlen unterstreichen den Handlungsbedarf: Laut einer aktuellen Studie der Innovate Europe Foundation (IE.F) laufen rund 93 Prozent des europäischen Internetverkehrs über Router und Heimnetz-Gateways. Chinesische Hersteller kontrollieren knapp 40 Prozent dieses Marktes. Während Europa bei Cloud und Halbleitern seine Abhängigkeiten reduziert, bleibt die zentrale Hardware-Schnittstelle unserer digitalen Kommunikation weitgehend unbeachtet.

Dabei gibt es die Alternative längst: Europäische Hersteller entwickeln und produzieren souveräne, vertrauenswürdige und innovative Netzwerktechnologie. Was fehlt, sind politische Aufmerksamkeit und geeignete regulatorische Rahmenbedingungen.

SAFENet wächst. Im September 2026 schlossen sich fünf weitere Unternehmen der Allianz an: Genexis, IPmotion, MB connect line, Teldat und Waystream. Weitere europäische Hersteller sind willkommen.

Digitale Souveränität ist keine Zukunftsvision. Sie beginnt mit den Technologien, die unsere Netze heute verbinden.



Das BSI-Zertifikat ist für TDT auch eine Verpflichtung, dafür Sorge zu tragen, dem Kunden die bestmögliche Sicherheit und Qualität zu gewährleisten.

Die **Sovereignty Alliance for European Network Technology (SAFENet)** ist eine Allianz führender europäischer Netzwerktechnologie-Unternehmen. Sie setzt sich für die technologische und digitale Souveränität Europas ein und bringt die Interessen europäischer Hersteller in den politischen und regulatorischen Dialog ein. **SAFENet steht für ein digitales Europa, das selbstbestimmt, resilient und zukunftsfähig ist.**

Mehr Informationen: safe-net.tech

Die TDT AG erstellt individuelle Netzwerkkonzepte, übernimmt das weltweite Netzwerkmanagement und bietet umfassenden professionellen Service. Das Unternehmen ist seit 2017 Silver Member der Linux Foundation und nach ISO 27001 auf Basis des BSI IT-Grundschutzes zertifiziert. **Entwicklung, Produktion und Support erfolgen in Deutschland – Made in Germany.**

Mehr Informationen: tdt.de


Bild: Monstar Studio – stock.adobe.com

WAS MUSS EINE SOLCHE TECHNOLOGIE KÖNNEN?

Für ma imalen chutz müssen aa Model le über eine tief integrierte, mehrschichtige Sicherheitsarchitektur verfügen. Dazu gehört ein präventiver Schutz durch Code-Verschlei erung, Verschlüsselung und Integritätsprüfun gen. Gleiches gilt für angemessene Abwehr mechanismen bei Bedrohungen, etwa durch Echtzeit-Erkennung von Debugging, Hooking oder Emulator-Nutzung. Unverzichtbar ist auch eine KI-gestützte Threat Detection: Künstliche Intelligenz bewertet Verhaltensmuster in Echt zeit, lernt aus neuen Angriffstaktiken und passt Schutzmaßnahmen dynamisch an.

Ein kritischer Vorteil ist zudem Compliance by Design: Sicherheitsmechanismen sind in die sem Fall so implementiert, dass sie regulato rische Anforderungen von Anfang an abdecken und automatisiert dokumentieren. Lückenlose Audit-Trails sind damit garantiert. Das erspart eine teure Beratung und manuelle Nachweis prozesse.

VORTEILE DER DYNAMISCHEN ANALYSE

Zur kontinuierlichen Erkennung von Sicher heitslücken sollten SECaaS-Lösungen sowohl auf statische als auch auf dynamische Analysen setzen. Eine statische Analyse untersucht den Code, ohne ihn auszuführen. Sie ist wichtig, aber ihre Aussagekraft ist begrenzt. Sie kann nicht vorhersagen, wie sich eine App im echten Laufzeitkontext verhält oder ob Sicherheits vorkehrungen in der Praxis umgangen werden können.

An dieser Stelle kommen dynamische Ana lysen ins Spiel. Sie testen die App im echten Laufzeitkontext – auf physischen Geräten oder Emulatoren – und simulieren tatsächliches An greiferverhalten. Die App wird aktiv attackiert, während KI-Agenten das Verhalten auswerten. Das Ergebnis ist ein detaillierter Sicherheits report mit konkreten, priorisierten Handlungs empfehlungen. Die Genauigkeit liegt nahezu bei 100 Prozent, weil sie auf tatsächlichem Verhalten basiert.

SKALIERBARE SICHERHEIT – VON STARTUP BIS KONZERN

Ein zentraler Vorteil automatisierter Security-as-a-Service-Modelle liegt in ihrer Skalierbarkeit. Die gleiche Technologie, die ein Startup nutzt, funktioniert in globalen Enterprise-Umgebungen mit hunderten Apps. Für Startups sind solche Lösungen besonders wertvoll. Sie ermöglichen einen schnellen, sicheren Markteintritt ohne eigene Security-Expertise. Der gesamte Prozess – vom Upload über die Analyse bis zur Aktivierung des Schutzes – kann in wenigen Minuten abgeschlossen werden. Das minimiert Entwicklungsrisiken und beschleunigt die Zeit bis zur Markteinführung.

Mittelständische und große Unternehmen profitieren davon, Sicherheit über alle mobilen Anwendungen hinweg zu standardisieren und zentral zu verwalten. Konsistente, erprobte Schutzmaßnahmen können automatisiert ausgerollt werden. Das reduziert Komplexität und verringert die Abhängigkeit von Sicherheitsexperten.

VERTRAUEN IST DIE NEUE WÄHRUNG

In einer digitalisierten Welt wird Vertrauen zum zentralen Wettbewerbsfaktor. Wenn Nutzer nicht glauben, dass ihre Daten sicher sind, entsteht kein langfristiges Kundenverhältnis. Sicherheitsvorfälle werden sofort öffentlich und können die jahrelang aufgebaute Reputation eines Unternehmens in kürzester Zeit zerstören.

Sicherheit ist ein strategischer Differenzierungsfaktor. Unternehmen, die Sicherheit von Anfang an mitdenken, schaffen nachhaltige Glaubwürdigkeit. Das wirkt sich direkt auf Markenwahrnehmung, Kundentreue und Geschäftserfolg aus. Wer in präventive Sicherheit investiert, reduziert zudem Kosten für Incident Response, vermeidet regulatorische Strafen und schützt sich vor Imageschäden.

AUSBLICK: DIE ZUKUNFT MOBILER SICHERHEIT

Die Entwicklung ist eindeutig: Wir werden einen weiteren Schub in Richtung Automatisierung und KI-gestützter Sicherheitsarchitekturen erleben. Autonome Systeme können Risiken erkennen, bewerten und abwehren – oft schneller und präziser als menschliche Experten. Gleichzeitig wird der Fokus stärker auf Datenschutz und digitale Identitäten rücken.

Mobile Sicherheit wird endgültig von einer technischen Notwendigkeit zur strategischen Grundlage digitaler Geschäftsmodelle. Der Schlüssel zum Erfolg: Automatisierung, Einfachheit und die Integration von Sicherheit als selbstverständlichen Bestandteil des Entwicklungsprozesses. □



Bild: KOBIL Gruppe

ÜBER DEN AUTOR

Ismet Koyun ist CEO und Gründer der KOBIL Gruppe.

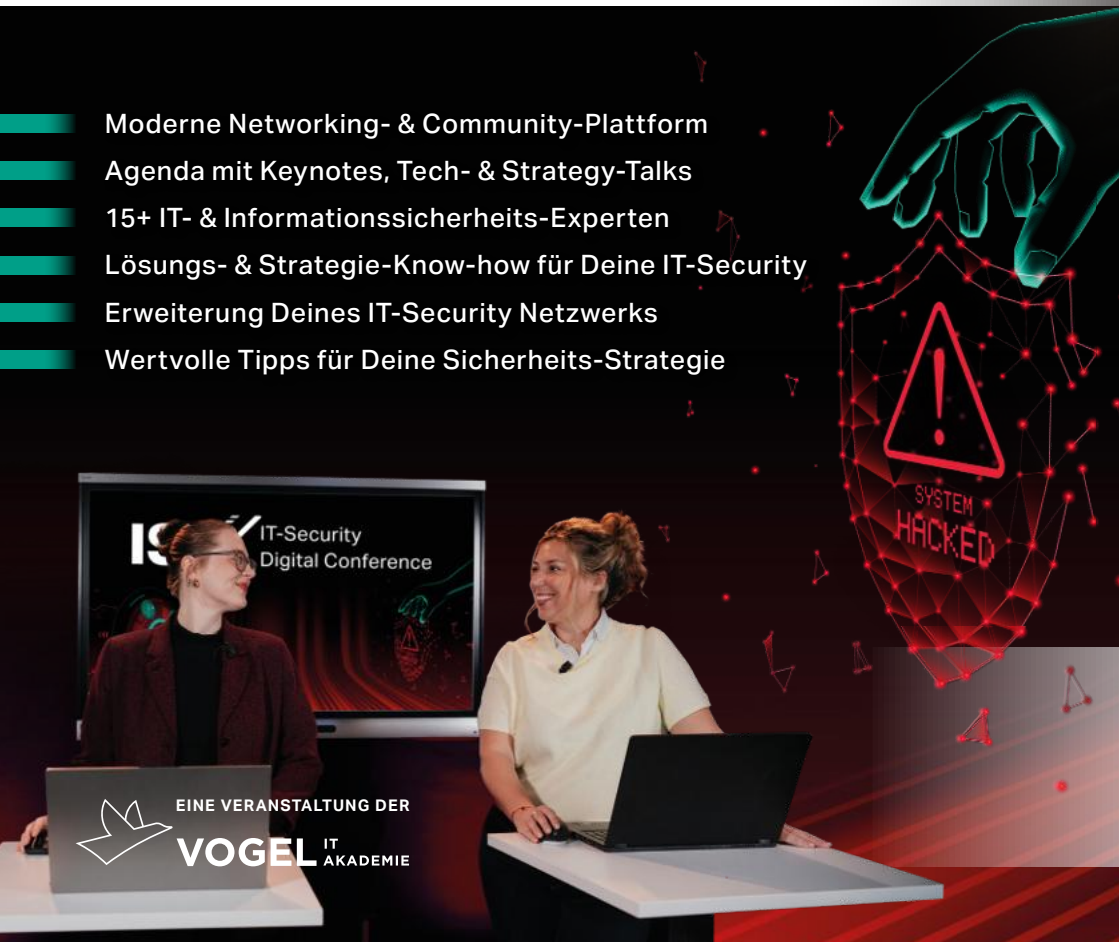
ISX IT-Security Digital Conference

17. November 2026

DETECT. RESPOND. DEFEND.

Mit **KI** Cyberrisiken voraus sein.

- Moderne Networking- & Community-Plattform
- Agenda mit Keynotes, Tech- & Strategy-Talks
- 15+ IT- & Informationssicherheits-Experten
- Lösungs- & Strategie-Know-how für Deine IT-Security
- Erweiterung Deines IT-Security Netzwerks
- Wertvolle Tipps für Deine Sicherheits-Strategie



EINE VERANSTALTUNG DER VOGEL IT AKADEMIE



Speaker Preview:



Candid Wüest
Principal Security Advocate, xorlab

»Der KI-Flaschengeist: Von Shadow AI bis Evil AI – Risiken erkennen und wirksam steuern«



Georgia Voudoulaki
Senior Legal Counsel, Robert Bosch

»Wenn KI zum Sicherheitsrisiko wird: Warum Cybersecurity AI Governance braucht«



Christian Schneider
Security Architect, Pentester & Trainer

»Jede Komponente grün, trotzdem gehackt: Threat Modeling für Agenten-Architekturen«

»GET YOUR FREE TICKET«

Sichere Dir Dein **kostenfreies** Ticket unter
www.isxconference.de/isx-digital

Post-Quanten-Kryptografie wird zur Pflicht

Quantencomputer können heute verbreitete asymmetrische Verschlüsselungsverfahren problemlos knacken. Experten rechnen mit ihrer breiten Verfügbarkeit in fünf bis zehn Jahren, aber Angreifer können schon heute Daten abgreifen und später entschlüsseln. Unternehmen müssen jetzt prüfen, wie sie Post-Quanten-Kryptografie implementieren können.

Von Dr. Markus von Detten, achelos

Die Ära der Quantencomputer ist angebrochen. Damit gerät die Nutzung aktueller kryptografischer Methoden, die ein zentraler Bestandteil unserer heutigen digitalen Welt ist, in Gefahr. Quantencomputer können gerade asymmetrische kryptografische Verfahren problemlos entschlüsseln. Neue, sichere Methoden, die auch von Quantencomputern nicht zu knacken sind, wurden bereits auf den Weg gebracht – die Post-Quanten-Kryptografie. Unternehmen sollten zeitnah analysieren, ob und in welchen Geschäftsbereichen sie diese implementieren müssen, damit ihre Prozesse auch künftig sicher bleiben.



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

Das inloggen in Accounts im Internet, die E-Mail-Verschlüsselung über Zertifikate, der Identitätsnachweis mit Chipkarten, etwa der Gesundheitskarte, oder der Zutritt zu Gebäuden mit Zugangstokens: All diese Vorgänge beruhen auf kryptografischen Verfahren. Sie ermöglichen den Nachweis der Identität (Authentisierung), stellen Integrität und Authentizität sowie Vertraulichkeit und Schutz vor Missbrauch sicher und erlauben einen kontrollierten Zugang (Autorisierung) in verschiedenen Anwendungsbereichen.

Kryptografie basiert auf mathematischen Operationen: Die symmetrische Kryptografie setzt denselben Schlüssel zum Ver- und Entschlüsseln von Informationen ein; die asymmetrische Kryptografie nutzt einen Schlüssel zum Ver- und einen weiteren zum Entschlüsseln. Ersterer kann beliebig verteilt werden, letzterer bleibt geheim und beim Empfänger.

Das Prinzip hinter der asymmetrischen Kryptografie: eine Rechenoperation, die einfach zu berechnen, aber schwierig rückzurechnen ist, etwa die Multiplikation großer Primzahlen. Da diese Operation zu sehr hohen Ergebnissen führt, war es lange Zeit nicht effizient möglich, auf die beiden Faktoren zurückzuschließen und damit die Entschlüsselung durchzuführen. Ein Ausprobieren hätte schlicht zu viel Zeit in Anspruch genommen: bei einer Zahl mit Hunderten von Stellen Millionen von Jahren.

Schon in den 1970er und 1980er Jahren waren sich Mathematiker aber darüber im Klaren, dass ein Problem entstehen würde, wenn Computer in der Lage wären, das Rückrechnen auf die Faktoren schneller durchführen zu können. Shor's Algorithmus war Anfang der 90er Jahre schließlich dazu in der Lage, aber es fehlte ein Rechner, der diesen dediziert für Quantencomputer entwickelten Algorithmus umsetzen konnte. Heute, rund 50 Jahre später, zeichnet sich ab, dass dieser bald Realität werden könnte: Unternehmen und Institutionen befinden sich im Wettlauf um den Bau von Quantencomputern. IBM ist dies bereits 2001 gelungen, verschiedene Forschungsgruppen und Google waren ebenfalls erfolgreich darin, den Shor-Algorithmus zu implementieren und eine Primzahlfaktorisierung kleiner Produkte durchzuführen.

Quantencomputer werden also in der Lage sein, die asymmetrische Verschlüsselung zu knacken. Symmetrische Verfahren sind ebenfalls durch einen Quantenalgorithmus, Grover's Algorithmus, angreifbar – sie verlieren etwa die Hälfte ihrer Stärke.

Experten rechnen damit, dass in fünf bis zehn Jahren Quantencomputer in der Breite verfügbar sein werden. Zunächst in den Händen von Regierungen und Geheimdiensten, Konzernen und Institutionen. Damit wären zahlreiche Kommunikationen abhörbar, Dokumente und Identitäten könnten gefälscht werden. Der Industriespionage würde Tür und Tor geöffnet und die Unsicherheit wäre groß: Denn niemand wird wissen, wer denn jetzt über einen solchen Rechner verfügt und wer nicht. Gegnerische Kräfte könnten dies verheimlichen und unbemerkt einfach mitlesen.

POST-QUANTEN-KRYPTOGRAFIE

Doch es gibt auch gute Nachrichten: Das Gegenmittel wurde bereits entwickelt – die Post-Quanten-Kryptografie (PQC). Sie beinhaltet kryptografische Verfahren, die mit bestehender Hardware durchgeführt werden können und von einem Quantencomputer tatsächlich nicht angreifbar sind. Dafür werden andere mathematische Operationen wie gitterbasierte Kryptografie eingesetzt.

Das National Institute for Standards and Technology (NIST) in den USA, das Äquivalent zum Bundesamt für Sicherheit in der Informationstechnik (BSI), hatte bereits in den 90er Jahren einen offenen Wettbewerb initiiert und Universitäten dazu aufgefordert, ein neues Verfahren ⮑

↳ für die symmetrische Kryptografie zu entwickeln. Daraus entstand der De-Facto-Standard AES (Advanced Encryption Scheme). Dieses Vorgehen wurde nun für die Post-Quanten-Kryptografie wiederholt und die vorgeschlagenen Verfahren in mehreren Auswahlrunden getestet und bewertet. Einige sichere Algorithmen wurden entwickelt, die für verschiedene Zwecke eingesetzt werden können: ML-KEM, ML-DSA und SLH-DSA.

UNTERNEHMEN SOLLTEN EINE PRÜFUNG ANSTOSSEN

Unternehmen sollten sich bereits heute damit beschäftigen, welche ihrer Prozesse durch den Einsatz von Quantencomputern nicht mehr sicher sein werden. Das Problem ist noch nicht akut und es besteht noch Zeit, zu handeln.

Es gibt eine weitere gute Nachricht: Nicht alle Anwendungen mit asymmetrischer Verschlüsselung liegen im eigenen Verantwortungsbereich. Microsoft wird mit Sicherheit Windows-Updates oder neue Versionen herausbringen, die die neuen PQC-Verfahren beinhalten, das gleiche gilt für die Anbieter von Browsern wie Mozilla oder Google. Allerdings muss hier sichergestellt werden, dass die Anwendungen korrekt konfiguriert sind: Bei der E-Mail-Verschlüsselung müssen zum Beispiel die alten Zertifikate, die die klassischen asymmetrischen Schlüsselalgorithmen wie RSA oder ECC nutzen, ersetzt werden. Andere Bereiche liegen direkt in der Verantwortung der Unternehmen: Wenn Forschungsdaten mit Werkzeugen verschlüsselt und abgelegt werden, dürfen diese nicht durch Quantencomputer angreifbar sein. Auch wenn Zugangsrechte mit Smartcards oder Tokens gewährt werden, müssen die genutzten Lösungen aktualisiert werden.

Hersteller, die standardmäßig kryptografische Verfahren in ihren Produkten unterstützen, müssen sie ebenfalls auf den Prüfstand stellen. Das gleiche gilt für Softwareanbieter, die Bibliotheken mit Kryptografie-Funktionen bereitstellen oder nutzen.

DIE UMSTELLUNG AUF PQC

In Unternehmen muss zunächst auf Geschäftsführungsebene ein Bewusstsein entstehen. Sie benötigen einen Überblick, in welchen Prozessen welche Art der Kryptografie angewendet und wie sie technisch gelöst wird. In einer perfekten Welt besitzt die Geschäftsführung diese Übersicht über die kryptografischen Verfahren, ein Krypto-Inventory, im Sinne der Kryptoagilität bereits. Denn abseits von PQC versetzt er sie in die Lage, bei Problemen schnell reagieren zu können, etwa wenn Algorithmen ausgetauscht werden müssen, weil sich eine Schwachstelle aufgetan hat. Bei SHA-1 wurden zum Beispiel konzeptionelle Probleme im Hash-Algorithmus aufgedeckt und er wurde flächendeckend durch SHA-2 ersetzt.

Im nächsten Schritt ist es wichtig, Automatisierungspotenziale zu identifizieren, sodass der Austausch kryptografischer Verfahren nicht mehr händisch erfolgen und zum Beispiel nicht für jede einzelne Person manuell ein neues E-Mail-Zertifikat ausgestellt und verteilt werden muss.

Bei der Bewertung des Handlungsbedarfs sollten Unternehmen die zeitliche Perspektive im Blick behalten. Logins am Rechner müssten zum Beispiel in Echtzeit angegriffen werden: Da es kryptografisch relevante Quantencomputer noch nicht gibt, besteht hier noch kein akuter Handlungsdruck. Bei der Verschlüsselung von Forschungs- und Entwicklungsdaten stellt sich die Lage anders dar: Sie könnten heute bereits entwendet und erst später entschlüsselt werden (harvest now, decrypt later), wenn die notwendige Technologie zur Verfügung steht. Sind die eigenen Anwendungsfälle nicht betroffen oder werden durch Updates von Drittanbietern gelöst, besteht gegebenenfalls wenig Handlungsbedarf.

nternehmen sollten sich aber darüber im Klaren sein, dass die Migration bestehender Infrastrukturen wie VP oder PKIs auf P aufwändig sein kann selbst wenn pdates der ersteller zur Verfügung stehen pgrades oder der Austausch von Komponenten, die Im plementierung und der Einbau erfordern Zeit. icht nur die Technik muss verfügbar sein, auch die davon abhängigen Prozesse müssen angepasst werden Deswegen ist eine Vorbe reitung schon heute sinnvoll

Die PQC-Algorithmen sind zwar konzeptionell ausgereift, aber größtenteils nicht so effizient oder performant wie die Vorgänger Die chlüs sel sind länger entsprechend kann die e rechnung mehr Zeit in Anspruch nehmen. Nor male Computer oder Laptops können das ohne Weiteres leisten, bei eingebetteten Systemen kann es etwas dauern. Auch Signaturen können signifikant größer werden. Viele Embedded hips und Tokens kommen hier an ihre Gren zen; ebenso Systeme mit weniger Prozessor leistung, Speicherplatz und Energieverbrauch. Hier ist die Frage noch offen, welche PQC-Ver fahren dort anwendbar sein werden. Es gibt aber bereits Ansätze, diese erausforderungen anzugehen In anderen ereichen gibt es dage gen schon Anbieter, die P Verfahren in ihren Produkten implementiert haben, etwa in Soft warebibliotheken oder Kryptohardware wie Hardware-Security-Modulen zur Verwahrung von chlüsseln

STANDARDISIERUNG DER VERFAHREN

Es ist noch nicht klar, welche PQC-Verfahren sich durchsetzen werden Das I T standardi sierte drei Algorithmen, mindestens zwei wei tere sind in Planung. Das BSI empfiehlt darüber hinaus weitere Verfahren, die das I T aus un terschiedlichen Gründen wohl nicht weiterver folgen wird Darüber hinaus werden auch neue P Verfahren entwickelt werden Das kann zu Unsicherheiten führen. Es ist aber wahrschein lich, dass sich bestimmte Standards für gewis se Anwendungsfälle durchsetzen und daneben Sonderlösungen für Spezialanwendungen exis tieren werden. Hersteller können dann abhän gig vom Einzelfall eine Entscheidung treffen.

FAZIT

An Post-Quanten-Kryptografie führt künftig kein Weg vorbei, da asymmetrische Kryptogra fie von Quantencomputern entschlüsselt wer den kann Für nternehmen bedeutet dies, dass ihre Anwendungen, die auf asymmetrischer Kryptografie basieren, auf neue Post-Quanten-Kryptografie-Verfahren umgestellt und konfi guriert werden müssen nternehmen sollten sich einen Überblick verschaffen, welche Ver fahren wo angewendet werden, und bewerten, wo andlungsbedarf besteht □



ÜBER DEN AUTOR

Dr. Markus von Detten ist Senior Consultant PKI bei der achelos GmbH.

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, Matthias Bauer

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 ,
David Holliday,
Stephanie Steen
Anzeigendisposition: Denise Falloni, Mihaela Mikolic

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

Grafik & Layout: Alex Preböck (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

Haftung: Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich

Copyright: Vogel IT-Medien GmbH. Alle Rechte vorbehalten. Nachdruck, digitale Verwendung jeder Art, Vervielfältigung nur mit schriftlicher Genehmigung der Redaktion.

Manuskripte: Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen.

Nachdruck und elektronische Nutzung: Wenn Sie Beiträge dieser Ausgabe für eigene Veröffentlichungen wie Sonderdrucke, Websites, sonstige elektronische Medien oder Kundenzeitschriften nutzen möchten, erhalten Sie Informationen sowie die erforderlichen Rechte über: lilli.kos@vogel.de



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

ads-tec Industrial IT GmbH	Nürtingen	https://www.ads-tec.com/	40
BAYOOSOFT GmbH	Darmstadt	https://www.bayoosoft.com/	36
Bundesverband IT-Sicherheit e.V. (TeleTrusT)	Berlin	https://www.teletrust.de/	U3
G DATA Software AG	Bochum	https://www.gdata.de	28, U2
genua GmbH	Kirchheim bei München	https://www.genua.de/	21, 23
INFODAS GmbH	Köln	https://www.infodas.com	32
M&H IT-Security GmbH	Berlin	https://mh-it-security.de/	44
NCP engineering GmbH	Nürnberg	https://www.ncp-e.com/de/	18
PFALZKOM GmbH	Ludwigshafen	https://pfalzkom.de/	14
Reiner Kartengeräte GmbH und Co. KG	Furtwangen	https://www.reiner-sct.com	8
TDT AG	Essenbach	https://tdt.de	48
Vogel IT-Akademie	Augsburg	https://www.vogelitakademie.de	52

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.

Secur**IT**y 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.


HIER GEHT'S
ZUR MICROSITE:
https://www.it-business.de/
Security_madeInGermany