OKTOBER 2023

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

MADE IN GERMANY

VOGEL IT MEDIEN

Eine Publikation von IT-BUSINESS SECURITY INSIDER

Powered by:

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

G DATA
CyberDefense

Managed EDR
Made in Germany

Ihr 24/7-Expertenschutz aus Deutschland:
Wir erkennen und stoppen Cyberangriffe für Sie.

itsa
Stand: 7-210

Besuchen Sie unsere hybriden Workshops. **Jetzt anmelden** und Gratis-Ticket sichern!

TRUST IN
GERMAN
SICHERHEIT

Liebe Leserinnen und Leser,

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

die IT-Sicherheit ist zu einem zentralen Thema in unserer digitalisierten Welt geworden. Die steigende Anzahl von Cyberangriffen und Datenlecks verdeutlicht die Notwendigkeit, unsere IT-Infrastrukturen effektiv zu schützen.

Unter der Überschrift "IT Security made in Germany" möchten wir in dieser Publikation neue Ansätze und Konzepte in der IT-Sicherheit vorstellen. Als führender Standort für IT-Sicherheit bietet Deutschland eine Vielzahl von Lösungen, die auf die spezifischen Bedürfnisse unserer Unternehmen und Organisationen zugeschnitten sind.

Ein Schwerpunkt der Publikation liegt auf der EU-Richtlinie zu NIS2 und den Auswirkungen auf Unternehmen. Diese Richtlinie zielt darauf ab, die Sicherheit und Resilienz kritischer Infrastrukturen zu verbessern und Unternehmen zu verpflichten, angemessene Sicherheitsmaßnahmen zu implementieren. Wir beleuchten, welche Anforderungen auf Unternehmen zukommen und wie sie sich darauf vorbereiten können.

Unternehmen und Organisationen sind heutzutage stark vernetzt und arbeiten mit Partnern und Lieferanten auf der ganzen Welt zusammen. Dies erhöht die Angriffsfläche und macht es schwieriger, die Sicherheit entlang der gesamten Lieferkette zu gewährleisten. Eine Schwachstelle in einem Unternehmen kann sich schnell auf andere ausbreiten und somit die gesamte Wirtschaft beeinträchtigen.

Ein weiteres Thema, das uns beschäftigt, ist die Sicherheit im öffentlichen Sektor. Behörden und Institutionen stehen vor einzigartigen Herausforderungen, wenn es um den Schutz sensibler Daten und Infrastrukturen geht. Wir diskutieren Ideen, Lösungen und Herausforderungen, mit denen der öffentliche Sektor konfrontiert ist und wie wir gemeinsam daran arbeiten können, die Sicherheit zu gewährleisten.

Schutzbedarf und Kostendruck sind zwei Faktoren, die oft als gegensätzlich wahrgenommen werden. Doch wie können Unternehmen beides in Einklang bringen und effektive Sicherheitsmaßnahmen implementieren, ohne ihr Budget zu sprengen. Insbesondere da die Angriffsmuster und -techniken ständig im Wandel sind. Cyberkriminelle und staatliche Akteure entwickeln kontinuierlich neue Methoden, um Sicherheitsmaßnahmen zu umgehen. Dies erfordert eine stetige Anpassung und Weiterentwicklung unserer Abwehrstrategien.

Schließlich ist die IT-Sicherheit auch eine Frage der individuellen Verantwortung. Jeder von uns trägt eine gewisse Verantwortung, um seine eigenen digitalen Geräte und Daten zu schützen. Die Sensibilisierung für Sicherheitsrisiken und die Umsetzung von Best Practices sind entscheidend, um die Sicherheit insgesamt zu verbessern.

Wir müssen uns bewusst sein, dass die IT-Sicherheit eine globale Herausforderung bleibt, die eine enge Zusammenarbeit und Koordination erfordert.

Die vorliegende Publikation gibt Orientierung und fasst die wichtigsten Maßgaben für die IT-Sicherheit zusammen.

Im Namen von TeleTrusT wünsche ich eine interessante Lektüre. □

IT SECURITY MADE IN GERMANY

Die Initiative: Vertrauen hat einen Namen 6

IT-SICHERHEIT IM CYBERRAUM

Die wachsende Bedrohung durch Cyberwar: Was zur Verteidigung gegen Cyberkriege noch getan werden muss 10

Standort ist kein Sicherheitsfaktor: Work Anywhere: IT, Nutzende und Daten sind überall 16

Besonderheiten von Cloud-Identitäten: Digitale Identitäten als Schlüssel zur Cloud 22

IT-SICHERHEIT FÜR RECHENZENTREN

Rechtsvorschriften für Rechenzentren: Datacenter sind kritische Infrastruktur 28

Aspekte der Rechenzentrumssicherheit: Was heißt Sicherheit von Rechenzentren im Jahr 2023? 34

GEFAHREN FÜR DEN DATENSCHUTZ

ChatGPT im Unternehmenseinsatz: Lässt sich ChatGPT datenschutzgerecht nutzen? 37

Cybersicherheit und Datenschutz: Datenschutzverletzungen durch Cyberattacken 42

Cloud-Regionen innerhalb der EU: Datengrenzen für die Cloud: Was bringt es für den Datenschutz? 47

CYBERVERSICHERUNG UND SOC

Risikomanagement: Sicherheitsbaustein Cyberversicherung 52

Security Operations Center (SOC) as a Service: Wie der richtige Vertrag die Haftung reduziert 55

REDAKTION

Editorial 3

Impressum / Inserenten 58

TeleTrusT-Initiative "IT Security made in Germany"

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

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

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

ISXQIV/23

IT-Security Virtual Conference

>> 29. NOVEMBER VIRTUAL
www.isxconference.de
JETZT ANMELDEN!

GET READY FOR **INTELLIGENT CYBERSECURITY!**

Unter diesem Motto erwarten Dich hochkarätige Speaker und brandaktuelle Themen, welche Dich und Dein Unternehmen im Kampf gegen Cyberangriffe voranbringen und Antworten liefern!

>> JETZT TICKET SICHERN

EINE VERANSTALTUNG DER VOGEL IT AKADEMIE

Vertrauen hat einen Namen

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

Träger des Vertrauenszeichens "IT Security made in Germany" (Stand 12.09.2023)

- 5Compliance
- Accellence Technologies GmbH
- AceBIT GmbH
- achelos GmbH
- Achtwerk GmbH & Co. KG
- ads-tec GmbH
- agilimo Consulting GmbH
- aigner business solutions GmbH
- AirID GmbH
- Alpha Strike Labs GmbH
- Alter Solutions Deutschland GmbH
- ANMATHO AG
- Antago GmbH
- APRO Computer & Dienstleistung GmbH
- apsec Applied Security GmbH
- ASOFTNET
- arian IT Service GmbH
- asvin GmbH
- ATIS systems GmbH
- Atruvia AG
- AUCONET Solutions GmbH
- AUTHADA GmbH
- authenton GmbH
- AWARE7 GmbH
- axilaris GmbH
- Bank-Verlag GmbH
- Bare.ID GmbH
- BAYOOSOFT GmbH
- BCC Unternehmensberatung GmbH
- Bechtle GmbH & Co. KG
- Beta Systems IAM Software AG
- Biteno GmbH
- Blue Frost Security GmbH
- Bosch CyberCompare
- Build38 GmbH
- Bundesdruckerei GmbH
- BvL.com GmbH
- CBT Systems & Services GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- CERTIX IT-Security GmbH
- CGM Deutschland AG
- Cherry Digital Health GmbH
- CHIFFRY GmbH
- COGNITUM Software Team GmbH
- COMback Holding GmbH
- comcrypto GmbH
- comforte AG
- Communisystems-Care GmbH
- comtime GmbH
- Condition-ALPHA Digital Broadcast Technology Consulting
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- Crashtest Security GmbH
- Cybersense GmbH
- dacoso data communication solutions GmbH
- dal33t GmbH
- DATAKOM GmbH
- datenschutzklinik
- DATUS AG
- DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
- DELIT AG
- DERMALOG Identification Systems GmbH
- Detack GmbH
- Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG
- DF Deutsche Fiskal GmbH
- DFN-CERT Services GmbH
- Digital Enabling GmbH
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- dinext. pi-sec GmbH
- Dirk Losse Consulting
- ditis Systeme Niederlassung der JMV GmbH & Co.
- DoctorBox GmbH
- DRACOON GmbH
- Dreyfield & Partner Deutschland GmbH
- DriveLock SE
- D-Trust GmbH
- EBRAND AG
- e-ito Technology Services GmbH
- eCom Service IT GmbH
- ecsec GmbH
- Edvation GmbH
- EgoMind GmbH
- enclaive GmbH
- Enginsight GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- essentry GmbH
- evolutionQ GmbH
- Exploit Labs GmbH
- FAST LTA GmbH
- FP Digital Business Solutions GmbH
- FSP GmbH
- FZI Forschungszentrum Informatik
- G DATA CyberDefense AG
- genua GmbH
- GORISCON GmbH
- Hanko GmbH
- HDPnet GmbH
- HiScout GmbH
- HK2 Rechtsanwälte
- Hornetsecurity GmbH
- IDEE GmbH
- if(is) - Institut für Internet-Sicherheit
- Infineon Technologies AG
- INFODAS GmbH
- Inlab Networks GmbH
- inlyse GmbH
- INNOSYSTEC GmbH
- innovaphone AG
- Insentis GmbH
- INSYS MICROELECTRONICS GmbH
- intarsys GmbH
- intelliCard Labs GmbH
- IS4IT KRITIS GmbH
- isits AG International School of IT Security
- ISL Internet Sicherheitslösungen GmbH
- ITConcepts PSO GmbH
- ITnovate UG
- ITSG GmbH

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

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

Die Liste der zertifizierten Unternehmen wächst stetig. Die aktuelle Liste können Sie einsehen unter: www.teletrust.de/itsmig/zeichentraeger □

- itWatch GmbH
- keepbit IT-SOLUTIONS GmbH
- KikuSema GmbH
- KnowledgeRiver GmbH
- KOPRAX Systemhaus GmbH & Co. KG
- KraLos GmbH
- Kroll Strategieberatung GmbH
- LANCOM Systems GmbH
- LEIBOLD Sicherheits- und Informationstechnik GmbH
- limes datentechnik gmbh
- Linogate GmbH
- LocateRisk UG
- maincubes Holding & Service GmbH
- MaskTech GmbH
- Matrix42 AG
- Mentana Claimsoft GmbH
- metafinanz GmbH
- MGR Integration Solutions GmbH
- MH-IT + Service GmbH
- M&H IT-Security GmbH
- MTG AG
- MTRIX GmbH
- Mühlbauer ID Services GmbH
- MY-CAMP GmbH
- NCP engineering GmbH
- Neosec GmbH
- NetComProtect
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- Nexis GmbH
- NG Guard Technology GmbH
- nicos AG
- nicos cyber defense GmbH
- Nimbus Technologieberatung GmbH
- OctoGate IT Security Systems GmbH
- ondeso GmbH
- ONEKEY GmbH
- Opexa Advisory GmbH
- OPTIMAbit GmbH
- OTARIS Interactive Services GmbH
- O&O Software GmbH
- P3KI GmbH
- pen.sec AG
- PFALZKOM GmbH
- PHOENIX CONTACT Cyber Security GmbH
- PHYSEC GmbH
- Pix Software GmbH
- PPI Cyber GmbH
- Primary Target GmbH
- procilon GmbH
- ProLog GmbH
- PSW GROUP GmbH & Co. KG
- QGroup GmbH
- QuoIntelligence GmbH
- real-cis GmbH
- Relution GmbH
- Resility GmbH
- retarus GmbH
- RheinByteSystems GmbH
- Robin Data GmbH
- Rohde & Schwarz Cybersecurity GmbH
- r-tec IT Security GmbH
- SAMA PARTNERS Business Solutions GmbH
- sayTEC AG
- Schönhofer Sales and Engineering GmbH
- SCHUTZWERK GmbH
- SC-Networks GmbH
- Secorvo Security Consulting GmbH
- secrypt GmbH
- SECUDOS GmbH
- secunet Security Networks AG
- Secure Service Provision GmbH
- Securepoint GmbH
- SECURITYSQUAD GmbH
- secuvera GmbH
- sequrium GmbH
- SerNet GmbH
- signotec GmbH
- simsystem GmbH
- Skyflare GmbH
- SL.IS Services GmbH
- Smartify IT Solutions GmbH
- Softline AG
- SoSafe GmbH
- Spike Reply GmbH
- SRC Security Research & Consulting GmbH
- Steganos Software GmbH
- suresecure GmbH
- SVA System Vertrieb Alexander GmbH
- Synedat Consulting GmbH
- syracom consulting AG
- TDT AG
- TE-SYSTEMS GmbH
- Tech-Prax GmbH
- Tenzir GmbH
- TG alpha GmbH
- TKUC GmbH
- Trufflepig IT-Forensics GmbH
- TrustCerts GmbH
- TrustSpace
- TÜV Informationstechnik GmbH
- TÜV Rheinland i-sec GmbH
- TWINSOFT biometrics GmbH & Co. KG
- UMH Systems GmbH
- Uniki GmbH
- Uniscon GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- virtual solution AG
- VisionmaxX GmbH
- VMRay GmbH
- Voleatech GmbH
- Vulidity GmbH
- wintercloud GmbH & Co. KG
- WMC Wüpper Management Consulting GmbH
- Würzburger Versorgungs- und Verkehrs GmbH
- XignSys GmbH
- XnetSolutions KG
- zeroBS GmbH
- Zertificon Solutions GmbH

GEWINNEN SIE SOFORT:
VORTEILSAKTIONEN FÜR
IT-SECURITY-LÖSUNGEN AUF

SECUREPOINT.DE/WINTERRALLY

·O· SECUREPOINT


S GEBEN UND
ST MACHEN!
SECUREPOINT

Was zur Verteidigung gegen Cyberkriege getan werden muss

Während auf staatlicher Ebene wie der EU und auf militärischer Ebene wie der NATO der Schwerpunkt auf gemeinsame Information und Verteidigung gelegt wird, sind Unternehmen meist Einzelkämpfer, wenn es um Cyberattacken geht.

Von Dipl.-Phys. Oliver Schonschek

Gerade bei hochprofessionellen Angriffen im Cyberwar haben Unternehmen keine gute Ausgangslage zur Verteidigung. Die Forderungen nach Veränderung sind bereits da.

Nach den großen Ransomware-Wellen und den weitreichenden Veränderungen in den IT-Landschaften durch die COVID-Pandemie führen nun auch die geopolitischen Folgen des Ukraine-Kriegs dazu, dass viele Organisationen erneut Anpassungen an ihrer Cyberverteidigung vornehmen müssen, so die IDC-Studie „Cybersecurity in Deutschland 2022".

Bild: busra/stock.adobe.com

Fast die Hälfte der Organisationen plant demnach wegen der geopolitischen Folgen des Ukraine-Krieges eine Anpassung ihrer Cyberbereitschaft und -verteidigung. Doch das alleine wird nicht ausreichen; nicht nur, weil laut IDC 60 Prozent der deutschen Organisationen einen akuten Security-Fachkräftemangel haben oder erwarten. Auch an anderen Stellen – zum Beispiel der Politik – sind Veränderungen nötig.

Auch die Wirtschaft braucht einen erhöhten Schutz

Angesichts der veränderten geopolitischen Situation infolge des Ukraine-Krieges forderte der Bundesverband IT-Sicherheit TeleTrusT von Politik, Regulierern und Betreibern weitreichende IT-Sicherheitsmaßnahmen und Investitionen zur Verbesserung der nationalen Sicherheit und der Versorgungssicherheit. Cyberangriffe auf Unternehmen, staatliche Einrichtungen und kritische Infrastrukturen der Ukraine haben demnach gezeigt, dass kritische Infrastrukturen und industrielle Netzwerke zunehmend in den Fokus politisch motivierter Cyberattacken geraten.

Steffen Heyde, Leiter der TeleTrusT-AG „Smart Grids / Industrial Security", erklärte dazu: „Die neue geopolitische Lage, ausgelöst durch den Ukraine-Konflikt, ist Zäsur und Zeitenwende auch für die IT-Sicherheit in Deutschland. IT-Sicherheit ist ein entscheidender Pfeiler der nationalen Sicherheit und letztendlich Garant der Aufrechterhaltung von Versorgungssicherheit und des Funktionierens unserer Volkswirtschaft auch in Krisenzeiten."

TeleTrusT forderte daher eine engagierte nationale Kraftanstrengung von Politik, Regulierern und Betreibern zur Verbesserung der Cybersicherheit und der nationalen Sicherheit, insbesondere auch eine wirksame Absicherung der Industrieproduktion und digitaler Industrie-Netzwerke, einschließlich Logistik und Supply Chain.

Notwendig ist ein übergreifendes Lagebild

Der Bundesverband IT-Sicherheit blieb dabei aber nicht stehen und forderte sofortige Lageberichte zu Cyberangriffen. Der Grund: Die Wirkungen und in der Regel auch Ursachen von herkömmlichen Angriffen sind für die Welt – mit Einschränkungen – berichtsfähig und überprüfbar. Cyberangriffe sind für die Bevölkerung innerhalb und außerhalb der Ukraine jedoch nicht oder nicht ohne Weiteres zeitlich, örtlich, technisch oder hinsichtlich ihrer sonstigen Wirkmächtigkeit einschätzbar oder auch nur wahrzunehmen, so TeleTrusT. Selbst IT-Sicherheitsfachleute könnten häufig nicht sicher ermitteln, welche Personen, Gruppierungen, Staaten oder Bündnisse an Cyberattacken oder an Cyberabwehrmaßnahmen beteiligt sind. Das betrifft auch die Motivlagen, konkrete Maßnahmenzwecke sowie direkte und indirekte Risiken von Maßnahmen.

Um ein aktuelles Bild von Cyberangriffen und -risiken zeichnen zu können, sind Unternehmen deshalb in besonderem Maße auf Angaben (nicht-russischer) Regierungen, der zuständigen Behörden und der Bündnispartner angewiesen. Das gibt es bislang nicht, weder auf nationaler, noch internationaler Ebene, wie der Bundesverband IT-Sicherheit beklagte. „Die Informationslage ist frappierend schlecht. Die Cybersicherheitslage wird aber in radikal zunehmendem Tempo das Vertrauen in unsere Wehrfähigkeit, unsere politische Strategie in kriegerischen Situationen und unsere Souveränität beeinflussen. Das scheint bislang in kaum jemandes Blick“, sagte Karsten Bartels, stellvertretender TeleTrusT-Vorstandsvorsitzender.

Was Marktforscher in Zukunft erwarten

Marktforschungshäuser wie Gartner haben sich damit befasst, wie die Unternehmen wohl in Zukunft auf Entwicklungen wie Cyberwar reagieren werden oder sollten. Zentrale Aussagen sind dabei:

- Es ist wahrscheinlich, dass Cyberbedrohungen mindestens so lange andauern werden wie der physische Konflikt. Der „Nebel des Krieges“ kann das Situationsbewusstsein herausfordern, und Panik erhöht das Risiko von Fehlern und schafft eine vorteilhafte Situation für die angreifenden Akteure. Während die Auswirkungen einzelner Angriffe unterschiedlich sein werden, werden die breiteren Auswirkungen einer erhöhten Bedrohungsumgebung weltweit zu spüren sein.
- Cyberkonflikte sind nicht nur ein Sicherheitsproblem, sondern auch ein Geschäftsproblem.

Bild: TeleTrusT

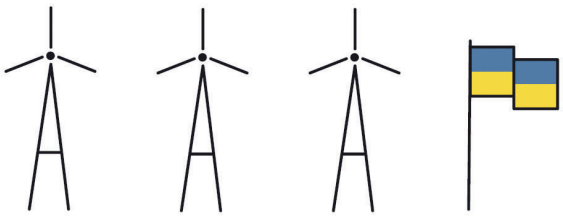
Karsten Bartels, stellvertretender TeleTrusT-Vorstandsvorsitzender: „Die Cybersicherheitslage wird in radikal zunehmendem Tempo das Vertrauen in unsere Wehrfähigkeit, unsere politische Strategie in kriegerischen Situationen und unsere Souveränität beeinflussen.“

Die Anzahl der Schadprogramme steigt stetig.
Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:
Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden
nach Angriff auf Satelliten-kommunikation



20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

Bild: BSI

Der Ukraine-Krieg hat auch konkrete Auswirkungen auf Unternehmen, teilt das Bundesamt für Sicherheit in der Informationstechnik mit.

Da ihre Auswirkungen weiter zunehmen, erfordern sie eine stärkere strategische Beteiligung der Unternehmensführung auf allen Ebenen.

- Geopolitik und Cybersicherheit sind untrennbar miteinander verbunden. Daher müssen Sicherheitsverantwortliche die globale Bedrohungslandschaft aus geschäftlicher Sicht betrachten. Jede in dieser Umgebung getroffene Geschäftsentscheidung hat Auswirkungen auf die Sicherheit und umgekehrt.
- Die russische Invasion in der Ukraine ist die jüngste Krise, die zeigt, dass Unternehmenssicherheit und -risiken vom CISO und seinem Team nicht im luftleeren Raum verwaltet werden können. Führungskräfte, die vertretbare, risikobewusste Entscheidungen treffen, steuern ihre Organisationen mit größerer Wahrscheinlichkeit mit Resilienz, von der Reaktion bis zur Wiederherstellung.

Cyberwar ist auch ein Unternehmensrisiko

Es zeigt sich: Cyberwar sollte spätestens jetzt auch als Unternehmensrisiko verstanden werden, nicht nur als militärisches Risiko. Alleine werden Unternehmen jedoch mit diesen Risiken überfordert sein, sie brauchen noch mehr Unterstützung durch die Sicherheitsbehörden und auch über die Unternehmensverbände, die an den gemeinsamen Lagebildern mitwirken könnten. □

Mit Managed EDR Made in Germany dem Fachkräftemangel in der IT-Sicherheit begegnen

Haben Unternehmen zu wenig Personal für IT-Sicherheit, geraten sie schnell in ernste Schwierigkeiten. Fast 50 Prozent der Firmen können dadurch keine angemessene Risikobewertung durchführen und diese nicht managen, weil die Zeit dafür fehlt (Quelle (ISC)[2]). Aufgaben rund um Security und IT werden daher auch zunehmend mit externer Hilfe erledigt. In 45 Prozent der Unternehmen kümmert sich ein Dienstleister um die IT und damit auch um die IT-Sicherheit. Allerdings stieg innerhalb von sieben Jahren der Anteil der Firmen, in denen sich sowohl interne Mitarbeitende als auch externe Anbieter darum kümmern (Quelle Destatis).

Die Zusammenarbeit mit erfahrenen Dienstleistern ist für Unternehmen sehr wertvoll, denn sie sind oft nicht in der Lage, sich allein um ihre Cybersicherheit zu kümmern. G DATA unterstützt IT-Teams mit einem leistungsstarken und effektiven Portfolio aus Lösungen, Dienstleistungen und Security Awareness Trainings „Made in Germany“.

Managed EDR aus Deutschland

IT-Sicherheit ist eine Rund-um-die-Uhr-Aufgabe, denn Angriffe finden auch außerhalb der Arbeitszeit statt. Eine umgehende Reaktion ist dabei essenziell, um Schäden zu minimieren. Allerdings haben Unternehmen oft nicht die Möglichkeit, diese zu leisten, weil Ressourcen, Personal und Know-how fehlen. Bei Managed EDR von G DATA CyberDefense überwachen gut ausgebildete IT-Security-Fachleute alle Aktivitäten auf den IT-Systemen und stoppen Cyberangriffe – egal zu welcher Uhrzeit. Das Analyseteam ist 24 Stunden täglich, an sieben Tagen in der Woche im Einsatz und wertet

G DATA CyberDefense

TRUST IN GERMAN SICHERHEIT

die Ergebnisse der Sensorik aus. Identifizieren die Experten von G DATA einen Angriff, analysieren sie diesen genaustens und reagieren umgehend – zum Beispiel mit der Separierung eines betroffenen Endpoints oder eines Dienstes. Unternehmen werden zudem über den Vorfall informiert. Sollte eine Mitwirkung durch die eigene IT-Abteilung nötig sein, geben die Experten von G DATA klare Handlungsempfehlungen.

Unternehmen profitieren beim Einsatz der gemanagten EDR-Lösung von der über 38-jährigen Erfahrung und dem Know-how des deutschen Cyber-Defense-Spezialisten. G DATA ist zudem zertifizierter APT-Response-Dienstleister und hat die Managed-EDR-Lösung selbst entwickelt. Hierdurch können die Ergebnisse der Sensorik zuverlässig gedeutet werden. Mitarbeitende in Unternehmen können sich ihren Kernaufgaben widmen, während G DATA die IT-Systeme überwacht und Angriffsversuche stoppt. Der deutschsprachige und kostenfreie 24/7-Support unterstützt bei Fragen und Problemen. Das Analyseteam ist ebenfalls am Unternehmensstandort in Bochum ansässig. Ein weiterer Vorzug der Dienstleistung: Die verarbeiteten Daten verbleiben ausschließlich in Deutschland auf den Servern des strategischen Partners IONOS in Frankfurt am Main und Berlin sowie auf den unternehmenseigenen Servern von G DATA am Bochumer Unternehmensstandort. Damit unterliegen die Informationen den strengen deutschen Datenschutzgesetzen und der EU-Datenschutzgrundverordnung.

G DATA Workshops auf der it-sa 2023

Auf der it-sa ist G DATA nicht nur mit einem Stand 210 in Halle 7 präsent, sondern veranstaltet auch drei kostenlose Workshops zu aktuellen Cybergefahren und Abwehrmaßnahmen. Im Workshop „IT-Security über die Cloud: Was bringen „managed“ und „as-a-Service“-Produkte?“ zeigen Stefan Hausotte (Head of Threat Intelligence & Infrastructure, G DATA CyberDefense), Florian Kuckelkorn (Head of OEM Solutions, G DATA CyberDefense) und Tobias Becker (Senior Partner Cloud Solutions Architect, IONOS) am 10. Oktober 2023 von 14.30 bis 16 Uhr im Live-Hacking, wie Angreifer in IT-Systeme einbrechen und wie ein gesamtheitliches Verteidigungskonzept davor schützt. ■

Work Anywhere: IT, Nutzende und Daten sind überall

Homeoffice und Remote Work klangen früher nach Ausnahmesituationen, die meiste Arbeitstätigkeit fand im Unternehmen selbst statt. Inzwischen aber ist aus Remote Work das neue Arbeitsmodell Work Anywhere geworden. Es ist deshalb höchste Zeit, bestehende Sicherheitsmodelle in Richtung Security Anywhere zu entwickeln.

Von Dipl.-Phys. Oliver Schonschek

Geopolitische Unsicherheiten, steigende Energiepreise, die Inflation und der stetig zunehmende Fachkräftemangel üben Druck auf die Unternehmen aus, ihre Arbeitsplatzmodelle zu transformieren, so das Marktforschungshaus IDC: Kaum ein Unternehmen steht erst am Anfang, allerdings haben auch erst wenige die Transformation vollständig vollzogen. Die Umsetzung ist ein unter Umständen aufwendiger Prozess, und die Realisierung umfasst viele Facetten.

62 Prozent der deutschen Unternehmen setzen laut IDC künftig auf hybride Arbeitsplatzmodelle, im Jahr 2021 waren es lediglich 36 Prozent. Budgetbeschränkungen und hohe Anschaffungskosten von IT bremsen die Transformation des Arbeitsplatzes jedoch zunehmend und spürbar aus. 3 von 4 Unternehmen wollen mit Schulungen und Zufriedenheitsanalysen die Arbeitskultur verbessern – die Mitarbeiterzufriedenheit rückt stärker in den Fokus.

Bild: stockyme/stock.adobe.com

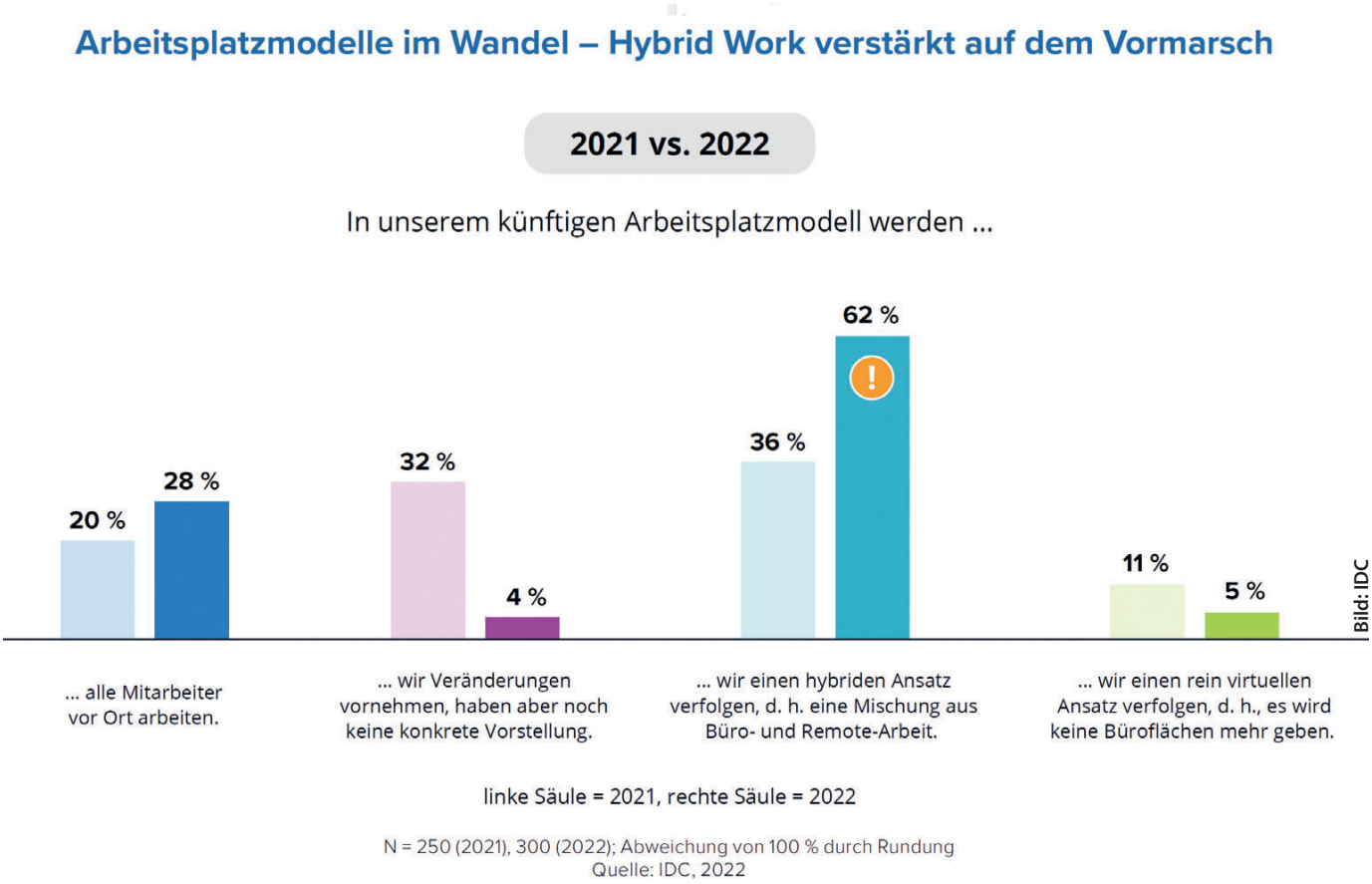
IT-Sicherheit wird als Hemmnis gesehen

30 Prozent der Unternehmen beklagen jedoch den Spagat zwischen Flexibilität und IT-Sicherheit. Zudem gibt es Bedenken in Bezug auf Datenschutz und Compliance (20 Prozent) und allgemeine Sicherheitsbedenken (20 Prozent). Sicherheitsrisiken wurden bereits zu Beginn der Corona-Pandemie beklagt. So berichtete der Verband der IT-Sicherheit TeleTrusT: „Während technisch gut aufgestellte Unternehmen ihre Mitarbeiter mit professionellem Equipment ausrüsten, ist anderswo Improvisation und Pragmatismus gefragt. Dabei kann die IT-Sicherheit auf der Strecke bleiben. Gerade jetzt aber schwärmen digitale Raubritter aus, um die Gunst der Stunde zu nutzen und mit Spam, Phishing, Malware, Identitätsdiebstahl und Datenklau schnelle Beute zu machen."

Leider hat sich die Situation in den letzten Monaten und Jahren nicht verbessert, im Gegenteil. „Die Bedrohungslage im Cyber-Raum ist angespannt, dynamisch und vielfältig und damit so hoch wie nie", so der Vizepräsident des BSI, Dr. Gerhard Schabhüser, mit Blick auf den Bericht zur Lage der IT-Sicherheit in Deutschland 2022 des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Sicherheitsrisiken steigen, Arbeit wird noch mobiler und flexibler

Nicht nur die Bedrohungslage verschärft sich: Auch die in der Corona-Pandemie beschleunigte Entwicklung hin zu Homeoffice und Remote ⇨



62 Prozent der deutschen Unternehmen setzen laut IDC künftig auf hybride Arbeitsplatzmodelle, im Jahr 2021 waren es lediglich 36 Prozent.

Work verstärkt und wandelt sich weiter. So berichtet der Digitalverband Bitkom: Mit dem Laptop unter Palmen sitzen, den Kunden-Call in den Bergen machen, in vielen Branchen ist im Zuge der Corona-Pandemie flexibles und ortsunabhängiges Arbeiten fernab der Fünftagewoche im Büro selbstverständlich geworden. Eine steigende Anzahl an Beschäftigten will dies auch aus dem Ausland tun. Zudem werden mit der flexibleren Arbeit auch Klimaziele verbunden, die für Unternehmen und Beschäftigte eine immer größere Relevanz erlangen. 74 Prozent sagen, dass Homeoffice in Deutschland allgemein noch sehr viel stärker genutzt werden sollte. 85 Prozent sagen, Homeoffice kann den Verkehr reduzieren und damit auch das Klima entlasten, so der Digitalverband Bitkom.

Work from Anywhere als neues Normal gewünscht

Der Bundesverband Digitale Wirtschaft (BVDW) e. V. hat in einer bevölkerungsrepräsentativen Umfrage untersucht, wie sich die Arbeitswelt durch die Corona-Pandemie verändert hat. Dabei wurden sowohl unterschiedliche Wahrnehmungen von Mitarbeitern und Führungskräften als auch von Unternehmen der digitalen Wirtschaft und klassischen Unternehmen gegenübergestellt. „Die Studie zeigt deutlich, dass sich die Vorstellungen von Mitarbeitern und Führungskräften unterscheiden“,

so BVDW-Vizepräsidentin Anna Kaiser. Nur 25 Prozent der Mitarbeiter möchten zum Präsenzmodell zurückkehren, die meisten der befragten Mitarbeiter sind sich darin einig, dass sie überwiegend ein flexibles Modell bevorzugen. Beim flexiblen Modell entscheiden Arbeitnehmer selbst, wo sie über welchen Zeitraum arbeiten: von 100 Prozent Homeoffice bis zu 100 Prozent Präsenzzeit im Büro ist alles möglich.

Work from Anywhere gegen den Fachkräftemangel

Nicht nur IT-Unternehmen suchen nach Strategien, Fachkräfte für sich zu begeistern. Entsprechende New-Work-Konzepte sind seit der Corona-Pandemie auch im Mittelstand angekommen. Mobiles Arbeiten und flexible Arbeitszeiten sehen viele Beschäftigte als selbstverständlich an.

„In der Pandemie haben viele Unternehmen begonnen, vorhandene New-Work-Konzepte weiter zu denken", sagte Lucia Falkenberg, CPO und Sprecherin der Kompetenzgruppe New Work im eco – Verband der Internetwirtschaft e. V. „Immer mehr Mitarbeiter:innen arbeiten zeitweise aus dem Ausland oder gar nur noch 4 Tage die Woche. Entsprechende Arbeitskonzepte setzen sich bei großen Internetkonzernen durch. Der Trend geht zu Work-Life-Blending, das heißt Berufliches und Privates stärker zu vermischen. So wird auch nach Feierabend in die Mails geschaut oder mit den Kolleginnen ein geselliger Abend verbracht." Die Vermischung von Arbeit und Privatleben bleibt aber nicht ohne Folgen für die IT-Sicherheit.

Die Folge für die IT-Sicherheit: Kein Standort kann als sicher gelten

Wenn aber die Mitarbeiterinnen und Mitarbeiter in Zukunft selbst entscheiden, wo sie arbeiten möchten, dieser Wunsch in Zeiten des Fachkräftemangels auch respektiert werden sollte und Arbeit und Freizeit immer mehr vermischt werden, kann dies nur bedeuten: Man kann als Unternehmen nicht mehr davon ausgehen, dass es einen sicheren Arbeitsort gibt, vielmehr muss die Sicherheit überall gewährleistet werden.

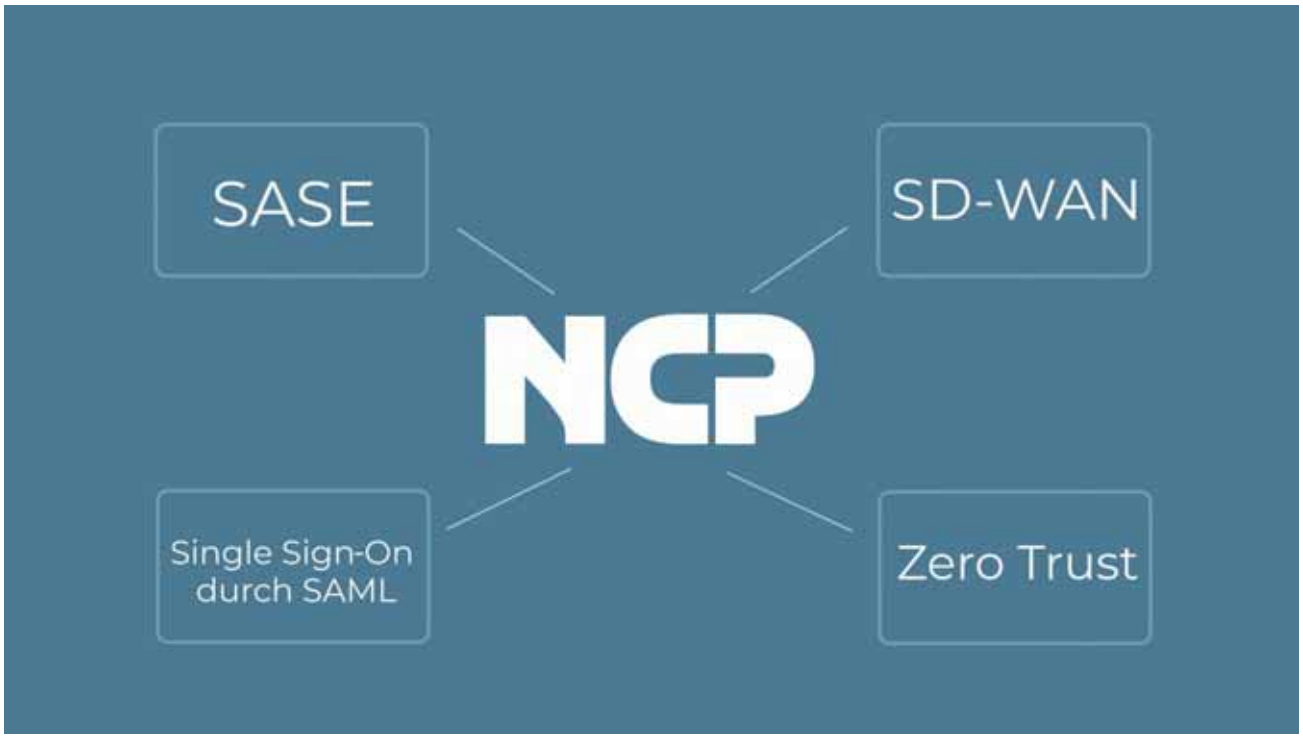
Work from Anywhere bedingt also Security Anywhere. Eine solche Security, die keinen Standort ungeprüft als sicher annimmt, folgt dem Zero-Trust-Gedanken. Einfach gesagt, bedeutet Zero Trust, dass man keiner IT-Komponente mehr ungeprüft trauen soll, keinem Rechner und keiner Anwendung – ganz gleich, ob die IT extern oder intern ist. □

Status der IT-Sicherheit im Homeoffice nach der Pandemie (Quelle: TeleTrusT)

- Homeoffice und Remote Work sind gekommen, um zu bleiben.
- Die aktuelle Arbeitswelt verändert sich parallel rasant. Menschen arbeiten in Projekten von überall auf der Welt mit ihrem Equipment.
- Mehr Homeoffice führt zu mehr Client-to-Site-VPN und somit zur Schwachstelle in der Unternehmens-IT (offene Tore für Schadsoftware-Angriffe).
- Homeoffice führt zur Zunahme von Virtualisierung/RDP, gleichzeitig stellt sich Windows RDP als anfällig für Cyberangriffe dar.
- Marktbeherrschende Lösungen wie VPN sind heute ein unzureichender Standard für die Herausforderungen.
- Der Aufwand (Kosten) und die Dauer, um Heim-Arbeitsplätze zu integrieren und zu administrieren, stehen in keinem Verhältnis zu heutigen Anforderungen (Realtime).
- Bring-Your-Own-Device (BYOD) ist gewünscht und gefordert, technisch aber kaum und nur sehr aufwendig umsetzbar.

Warum modernes VPN bei Zero Trust den entscheidenden Unterschied macht!

Neue Cloud-Konzepte und -Technologien wie Zero Trust, SD-WAN, SASE und Single Sign-On sollen steigenden Cyberangriffszahlen den Kampf ansagen. Vor allem das zugriffsbasierte Zero-Trust-Konzept kommt bei immer mehr Unternehmen zum Einsatz. Doch auch solche Cloud-Ansätze lassen sich noch optimieren – und zwar durch die Kombination mit einer zeitgemäßen VPN-Lösung. Wie funktioniert das?



Technische Ausrichtung & Kompatibilität

Wer Zero Trust in seinem Unternehmen einsetzt, arbeitet nach dem „Least privilege"-Prinzip, bei dem Nutzer nur Zugriff auf für sie relevante Anwendungen haben. Fortschrittliche VPNs wie die Secure-Enterprise-Produkte von NCP funktionieren bereits seit Jahren nach diesem technischen Prinzip: Per zentraler Management-Komponente wie dem NCP Secure Enterprise Management (SEM) definieren Administratoren alle Zugriffsrechte mit wenig Zeitaufwand und können auf diese Weise sogar Policies und Updates an alle Nutzer gleichzeitig verteilen. Außerdem muss die VPN-Lösung alle Technologien und Standards wie SASE, SD-WAN und SSO durch SAML unterstützen, um überhaupt ins entsprechende Konzept zu passen.

Dafür setzen Unternehmen am besten auf Lösungen wie die Enterprise-VPN-Produkte von NCP, die 100% softwarebasiert arbeiten und sich dadurch nahtlos in jede Security-Umgebung einfügen.

Unverzichtbare Security-Features

In der Praxis machen nicht zuletzt Features wie der NCP VPN-Bypass oder Application Based Tunneling den Unterschied, die datenhungrigen Traffic ohne Sicherheitsrelevanz am Tunnel vorbeileiten und so den Server entlasten. Für die Sicherheit des gesamten Netzes sind auch Endpoint Policy Checks unerlässlich, die unsicheren Endgeräten automatisch den Zugriff verweigern. Zeitgemäßes VPN kann daher als wertvoller Baustein in einem Zero-Trust-Konzept den Security-Faktor um ein Vielfaches steigern. ■

Wie Ihr Sicherheitskonzept das nächste Level erreicht, erfahren Sie am NCP-Stand (Halle 7A, Stand 412) auf der it-sa 2023 oder auf unserer Webseite unter **www.ncp-e.com**.

Digitale Identitäten als Schlüssel zur Cloud

Identity and Access Management (IAM) ist von grundlegender Bedeutung bei der Nutzung jedes IT-Systems. Darüber werden Zugang und Zugriffsrechte gesteuert. Das ist bei Cloud Computing nicht anders. Aber Cloud-Identitäten und Cloud-Berechtigungen selbst haben ihre Besonderheiten, die es zu beachten gilt. Bislang haben Unternehmen häufig noch Probleme bei der Verwaltung und Absicherung von Identitäten und Berechtigungen in der Cloud.

Von Dipl.-Phys. Oliver Schonschek

Bild: Treecha/stock.adobe.com

Wenn sich Unternehmen bisher nicht im Klaren darüber waren, dass digitale Identitäten und Berechtigungen bei Cloud-Services eine besondere Herausforderung darstellen können, dann haben sie dies in Zeiten der Pandemie schnell lernen müssen. Lösungen für das IAM, die im Unternehmensnetzwerk seit Jahren funktioniert haben, konnten nicht einfach in die Cloud übertragen werden. Aber die Beschäftigten mussten nun aus den Homeoffices heraus auf Cloud-Dienste zugreifen, mit ihren digitalen Identitäten und mit den passenden Berechtigungen. Die Folgen waren uneinheitliche Lösungen für die Identitäten und oftmals viel zu weitreichende Berechtigungen in der Cloud.

Warum aber sind Identitäten und Berechtigungen in der Cloud so eine Herausforderung? Der Grund ist: Die Verwaltung und Prüfung der Identitäten und die Zuordnung der Privilegien zu den Identitäten müssen nicht nur im Unternehmen selbst erfolgen, sondern bei allen Stellen, die an der Erbringung des Cloud-Dienstes entsprechend beteiligt sind. Zudem nutzen Unternehmen häufig verschiedene Cloud-Anbieter parallel, verfolgen also den Multi-Cloud-Ansatz. Das Cloud-IAM ist entsprechend weit verteilt und komplex. Nicht zuletzt ist die Kommunikation zur Übertragung der Identitätsdaten bei der Cloud-Anmeldung den Risiken von Cyberattacken ausgesetzt, sie muss also entsprechend geschützt werden.

Herausforderungen der Cloud-Identitäten

Marktforscher wie Forrester Research haben die Probleme eines IAM für die Cloud so dargestellt:

- Zugriffskontrollen in Cloud-Plattformen sind kompliziert: Da es keinen gemeinsamen Rahmen oder Ansatz gibt, variieren die Zugriffskontrollrichtlinien zwischen den Anbietern.
- Clouds stellen zu viele Privilegienherausforderungen dar: Problematisch ist die schiere Anzahl an Zugriffsmodellen, die Cloud-Dienste bieten. Es ist zwar möglich, granulare Privilegien für Tausende von Rollen festzulegen, aber die Kehrseite ist, dass dies oft zu übermäßigen Zugriffsrechten führt. Erschwerend kommt hinzu: Temporäre Cloud-Konfigurationen, die laxe Kontrollen verwenden und auf eine schnelle Entwicklung ausgelegt sind, erhöhen das Risiko.

Risiken der Cloud-Identitäten

Nicht nur die Verwaltung und Kontrolle der Cloud-Identitäten ist erschwert, auch die Absicherung. Die Anmeldung zu den Cloud-Diensten erfolgt in der Regel über das Internet, hier könnten die Zugangsdaten abgefangen werden (mittels Phishing-Attacken). Da bei vielen Cloud-Anbietern eine Mehr-Faktor-Authentifizierung noch optional ist, erhält der Passwortdieb dann den Schlüssel zu dem Cloud-Dienst mit allen Berechtigungen des Opfers.

Wie wichtig die Sicherheit der Cloud-Identitäten ist, zeigt auch der Bericht „Top Threats to Cloud Computing: Pandemic 11“ der Cloud Security Alliance (CSA): Während es ein Jahr zuvor noch Platz 4 unter den Top-Cloud-Risiken war, liegt nun „Insufficient identity, credential, access and key management“ auf Platz 1. „Insgesamt sind diese Sicherheitsprobleme ein Aufruf zum Handeln für die Entwicklung und Verbesserung des Cloud-Sicherheitsbewusstseins, der Konfiguration und des Identitätsmanagements“, sagte Jon-Michael C. Brook, Co-Vorsitzender der Top Threats Working Group und einer der Hauptautoren des CSA-Papiers.

Der Weg zu sicheren und nutzerfreundlichen Cloud-Identitäten

In Zeiten der Pandemie und Homeoffice-Pflicht mussten Lösungen für ein IAM, das auch für die Cloud genutzt werden kann, sehr schnell gefunden werden. Entsprechend waren die Ergebnisse mitunter nicht sicher genug und sehr ⇨

oft nicht komfortabel für den Nutzenden. Doch die Zeit der temporären Lösungen, die mit „heißer Nadel“ gestrickt wurden, sollte nun vorbei sein. Nun sollten Konzepte erstellt werden, wie sich IAM für die Cloud richtig einführen lässt. Hierfür gibt es zahlreiche Empfehlungen und Hinweise von Fachstellen.

Was die CSA den Unternehmen rät

Die Cloud Security Alliance (CSA) befasst sich regelmäßig mit dem Thema IAM und Cloud Computing, alleine schon wegen der Bedeutung der Cloud-Identitäten für die Cloud Security. Zu den wichtigsten CSA-Empfehlungen zählen:

- Der Aufbau eines zentralisierten Authentifizierungssystems für On-Premises und die (Multi-) Cloud ist nicht die Einführung neuer Software. Es ist die Einrichtung einer neuen Praxis. Geschwindigkeit sollte hier nicht die Priorität sein. Man sollte nicht versuchen, das System im Handumdrehen aufzubauen, sondern Schritt für Schritt.
- Der Beginn ist eine Bestandsaufnahme aller Informationssysteme, um die Möglichkeiten ihrer Integration mit IAM-Lösungen zu bewerten.
- Das Ziel sollten SSO (Single-Sign-On) und MFA (Mehr-Faktor-Authentifizierung) sein.
- Neben der Implementierung von Single-Sign-On darf auch Single-Logout nicht fehlen.
- Es werden verschiedene Authentifizierungsszenarien benötigt in Abhängigkeit von Benutzertypen, dem verwendeten Gerät, dem Standort des Benutzers und der Art der Anwendung.
- Anstatt Benutzerinformationen in verschiedenen Repositories zu speichern, sollten Unternehmen erwägen, ein einziges Benutzerverzeichnis zu erstellen.
- Beim Aufbau eines zentralisierten Authentifizierungssystems müssen Unternehmen ihre Computersysteme anpassen. Die häufigste Verbesserung besteht darin, die Authentifizierungsprotokolle SAML, OAuth 2.0 und OpenID Connect zu unterstützen.

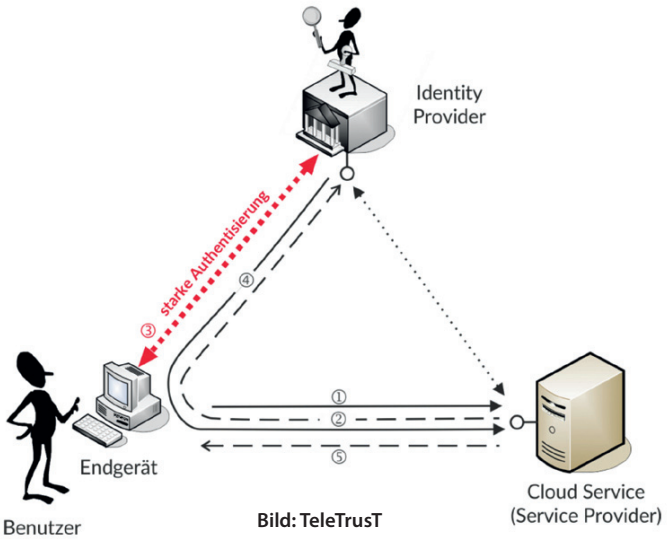
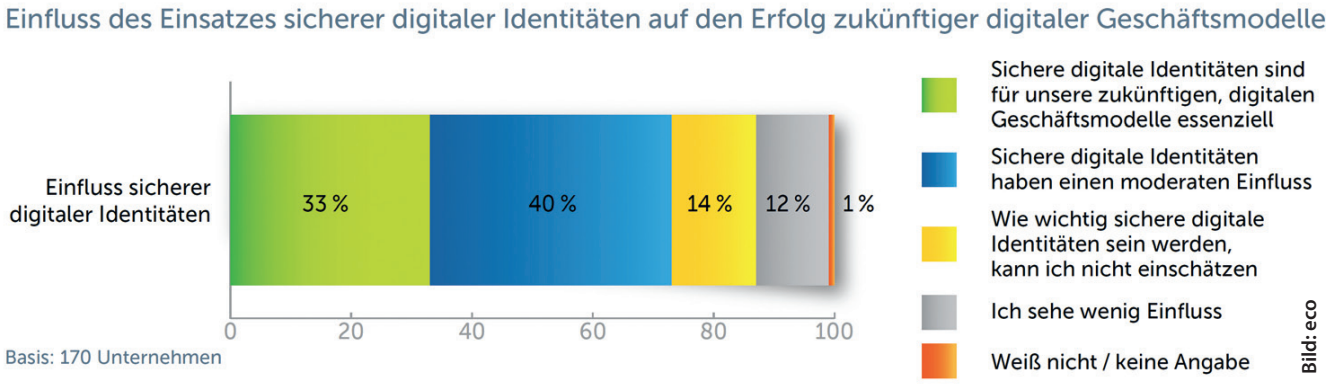


Bild: TeleTrusT

Um den Prozess der starken Authentifizierung von den einzelnen Cloud-Services zu entkoppeln, empfiehlt sich der Einsatz eines spezialisierten Identity Providers.

Verwendung eines Identity Providers

Der Bundesverband IT-Sicherheit e.V. TeleTrusT hat sich ebenfalls zur Cloud-Sicherheit geäußert und dabei wichtige Hinweise zur Nutzung eines zentralen Identity Providers gegeben: Verfahren zur starken Authentifizierung (MFA) können im einfachsten Fall direkt in den einzelnen Cloud-Services integriert werden, doch ist der Aufwand zur Integration unterschiedlicher Authentisierungsmechanismen oftmals proportional zur Anzahl der unterstützten Verfahren. Um den Prozess der starken Authentifizierung von den einzelnen Cloud-Services zu entkoppeln, empfiehlt sich der Einsatz eines spezialisierten Authentisierungsdienstes (Identity Provider), der über standardisierte Protokolle für das föderierte Identitätsmanagement angesprochen werden kann. In diesem Fall erfolgt



Drei von vier Unternehmen sehen einen Einfluss sicherer, digitaler Identitäten auf ihren Geschäftserfolg ergab eine Umfrage von eco – Verband der Internetwirtschaft e.V.

nach dem Zugriff des Benutzers auf den Cloud-Service eine Umleitung des Benutzers zum Identity Provider, der die starke Authentifizierung des Benutzers im Auftrag des Cloud-Services mit einem sicherheitstechnisch geeigneten Verfahren durchführt und das Ergebnis der Authentifizierung in einer gesicherten Weise zum Cloud-Service zurückschickt, bevor der Benutzer im Erfolgsfall Zugriff erhält.

Damit die ausgelagerte Authentifizierung nicht missbraucht werden kann, müssen geeignete Sicherheitsmaßnahmen implementiert werden, die regelmäßig im Rahmen von geeigneten Zertifizierungsverfahren geprüft und zertifiziert werden. Soweit im Rahmen der starken Authentifizierung auch personenbezogene Daten verarbeitet werden, sind die Anforderungen der DSGVO (Datenschutz-Grundverordnung) zu berücksichtigen.

Sicherheitsstandards zur Cloud-Nutzung

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) behandelt den Bereich Identitäts- und Berechtigungsmanagement ausführlich im C5-Standard (Cloud Computing Compliance Criteria Catalogue). Aus Sicht der Cloud-Nutzenden lässt sich ableiten, dass Folgendes vorhanden sein sollte:

- ein auf den Geschäfts- und Sicherheitsanforderungen basierendes Rollen- und Rechtekonzept sowie eine Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen für interne und externe Mitarbeiter sowie für Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen innehaben;
- geregelte Verfahren für die Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen für interne und externe Mitarbeiter sowie für Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen innehaben;
- Zugangsberechtigungen interner und externer Mitarbeiter sowie von Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen innehaben, werden gesperrt, wenn diese über einen definierten Zeitraum nicht genutzt wurden;
- Zugriffsberechtigungen werden bei Änderungen im Aufgabengebiet der internen und externen Mitarbeiter zeitnah entzogen;
- Zugriffsberechtigungen interner und externer Mitarbeiter sowie von Systemkomponenten, die eine Rolle in automatisierten Autorisierungsprozessen innehaben, werden regelmäßig daraufhin überprüft, ob diese noch dem tatsächlichen Aufgaben- bzw. Einsatzgebiet entsprechen. □

ENGINSIGHT

MEHR SICHERHEIT
MEHR KONTROLLE

mit der All-in-One Cybersecurity-Software, Made in Jena.

+ Ihr System zur Angriffserkennung (SzA)
+ Konzipiert für den deutschen Mittelstand
+ KRITIS-/NIS2-ready

Automatisierte Pentests
Schwachstellen-Scans
Konfigurations-Checks
IT-Monitoring
Eventlog-Analyse
Intrusion Detection
Intrusion Prevention
Mikrosegmentierung

Datacenter sind kritische Infrastruktur

Das Akronym KRITIS für kritische Infrastrukturen gibt es zwar schon länger in Deutschland, aber lange Zeit schien es eher Palliativum statt Energetikum zu sein. Spätestens seit dem Angriffskrieg der Russischen Föderation gegen die Ukraine hat sich auch da viel geändert. Nicht zuletzt für Rechenzentren.

Von Jürgen Höfling

Die (hoffentlich) hinter uns liegenden Pandemie-Zeiten sollten es auch einer breiten nichtfachlichen Öffentlichkeit deutlich gemacht haben: Rechenzentren gehören zur kritischen Infrastruktur. Ein Ausfall dieses digitalen Rückgrats hätte sehr weitreichende Folgen für die lokale und globale Wirtschaft und Gesellschaft. Folgerichtig unterliegen Rechenzentren ab einer bestimmten Leistung (derzeit ab 3,5 MW) der einschlägigen EU-weiten und nationalen Gesetzgebung. Derzeit zählen rund 1.600 Rechenzentren in Deutschland zu diesem kritischen Kreis.

Bild: Gorodenkoff/stock.adobe.com

Dass sich dieser Kreis in Zukunft noch deutlich erweitern wird, ist nicht ausgeschlossen. Neben der Kennzahl 3,5 MW gibt es noch weitere Kennzahlen wie beispielsweise die Marke „10.000 physische oder 15.000 virtuelle Instanzen“, die in einem Rechenzentrum verarbeitet werden. Auch ist bisher in den Gesetzen nicht genau definiert, wie beispielsweise Verbünde von Vor-Ort-Rechenzentren (Edge) und dem zentralen Rechenzentrum zu bewerten sind. Beispiele für einschlägige Gesetze sind auf EU-Ebene die Direktiven NIS2 (Netzwerk- und Informationssicherheit) und RCE / CER (Resilience of Critical Entities), auf nationaler deutscher Ebene das IT-Sicherheitsgesetz (IT-SIG) 2.0 und demnächst 3.0 sowie das neue KRITIS-Dachgesetz, des Weiteren viele Verordnungen und Ausführungsgesetze, zum Beispiel die KRITIS-Verordnung (KritisV) sowie Umsetzungspläne für die Sicherheit kritischer Infrastrukturen (UP KRITIS). Letztere wurden schon in den Nullerjahren in Deutschland etabliert.

203 Milliarden Euro Schaden in 2022

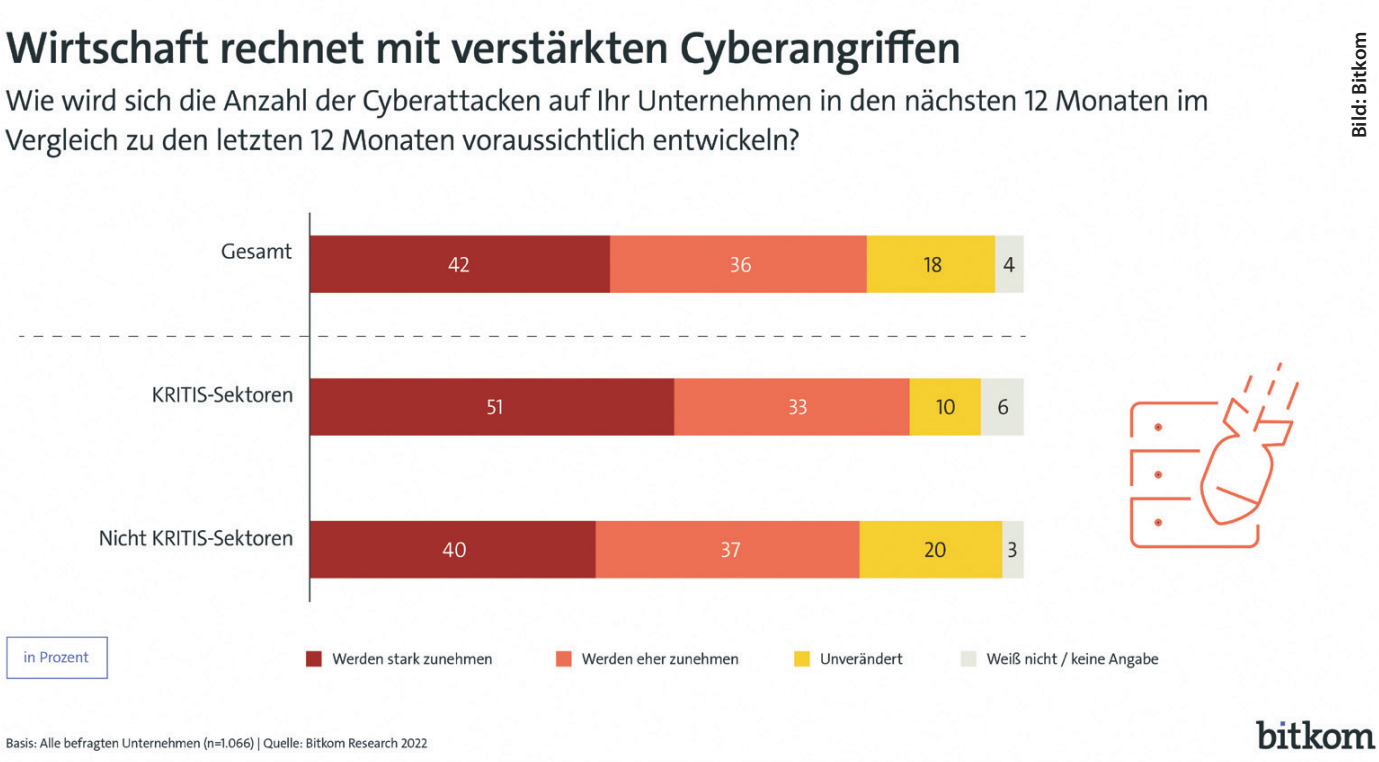
Dass die gesetzliche „Einrüstung“ notwendig und letztlich von den Unternehmen und Rechenzentrumsbetreibern mitgetragen wird, zeigt die Bitkom-Studie zum Thema Wirtschaftsschutz aus dem letzten Jahr. Danach entstand der deutschen Wirtschaft im Jahr 2022 ein Schaden von rund 203 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten sowie durch Spionage und Sabotage. Mehr als 1.000 Unternehmen quer durch alle Branchen waren repräsentativ für die Studie befragt worden. Praktisch jedes Unternehmen in Deutschland wurde in irgendeiner Form attackiert. 84 Prozent der Unternehmen waren im vergangenen Jahr sicher betroffen, weitere 9 Prozent gehen davon aus, dass sie attackiert wurden.

Dabei sind nicht nur die Angriffe aus Russland und China zuletzt sprunghaft angestiegen, sondern es ändert sich zunehmend auch die Art der ⇨

- Angreifer: Erstmals liegen im Jahr 2022 organisiertes Verbrechen und Bandenkriminalität an der Spitze der Rangliste der Täterkreise. Bei 51 Prozent der betroffenen Unternehmen kamen die Attacken aus diesem Umfeld.

Zweischneidige Sache: Bürokratie

Die Erwartungen der Unternehmen für die Zukunft sind deshalb in Sachen Wirtschaftskriminalität nicht rosig und das gilt insbesondere für die Betreiber kritischer Infrastrukturen. Im letzteren Bereich rechnen 51 Prozent mit einem starken, 33 Prozent mit einem eher starken Anstieg entsprechender krimineller Aktivitäten. Von der Politik wünschen sich 98 Prozent mehr Einsatz für eine verstärkte EU-weite Zusammenarbeit bei der Cybersicherheit. 97 Prozent fordern, dass die Politik stärker gegen Cyberattacken aus dem Ausland vorgehen soll. Und drei Viertel (77 Prozent) meinen, die Politik solle die Ermittlungsbefugnisse erweitern, damit Cyberangriffe aufgeklärt werden können.
Freilich beklagen zugleich 77 Prozent, dass der bürokratische Aufwand bei der Meldung von Vorfällen zu hoch ist. Die letzte Forderung klingt auf den Autor dieses Artikels allerdings ein bisschen so, also wolle man „gewaschen werden, ohne dabei nass zu werden". Denn – mit Verlaub – Gesetze, nach denen man ruft, erzeugen ohne Zweifel Pflichten im Unternehmen, die man dann leicht als „bürokratisch" empfinden kann.
Auch kostet mehr Schutz mehr Geld. Zwar ist laut der Bitkom-Studie der Anteil der Ausgaben für IT-Sicherheit am IT-Budget der Unternehmen, verglichen mit dem Vorjahr, von 7 auf 9 Prozent gestiegen. Doch der Verband mahnt: Bei den Ausgaben für IT-Sicherheit müssten die Unternehmen dringend zulegen. Die Erkenntnis, welche dramatischen Folgen ein erfolg-



Die Betreiber kritischer Infrastrukturen in Deutschland rechnen mit einer besonders hohen Zunahme krimineller Aktivitäten.

reicher Angriff haben kann, sei längst da. Den notwendigen Schutz davor gebe es nicht zum Nulltarif.

KRITIS-Dachgesetz schließt Lücken

Jenseits der gesetzlichen Vorgaben und Regulierungen im Bereich Cybersicherheit gab es in Deutschland bislang keine gesetzliche Regelung zum Schutz von kritischen Infrastrukturen in ihrer Gesamtheit und vor allem nicht in ihrem komplexen Zusammenspiel. Wenn Energieerzeuger ausfallen, hat das unter anderem Auswirkungen auf den Betrieb von Rechenzentren. Und wenn Rechenzentren in einem Energieverbund mit Nahwärme-Erzeugern sind, sind die wechselseitige Abhängigkeit und die Gefahr von Havarie-Kaskaden noch einmal größer. Derartige Lücken sollen durch das KRITIS-Dachgesetz, das beim Schreiben des vorliegenden Artikels in der Ressort-Abstimmung beziehungsweise in der Gesetzgebungsphase ist, geschlossen werden.

„Vor dem Hintergrund uneinheitlicher beziehungsweise fehlender Regelungen für den physischen Schutz kritischer Infrastrukturen und angesichts sektoren- sowie länderübergreifender Abhängigkeiten wird mit dem KRITIS-Dachgesetz zum ersten Mal das Gesamtsystem zum physischen Schutz kritischer Infrastrukturen in Deutschland in den Blick genommen und im Rahmen der dem Bund zustehenden Zuständigkeiten gesetzlich geregelt“, heißt es dazu in einem Eckpunktepapier des Bundesinnenministeriums.

Für Organisationen und Einrichtungen in den vom Gesetz betroffenen Bereichen soll es künftig mindestens alle vier Jahre eine Risikobewertung geben. Dabei werden laut den Eckpunkten des Bundesinnenministeriums „alle relevanten natürlichen und vom Menschen verursachten Risiken (All-Gefahren-Ansatz) sowie sektorenübergreifende und grenzüberschreitende Risiken“ berücksichtigt. In allen Sektoren sollen die gleichen Mindestvorgaben im Bereich der physischen Sicherheit gelten. Dazu zählt beispielsweise die Einrichtung eines betrieblichen Risiko- und Krisenmanagements, die Erstellung von Resilienz-Plänen sowie die Umsetzung geeigneter und verhältnismäßiger technischer, personeller und organisatorischer Maßnahmen. Parallel zum bestehenden Meldewesen im Bereich Cybersicherheit soll es künftig ein zentrales Störungs-Monitoring geben, welches einen Gesamtüberblick über mögliche Schwachstellen beim physischen Schutz kritischer Infrastrukturen verschaffen soll. Ziel ist es, andere Einrichtungen oder auch andere EU-Staaten bei drohender Gefahr warnen zu können. Gleichzeitig soll die Zusammenarbeit zwischen den Betreibern und den staatlichen Akteuren klarer herausgearbeitet werden, beispielsweise durch eindeutige Verantwortlichkeiten und Ansprechpartner. Eine zentrale Rolle kommt dabei dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK) zu. Dieses soll zu der übergreifenden zuständigen Behörde für physischen Schutz kritischer Infrastruktur ausgebaut werden.

Zertifizierung als ständiger Lernprozess

Keine Frage: Das von allen gewünschte immer umfassendere gesetzliche Korsett in Sachen kritischer Infrastrukturen im Allgemeinen und Rechenzentren im Besonderen wird für die Betreffenden auf jeden Fall mehr Aufwand bedeuten. Aufwand für die Vorbereitung und Durchführung regelmäßiger Audits, Aufwand für Schulung der Mitarbeiter, Aufwand für Kommunikation mit anderen KRITIS-Organisationen und Aufwand für die Dokumentation der getroffenen Maßnahmen, so dass man im Havariefall nachweisen kann, dass man alles Notwendige zur Gefahrenabwehr getan hat. Doch diese „Mühewaltung“ ist Mühe und Serviceleistung für unser Gemeinwesen. □

45 Jahre TDT: IT-Security Made in Germany

TDT ist ein Pionier der Telekommunikation; das Unternehmen wird im Jahr 1978 gegründet. Lange vor dem Internet forscht TDT bereits zu den Möglichkeiten, sich digital zu vernetzen. Dieser Blick nach vorn macht das Unternehmen erfolgreich – bis heute. Ein wichtiger Aspekt ist dabei, dass der Ausbau der inhabergeführten Firma und die Geschwindigkeit in ihrer Entwicklung ganz bewusst kontrolliert geblieben sind. Zum 45. Geburtstag lesen Sie hier einen kurzen Rückblick auf die Anfänge von TDT und ausgewählte Ereignisse vergangener Jahrzehnte, die das Fundament für die Gegenwart und den Fortschritt in Richtung Zukunft sind.

Am Anfang von TDT steht eine Gründerfigur mit Know-how und einer technisch-betriebswirtschaftlichen Vision: Antherm Pickhardt, ein ausgebildeter Bankkaufmann, der im Management der deutschen „Olivetti“ arbeitet, die damals für ihre vielfältigen Bürosysteme bekannt ist. Er erkennt früh, dass Büromaschinen als Geschäftsfeld nicht zukunftsträchtig sind, und macht sich selbstständig. Sein Ansatz ist Datenkommunikation als klassisches Einkaufs- und Verkaufsgeschäft. Antherm Pickhardt findet Firmen in Kanada und in den USA, die noch nicht in Deutschland präsent sind und Messgeräte für Datenübertragung bauen. Er übernimmt den Vertrieb dieser Produkte. Sein Sohn Michael Pickhardt, der Vorstandsvorsitzende der heutigen TDT AG (Foto rechts), erinnert sich: „Aus diesem allerersten Geschäftsfeld heraus, Testgeräte für Datentransfer anzubieten, erklären sich die drei Buchstaben, die von den Anfangstagen bis heute für das Unternehmen stehen: TDT. Der Firmenname ist das Kürzel für Transfer Data Test.“ Auf der Hannover-Messe 1979 stellt TDT einen Protokollkonverter einer kanadischen Firma vor: ein Gerät, das bei der Übermittlung von Datenpaketen ein Übertragungsprotokoll in ein anderes umwandelt. Damit bietet das Unternehmen funktionsfähige Systeme für das öffentliche X.25-Netz an. TDT gehört zu den ersten Anbietern für das damalige erste digitale Kommunikationsnetz Datex-P. „Das Besondere am X.25-Protokoll ist das Prinzip, Daten nicht in einem String zu übertragen, sondern sie in Pakete zu unterteilen, die gesichert durch das Netz geleitet werden, um sie dem Endgerät zu übergeben“, erläutert

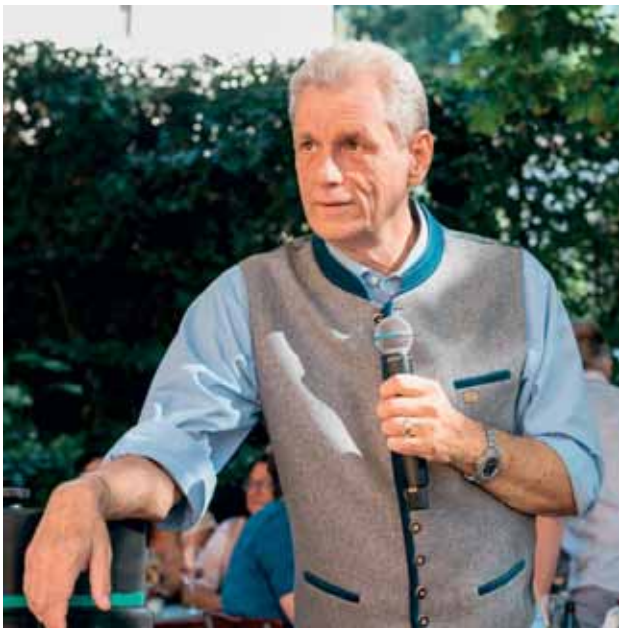


Bild: Marina Geckeler/TDT AG

Your experts in **TELE COMMUNICATION**

Michael Pickhardt. „Diese Paketvermittlung der X.25-Technologie war somit eine Art Vorreiter des heutigen Internets!“ Zu Beginn der 1980er-Jahre startet TDT mit eigener Soft- und Hardware-Entwicklung von Datenkommunikationsgeräten. Michael Pickhardt: „Wir waren damals wahrscheinlich weltweit die Ersten, die echtes Netzwerkmanagement gemacht haben. Etwas, was heute ja ‚state of the art‘ ist.“ Auch für TDT ist die Zeit der Wende und der Wiedervereinigung ein historischer Meilenstein und eine Phase großer technologischer Herausforderungen. Michael Pickhardt: „Es gab, von einigen wenigen handvermittelten Telefonverbindungen mal abgesehen, keine Verbindungen von Westdeutschland nach Ostdeutschland und umgekehrt. Im Zuge der Wiedervereinigung entstand ein plötzlicher und vielfältiger Bedarf, neue Filialnetze im Osten aufzubauen – doch wie sollte das ohne Datenkommunikation gehen? Leitungen gab es keine, Mobilfunknetze lagen noch in geschichtlicher Ferne – aber es gab Satellit, und darauf setzten wir mit unserer Idee auf. Wir bauten unser bestehendes X.25-Protokoll um, und machten es satellitenfähig.“ Zur damaligen CeBIT in Hannover richtet TDT so – in Zusammenarbeit mit der Deutschen Bundespost, mit der Deutschen Post, mit Dornier, Robotron und Gricon – die erste X.25-Satellitenverbindung in die ehemalige DDR ein, in der Rekordzeit von zehn Tagen. Heute wie damals steht TDT für sichere und innovative Telekommunikation. Es bietet professionellen Anwendern maßgeschneiderte, erfolgreiche Lösungen, die auf Open-Source-Technologien basieren. Das Produktportfolio umfasst High-End-VPN-Gateways für die Hostumgebung zur Anbindung tausender Außenstellen, Industrie-Class-VPN-Zugangsrouter mit modularer Hard- und Software-Architektur, mobile Router für Einsatzfahrzeuge sowie Telefonie-Lösungen und Firewalls. ■

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

Die TDT AG erstellt Netzwerkkonzepte, betreibt ein weltweites Netzwerkmanagement und bietet ihren Kunden professionellen Service. Das Unternehmen ist seit 2017 Silver Member der Linux Foundation und vollumfänglich vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach IT-Grundschutz (ISO 27001) zertifiziert. Das Unternehmen entwickelt, produziert und supportet in Deutschland – Made in Germany.

Was heißt Sicherheit von Rechenzentren im Jahr 2023?

Das funktionale Gebilde „Rechenzentrum“ ist im Wandel und desgleichen die Sicherheitsaspekte in und um das Rechenzentrum. Dieser Wandel stellt nicht zuletzt hohe Anforderungen an die Menschen, die in diesem Umfeld arbeiten.

Von Jürgen Höfling

Der Titel dieses Artikels stellt eine scheinbar einfache Frage, die sich bei näherem Hinsehen und Nachdenken aber zunehmend „verkompliziert“. Was bitte ist genau „Sicherheit“, ja mehr noch: Was bitte ist in Cloud- und Edge-Zeiten genau ein Rechenzentrum? Trotz allem ist die obige Frage nicht unsinnig, man kann sie aber nur approximativ beantworten.

Eine solche approximative Beantwortung ergibt sich fast von selbst, wenn man einmal durchspielt, was man als Rechenzentrumsbetreiber an Versicherungsprämien zu zahlen fähig und vor allem auch willens ist, um sich auf diesem Weg mehr Sicherheit quasi zu erkaufen. Wer meint, sich auf sein Wissen und seinen Instinkt in puncto Sicherheit gut verlassen zu können, und zudem glaubt, gut vorgesorgt zu haben, wird eher wenig an Risiken durch Versicherungsprämien reduzieren wollen. Wer das unbestimmte oder auch sehr bestimmte Gefühl hat, dass „in seinem Laden“ sicherheitsmäßig nicht alles zum Besten steht, wird mehr Prämien zahlen oder vielleicht auch schlussfolgern, dass er oder sie schleunigst Sicherheitsmaßnahmen ergreifen sollte, statt immer höhere Prämien zu zahlen.

Bild: Damian Sobczyk/stock.adobe.com

Der Gesetzgeber hält sich in der Regel mit dem Vorschreiben von Versicherungspflichten zurück. Vermutlich ist dabei ein leitender Gedanke, dass es in der Regel nur die zweitbeste Lösung ist, Risiken durch Prämienzahlung und nicht durch entsprechende Maßnahmen an Ort und Stelle zu minimieren. Auch das neue IT-Sicherheitsgesetz 2.0 sieht beispielsweise keine allgemeine Versicherungspflicht für Betreiber kritischer Infrastrukturen vor. Es wird jedoch eine Versicherungsverpflichtung für Betreiber kritischer Infrastrukturen in den Bereichen Energie, Telekommunikation, Verkehr und Gesundheit eingeführt.

Sicherheit als Näherungslösung

Sicherheit im Rechenzentrum kennt nur eine Näherungslösung, gehört also in den Bereich der „ungenauen Mathematik“, die in vielen Lebensbereichen immer wichtiger wird. Wie steht es aber nun mit dem „Rechenzentrum“? Wird auch dies immer mehr zu einer Näherungslösung in der Wolke? Ja und Nein: Für einen Anwender, der sich je nach Bedarf Rechenleistung kauft und dessen Mitarbeiter irgendwo auf der Erde zuhause oder im Café Central oder Oriental arbeiten, mag das Rechenzentrum tatsächlich eher „wolkig“ wirken. Ganz und gar nicht wolkig ist für ihn und seine Mitarbeiter der Begriff Sicherheit. Die wollen er und sie im ⇨

Übrigen nicht als Näherungslösung, sondern als Produkteigenschaft, ohne die ein bestimmtes Produkt nichts taugt.

In dem beschriebenen Produktions- und Arbeitsambiente hat das Rechenzentrum eine genau definierte Gesamtfunktionalität, ja es IST ein solches Funktionspaket. Und Sicherheit ist Teil dieses Funktionspakets und kann durch Service Level Agreements exakt beschrieben werden. Vor allem wird dadurch auch genau festgelegt, welche vertraglichen Auswirkungen Abweichungen von den im Vertrag fixierten Zusagen haben. Nur nebenbei: Derartige Verträge werden künftig vermutlich immer öfter den Charakter von „Smart Contracts" haben, also codierten Prozessen in der Blockchain, bei der die Vertragsstrafen ebenfalls durch einen Algorithmus definiert und abgerechnet werden.

Es steht zu vermuten, dass künftig Rechenzentren in ihren materiellen Ausprägungen immer variantenreichere Formen annehmen werden und dass sie in fünf bis zehn Jahren weitgehend anders aussehen als heute.

Rechenzentrumssicherheit in ihren Ausprägungen

Ein prinzipieller Sicherheitsaspekt von Rechenzentren ist die Forderung nach möglichst ganzheitlicher Betrachtungsweise. Ein modernes Schließsystem, bei dem eine Tür in einem vergessenen Winkel zu integrieren vergessen wurde, mag sicherheitsmäßig vielleicht angehen, aber wenn Cybersicherheit „hui" ist, der Objektschutz (wie immer dieses Objekt in Zukunft aussieht) aber „pfui", dann ist diese Diskrepanz mehr als problematisch.

Ein weiterer Sicherheitsaspekt in einer Welt, die trotz aller politischen und wirtschaftlichen Konkurrenzkämpfe und kriegerischen Auseinandersetzungen rechenzentrumsmäßig tendenziell im Moment doch eher als ein globales Ganzes wahrgenommen wird, ist die geopolitische Sicherheit. Wird es zunehmend zu einer geografischen beziehungsweise geopolitischen Segmentierung von Rechenzentrumskapazitäten kommen? Wie ist dann ein Chemie-Komplex der BASF in Guangdong oder ein Airbus-Werk in Schanghai „IT-mäßig" einzuschätzen?

Beides sollen hier nur Beispiele sein, um das Problem zu illustrieren. Wie geht man vor, wenn sich geopolitische Verbindungen einerseits auflösen und andererseits neu geknüpft werden? Das kann schneller passieren, als man denkt. Gibt es dann eine neue Art von Software-definierten Rechenzentren, die je nach geopolitischer Couleur neu „zusammengesteckt" werden? Man sollte dies nicht für eine fantasievolle Zukunftsschau ohne Realitätsbezug halten. Neben den bisherigen ökonomischen Spielern aus Europa, Asien und Nordamerika werden zunehmend Afrika und Südamerika das ohnehin schon labile Gleichgewicht ins Wanken bringen, zumal auch die oben angeführte traditionelle Triade keineswegs homogen ist.

Menschen als Gefahr und Rettung

Trotz aller Künstlichen Intelligenz, die vermutlich in Zukunft eine immer größere Rolle für die Sicherheit des funktionalen Gebildes namens Rechenzentrum spielen wird, geht es in Fragen der Sicherheit auch und nicht zuletzt um Menschen. Menschen sind immer Gefahr und Rettung zugleich: Sie können durch fahrlässige oder vorsätzliche Fehlentscheidungen Havarien und Katastrophen verursachen; sie können aus Kurzsichtigkeit, Feigheit oder Dummheit einer räuberischen Erpressung nachgeben und mit der Lösegeldzahlung weiteren Erpressungen Vorschub leisten; sie können aber auch verantwortungsbewusst, vorausschauend und mutig handeln und mit neuen Ideen die Sicherheit von Rechenzentren verbessern. Nicht zuletzt sind menschliche Entscheidungen essenziell für die Zukunftssicherheit von Rechenzentren und die Erhaltung von Wohlstand und Wohlergehen auf unserem kleinen Planeten. □

Datenschutzverletzungen durch Cyberattacken

Cybersicherheit und Datenschutz gehen Hand in Hand und sind zwei wesentliche Verbündete für den Schutz des Einzelnen und seiner Rechte, so der Europäische Datenschutzbeauftragte. Viele Datenpannen lassen sich ohne Cybersecurity nicht vermeiden. Ein Überblick, wie Cyberattacken und Datenschutzverletzungen zusammenhängen – bei DDoS, Ransomware, Phishing und Deep Fakes.

Von Dipl.-Phys. Oliver Schonschek

„Die vielen Meldungen von Datenschutzverletzungen, die ich täglich erhalte, verdeutlichen, dass Datenschutz nur funktioniert, wenn die Sicherheit der IT-Systeme gewährleistet ist", so die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg. „Anders als früher kann eine kleine Schwachstelle schnell die Grundrechte einer riesigen Zahl Betroffener beeinträchtigen. Bestehende Regelungen für technisch-organisatorische Maßnahmen des Datenschutzes müssen deshalb tatsächlich umgesetzt werden."

Die Landesbeauftragte nennt auch Beispiele für Cybergefahren, die sich auf den Datenschutz auswirken können: „Ransomware, Passwort-Phishing und die aktuelle Gefahr von Cyberangriffen zeigen auch, wie wichtig es ist, dass Verwaltungen und Unternehmen selbst Mechanismen etablieren, die Datenschutz und IT-Sicherheit von vornherein gewährleisten, deren Wirksamkeit kontinuierlich überprüfen und sie an neue Bedrohungslagen anpassen."

Wie aber ist der genaue Zusammenhang zwischen Datenpanne und Cyberattacke? Dies ist wichtig zu wissen, damit Cybersicherheit den richtigen Stellenwert in dem Datenschutzkonzept eines Unternehmens bekommt.

Das Datenrisiko bei DDoS

Personenbezogene Daten müssen verfügbar sein, so fordert es die DSGVO (Datenschutz-Grundverordnung). Damit die Daten aber verfügbar sind, müssen auch die dafür notwendigen Dienste bereitstehen und verfügbar sein. Einfach gesagt, kommt man ohne funktionierende Dienste und Anwendungen nicht an die Daten. Die Verfügbarkeit der Daten hängt deshalb auch mit der Belastbarkeit der Dienste und der Wiederherstellbarkeit der Daten nach einem Ausfall der Dienste zusammen.

Wenn man diesen Gedanken verinnerlicht, wird schnell klar, dass eine Überlastung der Dienste auch die mangelnde Verfügbarkeit personenbezogener Daten nach sich ziehen kann. Mehr noch: Die DSGVO fordert explizit die Fähigkeit, die Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, sowie die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ⇨

ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Offensichtlich bedeutet dann ein unzureichender Schutz gegen Überlastungsangriffe (DDoS), dass die genannten Schutzziele der DSGVO nicht erreicht werden können. Erfolgreiche DDoS-Attacken führen deshalb zu einer Verletzung des Datenschutzes, wenn Daten mit Personenbezug betroffen sind, direkt oder indirekt.

Ransomware als Datenschutzverletzung

Ransomware zielt auf die Verschlüsselung von Daten ab, häufig werden die Daten auch noch zusätzlich ausgespäht und gestohlen, so dass nicht nur für die (angebliche) Entschlüsselung Lösegeld verlangt wird. Gleichzeitig drohen die Angreifenden damit, die Daten auf Leak-Seiten zu veröffentlichen, wenn das Lösegeld nicht fließt. Für das betroffene Unternehmen sind dann zum einen die Daten nicht mehr verfügbar, wenn es kein sicheres und vollständiges Backup gibt. Zum anderen ist die Vertraulichkeit der Daten in Gefahr, wenn diese auf einer Leak-Seite landen würden.

Es ist deshalb nicht überraschend, wenn Datenschutzaufsichtsbehörden Ransomware sehr ernst nehmen. So erklärte das Bayerische Lan-

Bild: Andrey Popov/stock.adobe.com

Ransomware gefährdet die Verfügbarkeit und die Vertraulichkeit von sensiblen Unternehmensdaten und zeigt damit exemplarisch, dass IT-Sicherheit beim Datenschutz immer wichtiger wird.

desamt für Datenschutzaufsicht (BayLDA): Neben der Verschlüsselung von Dateien samt exorbitanter Lösegeldforderung kommt es vielfach auch zum Diebstahl sensibler Gesundheitsdaten, Kontodaten oder Bewerbungsunterlagen verbunden mit der Drohung, bei einer Verweigerung der Zahlung diese im Internet zu veröffentlichen.

Alleine innerhalb eines Jahres wurden dem Bayerischen Landesamt für Datenschutzaufsicht von bayerischen Unternehmen mehrere hundert Ransomware-Angriffe gemeldet, bei denen Lösegeld von 10.000 bis zu 50 Millionen Euro gefordert wurden. Der Präsident des BayLDA, Michael Will, betonte: „Schon im eigenen Interesse müssen bayerische Unternehmen ihre Daten gegen Angriffe Cyberkrimineller absichern. Die Einhaltung des Datenschutzrechts schafft einen Sicherheitswall für die Daten der betroffenen Personen, der häufig schon mit einfachen Maßnahmen errichtet werden kann."

Die Datenpanne bei Phishing

Passwort-Diebstahl bedroht personenbezogene Daten gleich doppelt. Zum einen ist die Kombination aus Benutzername und Passwort der einfachste Fall, um eine digitale Identität zu überprüfen. Phishing ist deshalb auch immer ein Diebstahl digitaler Identitäten, der Personenbezug dabei liegt auf der Hand, wenn es sich bei der Identität um eine „menschliche" Identität handelt.

Selbst bei Maschinenidentitäten kann der Diebstahl der Zugangsdaten den Datenschutz berühren, wenn sich aus den Maschinendaten Bezüge zu Personen herstellen lassen. Wenn also zum Beispiel die digitale Identität eines Fahrzeugs gestohlen wird, können schnell die Daten der Fahrzeugnutzenden in Gefahr geraten.

Phishing ist aber zugleich das Tor zu weiteren personenbezogenen Daten und führt in aller Regel zu weiteren Datenschutzverletzungen, indem die Rechte des Opfers missbraucht und zusätzliche Daten ausgespäht werden. Phishing-Schutz ist deshalb immer auch Datenschutz.

Deep Fake aus Sicht der Aufsichtsbehörde

Um eine digitale Identität zu stehlen und vorzutäuschen, wird zunehmend auch der Weg gewählt, Fotos, Videos und Audios zu manipulieren und mit Hilfe von KI (Künstliche Intelligenz) das Aussehen und die Stimme des Angreifenden in das oder die einer anderen Person zu verwandeln.

Solche Deep Fakes bedrohen also zum einen die digitale Identität der vorgetäuschten Person und dann auch weitere Daten, an die der Angreifende durch die Täuschung gelangt. Das könnten auch medizinische Daten einer anderen Person sein, wenn eine Deep-Fake-Attacke bei einer Videosprechstunde mit Ärzten gelingt. Deep Fakes und Maßnahmen zur Erkennung einer solchen Täuschung gehören deshalb auch zum Datenschutz, wie auch diese Warnung der Kirchlichen Datenschutzaufsicht der ostdeutschen Bistümer und des Katholischen Militärbischofs zeigt: „Je mehr persönliche Informationen über einen bekannt sind, desto besser kann eine Deep-Fake-Falle zuschnappen. Cyberkriminelle nutzen jetzt schon diese Technik in Verbindung mit Social Engineering (Mensch als Schwachstelle), beispielsweise, um in betriebliche Umgebungen einzudringen oder Finanztransaktionen anzuweisen."

Fazit: Cybersicherheit gehört zum Datenschutz

Diese Beispiele zeigen sehr deutlich: Ohne Cybersecurity kann der Datenschutz seine Ziele nicht erreichen. Es ist deshalb nur konsequent, wenn der Europäische Datenschutzbeauftragte nun auch ganz offiziell eine enge Kooperation mit der EU-Agentur für Cybersicherheit ENISA vereinbart hat. □

Existenzielles Risiko Zero-Days: Ein umfassender Ansatz zur Mitigation für Unternehmen

Zero-Day-Exploits sind eine der gefährlichsten Cyber-Bedrohungen für Unternehmen. Diese bisher unbekannten Schwachstellen können von Angreifern ausgenutzt werden, bevor die Hersteller einen Patch zur Verfügung stellen können.

Insentis

Beispiele wie die log4Shell-Schwachstelle, die eine vollständige Systemübernahme betroffener Webserver aus dem Internet ermöglichte, die WinRAR-Schwachstelle vom August 2023, die seit April 2023 ausgenutzt und erst vier Monate später veröffentlicht wurde, und die darin enthaltenen verwundbaren unrar*.DLLs von über 400 weiteren Programmen. Ein weiteres berüchtigtes Beispiel ist „Eternal Blue“, ein Exploit, der die Server Message Block (SMB)-Implementierung von Windows angreift und jahrelang von der NSA geheim gehalten und ausgenutzt wurde, um in Systeme einzudringen. Nach Bekanntwerden der Schwachstelle nutzten bekannte Ransomware-Programme wie „WannaCry“ oder „Petya“ genau diese Schwachstelle, um zahlreiche ungepatchte Systeme zu übernehmen.
Besonders kritisch sind auch Zero-Days in Browsern, da sie Drive-By-Compromise-Angriffe ermöglichen, die eine Kompromittierung der Systeme ermöglichen.

Schlüssel zum schnellen Erkennen und Reagieren auf Zero-Days

Asset Management ist unerlässlich, um schnell feststellen zu können, ob die unternehmenseigenen Assets wie IT-Systeme, Anwendungen, Bibliotheken von Drittanbietern von einer Zero-Day-Attacke betroffen sind.

Watchlists: Alle Abteilungen, Teams und Asset Owner sollten Watchlists für Zero-Days in Übereinstimmung mit ihrem Asset Management pflegen. So werden sie proaktiv benachrichtigt, wenn ein Zero-Day für eine Komponente auf der Watchlist veröffentlicht wird. Ein vollständiger Überblick über Komponenten von Drittanbietern wie Bibliotheken, Anwendungen, Dienste und Betriebssysteme ist in diesem Zusammenhang von entscheidender Bedeutung.

Vulnerability Management: Als Ergänzung zur Feststellung der Betroffenheit über Watchlists kann auch Vulnerability Scanning eingesetzt werden. Entsprechende Scan-Module prüfen, ob eine Zero-Day-Schwachstelle vorliegt oder nicht. Ein Nachteil gegenüber Watchlists ist, dass die Scan-Module fehlerhaft sein können und vor allem neben False-Positives auch False-Negatives produzieren können, außerdem benötigen die Hersteller von Vulnerability Scannern auch eine gewisse Zeit, um ein Scan-Modul für eine neue Zero-Day zu entwickeln, zu testen und zu veröffentlichen – 24 Stunden nach Bekanntwerden einer Zero-Day sind keine Seltenheit.

Mitigierende Maßnahmen

Sobald eine Bedrohung erkannt wurde, können Unternehmen mit Patching, Workarounds oder der Isolierung der betroffenen Systeme reagieren. Auch virtuelles Patching über eine Web Application Firewall (WAF) kann eine effektive Lösung sein. Dabei werden Anfragen nach typischen Angriffsmustern blockiert und so die Ausnutzung von Exploits verhindert. Kurze Reaktionszeiten sind entscheidend, da die meisten Zero-Day-Angriffe erfahrungsgemäß in den ersten Stunden nach Bekanntwerden stattfinden.

Eine der einfachsten und wichtigsten Präventivmaßnahmen ist es, die Versionsinformationen der eigenen Assets, wie z.B. des Webservers, nicht nach außen zu geben. Denn Angreifer attackieren in erster Linie Systeme, die eine betroffene Version preisgeben.

Proaktive Identifizierung von Zero-Days

Penetration Testing und statisches Security Testing

Unternehmen sollten nicht nur reaktiv, sondern auch proaktiv handeln. Statische und dynamische Security-Testing-Instrumente wie Penetrationstests und Red-Teaming-Assessments, statische Analysen, Code-Reviews und Threat Modeling sind unerlässlich, um proaktiv Zero-Days zu identifizieren. Insentis bietet beispielsweise Penetrationstests für Webanwendungen, iOS- und Android-Apps sowie IoT-Geräte an, die sich an den OWASP-Standards, wie dem Web Security Testing Guide oder der Mobile Application Security orientieren.

Bug-Bounty-Programme als Monitoring-Instrument für Zero-Days

Bug-Bounty-Programme, bei denen externe Sicherheitsforscher für das Finden und Melden von Schwachstellen belohnt werden, dienen als Überwachungsinstrument zur kontinuierlichen Erkennung von Zero-Days zusätzlich zu wiederkehrenden intensiven Penetrationstests, um das Risiko von Zero-Days auch zwischen den Tests zu reduzieren. Insentis berät bei der Umsetzung von Bug-Bounty-Programmen geregelt mit einem genau definierten Rahmen via Policies sowohl mit professionellen Bug-Bounty-Anbietern, wie HackerOne, als auch mit offenen Standards wie der „security.txt“ nach RFC 9116.

Das Risiko von Zero-Days kann nie vollständig eliminiert werden

Trotz aller Bemühungen können Zero-Days nicht vollständig verhindert werden. Daher ist es notwendig, Systeme zur Angriffserkennung zu implementieren, reaktive Maßnahmen wie Incident Response und Disaster Recovery zu etablieren und diese durch präventive Maßnahmen nach dem Defense-in-Depth-Ansatz zu ergänzen. ■

Ihr Ansprechpartner:

Valeri Mike
Senior Manager

Mehr als 15 Jahre Erfahrung in IT-Security
Whitehat-Hacker & Penetrationtester
Insident Response & Forensics
Application Security & DevSecOps
ISMS ISO 27001 Lead Auditor
Betrieblicher Datenschutzbeauftragter (IHK)

Mobil: +49 151 20016884
valeri.mike@insentis.com

Datengrenzen für die Cloud: Was bringt es für den Datenschutz?

Cloud-Provider bieten an, dass Cloud-Nutzende bestimmen können, in welchen Regionen ihre Daten verarbeitet werden. Die Daten bewegen sich dann nur innerhalb definierter Grenzen. Welche Bedeutung hat das für den Datenschutz in der Cloud? Lassen sich Datenrisiken begrenzen? Oder stellt sich die Frage nicht mehr, seit das Data Privacy Framework für EU-US-Datentransfers gültig ist?

Von Dipl.-Phys. Oliver Schonschek

Bild: Sono Creative/stock.adobe.com

Die Datenschutz-Grundverordnung (DSGVO) enthält zahlreiche Regelungen, die bei einer Übermittlung personenbezogener Daten in Drittstaaten zu beachten sind. All diese Vorgaben dienen aber nur einem Zweck: Es soll gewährleistet sein, dass die personenbezogenen Daten überall, auch nach Übermittlung in das Drittland, angemessen geschützt sind.

Da liegt die Idee auf der Hand, die Daten direkt innerhalb der EU zu belassen und auf eine Datenübermittlung zu verzichten. Dazu definiert man räumliche Grenzen, innerhalb deren sich die Daten befinden und bewegen, also Datengrenzen. Doch bedeuten Datengrenzen automatisch, dass der Datenschutz gewährleistet ist? Grundsätzlich: Automatisch ist der Datenschutz nie gewährleistet, man muss immer etwas dafür tun, auch innerhalb der EU, das versteht sich. Was aber bringen Datengrenzen? Und braucht man sie für US-Clouds überhaupt, wo es doch jetzt das DPF (Data Privacy Framework) gibt?

Data Privacy Framework ist kein Allheilmittel

Auch wenn die Freude groß war, als das Data Privacy Framework endlich da war, sind dadurch nicht etwa alle Datentransfers von der EU in die USA aus Datenschutzsicht unproblematisch. Zum einen müssen sich die Empfänger zuerst und nachweislich dem DPF unterwerfen, das DPF kann nicht ohne weiteres einfach als gegeben angenommen werden.

Zum anderen ist bereits Kritik laut geworden und so manche Stimmen waren zu hören, die keine lange Rechtssicherheit dank DPF sehen. Das DPF könnte ein echter Nachfolger des Privacy Shield werden, also das gleiche Ende finden, so die Kritiker.

Gleichzeitig muss betont werden, dass es auch Datenübermittlungen gibt, für deren Zielland es keinen Angemessenheitsbeschluss der EU-Kommission gibt. Deshalb sollten Unternehmen grundsätzlich vor einer geplanten Datenübermittlung ein Transfer Impact Assessment (TIA) durchführen und dabei die rechtliche Situation genau hinterfragen, die in dem Zielland gilt.

Datengrenzen: EU oder sogar nur Deutschland?

Ein weiterer Punkt kann die Frage nach den Datengrenzen weiterhin sinnvoll machen: Umfragen zeigen immer wieder, dass Unternehmen in Deutschland bei Cloud Computing einen Unterschied machen, ob das Rechenzentrum in der EU oder wirklich in Deutschland steht. Dahinter steckt keine Datenschutzanforderung, denn der Datenschutz macht hier keinen Unterschied innerhalb der EU.

Doch die Kunden selbst machen womöglich einen Unterschied, sie bevorzugen unter Umständen Cloud-Dienste direkt aus Deutschland. So ergab der „Cloud Report 2023“ des Bitkom: Mit Blick auf Sicherheit und Datenschutz ist 8 von 10 Unternehmen (81 Prozent), die Cloud Computing nutzen, dies planen oder diskutieren, wichtig, in welchem Land sich das Rechenzentrum des Cloud-Anbieters befindet. Klarer Standort-Favorit ist Deutschland: 93 Prozent bevorzugen ein heimisches Rechenzentrum.

Datengrenzen oder souveräne Cloud

Oracle zum Beispiel nennt sein Cloud-Angebot mit Datengrenze „Oracle EU Sovereign Cloud“, Microsoft spricht von „Microsoft EU Data Boundary“. Neben den Datengrenzen gibt es auch die Fragen nach der souveränen Cloud. Hierzu haben sich die Datenschutzaufsichtsbehörden bereits positioniert.

Souveräne Clouds müssen es demnach den Verantwortlichen (nach DSGVO) ermöglichen, die Einhaltung der datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft sicherzustellen. Die Kriterien für souveräne Clouds umfassen die Punkte „Nachvollziehbarkeit durch Transparenz“, „Datenhoheit und Kontrollierbarkeit“, „Offenheit“, „Vorhersehbarkeit ⇨

E-Mail im Visier von Hackern: So schützen sich Unternehmen ganzheitlich

Mit der Retarus Secure Email Platform sichern Unternehmen ihre E-Mail-Kommunikation wirkungsvoll gegen Cyberangriffe ab.

Egal ob Spam, Malware oder Phishing durch Business Email Compromise – die Angriffsmethoden Cyberkrimineller sind vielfältig. Dadurch können herkömmliche E-Mail-Sicherheitslösungen Angriffe nur schwer erkennen. Umso wichtiger ist es, dass Unternehmen bei ihrer Abwehrstrategie einen ganzheitlichen Ansatz verfolgen. Retarus bietet hierfür aus einer Hand eine Cloud-basierte Komplettlösung für Business-E-Mail, mit der Unternehmen für alle Eventualitäten gerüstet sind:

1) Social Engineering

Business Email Compromise (BEC) ist mittlerweile eine der häufigsten Cyber-Betrugsarten. Mithilfe der Retarus CxO Fraud Detection können Unternehmen gefälschte Absenderadressen identifizieren, die für solche Angriffe verwendet werden, und die E-Mails als Betrugsversuche entlarven, noch bevor eine vermeintlich vom Chef angeordnete Finanztransaktion stattfindet. Dabei stellen moderne Algorithmen „From-Spoofing“ und „Domain-Spoofing“ fest und erkennen dadurch gefälschte Absenderadressen zuverlässig. Als BEC eingestufte Nachrichten werden nicht unmittelbar zugestellt, sondern zunächst in einer Quarantäne isoliert.

2) Zero-Day-Attacken

In der Regel arbeiten Sicherheitslösungen zuverlässig und erkennen einen Großteil der Malware, bevor diese überhaupt in das Netzwerk eindringt. Einen hundertprozentigen Schutz vor Angriffen gibt es jedoch nie. Patient Zero Detection® geht als Post Delivery Protection noch einen Schritt weiter und identifiziert auch Malware- und Phishing-E-Mails, die bereits zugestellt wurden. Betroffene Nachrichten werden automatisch verschoben oder gelöscht. Darüber hinaus alarmiert Patient Zero Detection entsprechend der Kundeneinstellungen den zuständigen Administrator und optional auch den E-Mail-Empfänger.

Wenn bisher unbekannte Bedrohungen wie Ransomware zum ersten Mal auftauchen, werden sie oft nicht sofort herausgefiltert und können sich unbemerkt im Unternehmensnetzwerk verbreiten. Retarus hat für

solche Fälle unter anderem KI-basierte Sandboxing-Technologie integriert: Dabei werden Anhänge in einer virtuellen, sicheren Testumgebung ausgeführt und auf ungewöhnliches Verhalten überprüft, bevor die E-Mail zugestellt wird. Als infiziert eingestufte E-Mails werden je nach Konfiguration automatisch gelöscht oder in die Quarantäne verschoben.

3) Cyberangriffe aus bestimmten Ländern

Gerade in der aktuellen politischen Situation kann es hilfreich sein, alle Nachrichten aus bestimmten Regionen oder Ländern präventiv und ohne Rücksicht auf den Inhalt zu isolieren, sei es aus reinen Sicherheitsgründen oder aufgrund interner Compliance-Anforderungen. Die Retarus Predelivery Logic ermöglicht es IT-Verantwortlichen, den gesamten E-Mail-Verkehr auf der Grundlage selbst definierter Regelwerke zu analysieren und gegebenenfalls zu blockieren, bevor er überhaupt die Unternehmensinfrastruktur erreicht. So ist es beispielsweise möglich, E-Mails gezielt auf Basis ihres Herkunftslandes (GeoIP) zu bearbeiten. Je nach Konfiguration kann dies etwa die Isolierung der Nachricht in der Benutzerquarantäne sein.

4) Trotz Cyberangriff weiter per E-Mail erreichbar

Retarus bietet zudem eine Cloud-Lösung für E-Mail Continuity, mit der die Mitarbeiter jederzeit unterbrechungsfrei per E-Mail weiter kommunizieren können, falls die IT-Infrastruktur dennoch einmal ausfällt. Tritt das Krisenszenario ein, werden die E-Mails über einen externen, vom primären E-Mail-System unabhängigen sicheren Webmail-Service geleitet. Als Failover-Service hält sich dieser ununterbrochen im Hintergrund mit provisionierten Postfächern bereit. Die Mitarbeiter sind somit auch bei einem Ernstfall weiter über ihre bekannten Adressen erreichbar und haben Zugriff auf vergangene E-Mail-Konversationen und abgespeicherte Kontaktdaten. ■

Besuchen Sie Retarus auf der it-sa in Nürnberg, in Halle 7 an Stand 109.

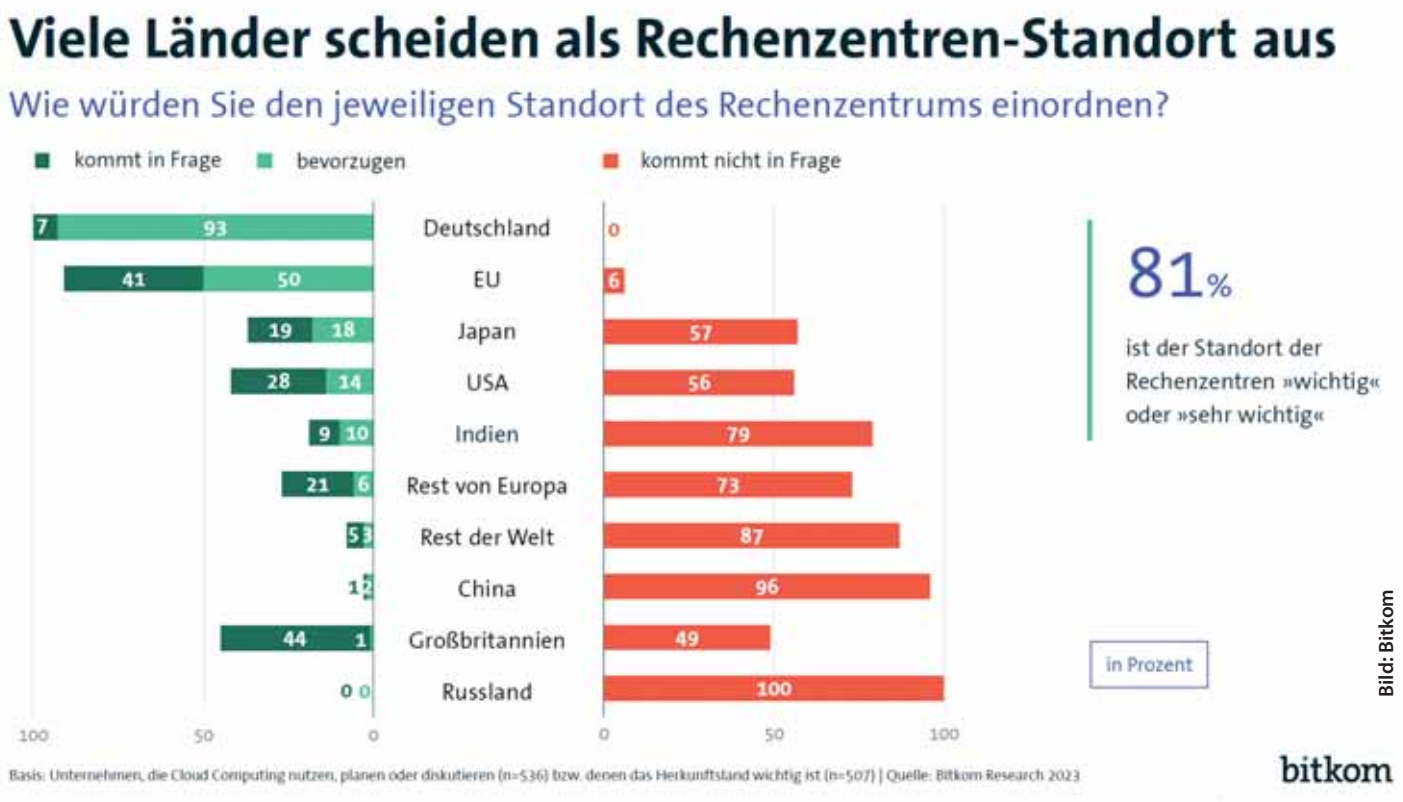
www.retarus.de

und Verlässlichkeit“ sowie „Regelmäßige Prüfung der aufgestellten Kriterien“. Hier geht es offensichtlich nicht nur um Grenzen für Cloud-Daten.

Folgen der Datengrenze werden noch untersucht

Der frühere Datenschutzbeauftragte des Landes Schleswig-Holstein, Thilo Weichert, bewertete im April 2023 die Datengrenzen so: „Mit einem Anfang 2023 gestarteten ‚EU Data Boundary‘ wirbt Microsoft um Vertrauen für Microsoft 365, Azure und Konsorten. Microsoft baut derzeit 17 Rechenzentren in Europa auf und aus. Dies ändert aber nichts an dem Umstand, dass US-Behörden auf diese Daten per Cloud-Act und Foreign Intelligence Surveillance Act Zugriff einfordern. Diese Gesetze verpflichten Microsoft, auch im Ausland verarbeitete Daten den US-Sicherheitsbehörden zur Verfügung zu stellen und hierüber Stillschweigen zu wahren.“ Noch haben sich die Aufsichtsbehörden nicht explizit zu den Auswirkungen der Datengrenzen geäußert, aber sie hinterfragen diese. Das Gremium der Datenschutzaufsichtsbehörden, Datenschutzkonferenz (DSK) genannt, hat festgehalten, dass „die AG DSK ‚Microsoft-Onlinedienste‘ ihr (...) über die Änderungen berichten soll, die sich aus der EU Data Boundary ergeben“.

In jedem Fall aber sollten Unternehmen auch für sich prüfen, welche der genutzten Cloud-Dienste denn innerhalb der Datengrenzen erbracht werden, wie es um Supportzugriffe steht und nicht zuletzt, wie die rechtlichen Möglichkeiten zum Beispiel für Nachrichtendienste der Drittstaaten aussehen, mögliche Datengrenzen zu „überschreiten“. □



Der Datenschutz macht keinen Unterschied innerhalb der EU, doch die Kunden selbst bevorzugen Cloud-Dienste direkt aus Deutschland.

Lässt sich ChatGPT datenschutzgerecht nutzen?

Trotz der laufenden Datenschutz-Diskussion rund um ChatGPT kommt der KI-Dienst bereits betrieblich zum Einsatz. Leserinnen und Leser fragten, ob sich denn ChatGPT überhaupt datenschutzkonform nutzen lässt. Wir haben Prof. Dieter Kugelmann, Leiter der KI-Taskforce der Datenschutzkonferenz (DSK) und Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, dazu befragt.

Von Dipl.-Phys. Oliver Schonschek

Viele Startups sind sehr innovativ und entsprechend aufgeschlossen für neue Technologien wie Künstliche Intelligenz (KI). Wie eine Umfrage des Digitalverbands Bitkom ergab, kommt in mehr als der Hälfte der deutschen Startups (53 Prozent) generative KI zur Textgenerierung wie ChatGPT bereits zum Einsatz. Weitere elf Prozent nutzen solche Tools noch nicht, haben dies aber bereits geplant, 21 Prozent können es sich für die Zukunft vorstellen. Betrachtet man die Unternehmen in Deutschland generell, ist der Einsatz von ChatGPT zwar noch nicht so verbreitet wie unter den Startups, geplant wird die Nutzung aber dennoch: Jedes sechste Unternehmen (17 Prozent) plant den Einsatz solcher KI-Anwendungen, weitere 23 Prozent haben keine konkreten Planungen, können sich die Nutzung aber vorstellen. Demgegenüber stehen 29 Prozent der Unternehmen, die einen solchen KI-Einsatz für sich ausschließen, so Bitkom.

Im Bereich Datenschutz gibt es offene Fragen

Einer der Gründe, solche KI-Dienste für sich auszuschließen, werden im Datenschutz gesehen. So sieht sich eine Mehrheit von 58 Prozent bei Künstlicher Intelligenz vor neue Herausforderungen gestellt, etwa beim Datenschutz. Gibt es für Unternehmen bei ChatGPT einen Weg zum Beispiel über Datenschutz-Folgenabschätzung (DSFA), Nutzungsbedingungen und Schulung, um diesen KI-Dienst datenschutzgerecht nutzen zu können? Fragen wie diese sollte man vor dem Einsatz von ChatGPT & Co. klären.

Hinweise einer Datenschutzaufsicht zu ChatGPT

Was sagen die Aufsichtsbehörden für den Datenschutz in Deutschland beziehungsweise das Gremium der unabhängigen Datenschutzbehörden in Deutschland, also die Datenschutzkonferenz (DSK), dazu? Wir haben Prof. Dieter Kugelmann, Leiter der KI-Taskforce der Datenschutzkonferenz (DSK) und Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, dazu befragt.

Worauf sollten Unternehmen bei einer Datenschutz-Folgenabschätzung (DSFA) für ChatGPT achten?

Prof. Dieter Kugelmann: Um die möglichen Risiken durch die Nutzung eines KI-basierten ⇨

- Dienstes wie ChatGPT zu minimieren, sollten Unternehmen den Zweck, für den ein solcher Dienst genutzt werden darf, möglichst eng begrenzen.
  Aus Sicht des Datenschutzes bedeutet dies auch, den Personenbezug so gering wie möglich zu halten. Viele KI-Anwendungen benötigen gar keinen direkten Personenbezug, vielmehr reicht die Verwendung von Pseudonymen oder noch besser anonymen Daten völlig aus.
  Wichtig ist es zudem, einem Dienst wie ChatGPT die Übernahme der Eingabedaten (Prompts) in den Trainingsdatenbestand zu verbieten. Hierzu gibt es spezielle Einstellungen, die OpenAI inzwischen vorgesehen hat.

Insgesamt sollten Unternehmen einen solchen Dienst nur zur schnellen Recherche und zur Vorbereitung menschlichen Entscheidens verwenden und nicht etwa für eine automatisierte Entscheidung im Einzelfall oder Profiling.
Ich möchte an dieser Stelle nochmals auf die sogenannte „Hambacher Erklärung zur Künstlichen Intelligenz“ verweisen, deren Lektüre ich nur empfehlen kann.

Können Sie bereits etwas zu den Nutzungsbedingungen von ChatGPT sagen?
Wir sind noch in der Prüfung, jedoch kann man schon sagen, dass die Nutzungsbedingungen vieles offen lassen. Alleine ein Verweis auf

Bild: phonlamaiphoto/stock.adobe.com

Als Unternehmen sollte man zurückhaltend bei der Nutzung eines Dienstes wie ChatGPT sein. Es empfiehlt sich, die weiteren Ergebnisse der Datenschutzaufsichtsbehörden genau zu beachten.

derartige Nutzungsbedingungen wird also aus Datenschutzsicht nicht ausreichen, um hinreichende Transparenz für die Nutzung herzustellen.

Was sollten interne Richtlinien im Unternehmen zu ChatGPT mit Blick auf die Datenschutz-Grundverordnung (DSGVO) enthalten? Kann man hier schon etwas empfehlen?
Was man schon sagen kann: Grundsätzlich sollten Unternehmen solche Dienste, wenn überhaupt, nur für die Unternehmenszwecke verwenden und freigeben. Eine Privatnutzung am Arbeitsplatz sollte nicht erlaubt werden, um die Daten der Beschäftigten keinem möglichen Datenrisiko auszusetzen.
Vertrauliche und personenbezogene Daten sollten in entsprechende Dienste nicht eingegeben werden. Das gilt insbesondere auch für sensible Daten im Sinne des Artikels 9 DSGVO. Zudem sollte die Weitergabe der Ergebnisse eines solchen Dienstes an unbefugte Dritte ausgeschlossen werden.

Was sollte in einer Schulung zu ChatGPT nicht vergessen werden?
Natürlich sollten die internen Richtlinien des Unternehmens nicht nur aufgestellt, sondern auch in einer Schulung vermittelt werden. Wichtig ist zudem der Hinweis: ChatGPT kann auch falsche Ergebnisse liefern. Man muss also immer nachprüfen.
Und: Spaß mit der offenen Version ist eine Sache, sachorientierte Ergebnisse zu erreichen, eine andere.

Kann die KI Taskforce schon etwas sagen zur Prüfung von ChatGPT? Bis wann rechnen Sie mit ersten Ergebnissen?
Wir sind noch mit der Prüfung der umfangreichen Antworten von OpenAI befasst. Es hat sich schon gezeigt, dass unsererseits wohl Bedarf an zusätzlichen Nachfragen besteht, der Abstimmungs- und Auswertungsprozess wird also noch einige Zeit dauern.

Seit dem 1. Oktober 2015 ist Prof. Dr. Dieter Kugelmann Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz.

Bild: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

„Spaß mit der offenen Version von ChatGPT ist eine Sache, sachorientierte Ergebnisse zu erreichen, eine andere."

Fragenkatalog zu ChatGPT liefert Beispiel für eine KI-Prüfung

Es lohnt sich, den Fragenkatalog, den die Aufsichtsbehörden für den Datenschutz zur Beantwortung an OpenAI geschickt haben, genauer anzusehen. Man findet darin zentrale Fragen, die der Datenschutz an einen KI-basierten Dienst stellt. Damit kann der Fragenkatalog auch eine Hilfe sein, wenn ein Unternehmen selbst einen KI-Dienst hinterfragen will, zum Beispiel für eine Datenschutz-Folgenabschätzung (DSFA) nach DSGVO.
Es zeigt sich also: Als Unternehmen sollte man zurückhaltend bei der Nutzung eines Dienstes wie ChatGPT sein. Noch ist vieles offen. Alleine ein Verweis auf die Nutzungsbedingung, eine Schulung und eine interne Risikoanalyse wird nicht ausreichen. Es empfiehlt sich, die weiteren Ergebnisse der Datenschutzaufsichtsbehörden genau zu beachten. □

Die ideale und sichere IT-Netzwerkinfrastruktur

Die Anforderungen für die Netzwerkinfrastruktur und Datensicherung eines Unternehmens, staatliche Organisationen, Kommunen und Städte steigen stetig an. Eine Vielzahl von Software- und Hardwarekomponenten müssen miteinander funktionieren, verwaltet und gepflegt werden. Mit der Komplexität der IT-Infrastruktur nehmen auch Administrations-, Anschaffungs- und Wartungskosten zu. Aber auch die Anfälligkeit und die Gefahr für Sicherheitslücken oder Ausfälle steigen zunehmend. Die Abhängigkeit von vielen unterschiedlichen Lieferanten und Fachpersonal wächst massiv.

Mitarbeiter sind heute mobil. Sie arbeiten im Büro, unterwegs, von zu Hause aus, mit lokalen oder remote bereitgestellten Anwendungen oder auf einer cloudbasierten Lösung. Das erhöht die Risiken exponentiell. Das Endgerät des Anwenders, das Home-Netzwerk oder Hotspots aus dem er arbeitet oder mögliche Schadanwendungen auf Fremdgeräte in diesem Netzwerk, machen ein „sicheres“ Arbeiten unmöglich. Das Ganze wird durch die Kommunikation über das unsichere Medium Internet nochmal deutlich schwieriger.

Nicht einhaltbare Vorgaben, Strafzahlungen bei Cyberangriffen und immer wiederkehrende Hard- und Softwarekosten, steigende Energie- und CO_2-Emissionskosten belasten zudem die Unternehmen.

Eine ganzheitlich durchdachte IT-Infrastruktur umfasst alle diese Anforderungen, minimiert die Risiken und stellt eine unterbrechungsfreie Plattform für Business Continuity sicher. Sie ermöglicht Flexibilität und Skalierbarkeit für zukünftiges Wachstum oder Veränderungen, reduziert die Komplexität und minimiert den Hard- und Softwarebedarf. Gleichzeitig wird der Energieverbrauch und damit der CO_2-Ausstoß stark reduziert.

Das Dreibein der ganzheitlichen IT-Infrastruktur

Das Dreibein der ganzheitlichen IT-Infrastruktur besteht aus den drei Komponenten,

- **sayFUSE HCI** (Fast Universal Storage HCI Engine) zur Bereitstellung der hyperkonvergenten Infrastruktur. Hier werden CPU, RAM, Storage und Netzwerkressourcen zu einem einzigen Software-definierten System zusammengefasst und können über die Nodes hinweg verwaltet werden. Sie ist fehlertolerant gegenüber Komplettausfällen von einem oder mehreren Nodes und ermöglicht einen unterbrechungsfreien Betrieb. Die zukünftigen Erweiterungen

werden durch Ergänzung weiterer Nodes problemlos und ohne Migrationsaufwand durchgeführt.

- **sayFUSE Backup** (Fast Universal Storage Backup Engine) für Backup, Restore mit bis zu 12 TB in der Stunde, Archivierung und Auslagerung als wichtigste Unternehmensversicherung für Daten und Unternehmenswerte.
- **sayTRUST VPSC** (Virtual Private Secure Communication) für Zero Trust Client Access für den Zugang der Anwender auf die einzelnen Anwendungen, Dienste, Netzwerke oder den eigenen virtuellen Arbeitsplatz-Computer nach Prüfung der Identität über mehrstufige „Defence in Depth"-Sicherheitsverfahren.

Das Dreibein der ganzheitlichen IT-Infrastruktur stellt

- **eine beliebig skalierbare, ausfallfreie Hochsicherheitsinfrastruktur** auf und schützt die Unternehmenswerte gegen Cyberangriffe und Katastrophenfälle.
- **ist eine ideale Lösung für Unternehmen jeder Größe**, auch für Rechenzentren, Banken, Städte und Kommunen. Für Unternehmen, die auf Qualität, Sicherheit, hohe Leistung und Nachhaltigkeit bedacht sind.
- **bietet eine Plattform für eine oder mehrere Standorte/Mandanten** oder viele Abteilungen.
- **bietet für Big-Data-Analysen eine fortschrittliche Hochgeschwindigkeits-Plattform** für Analysen sehr großer und vielfältiger Datensätze. Für strukturierte, teilstrukturierte und unstrukturierte Daten aus unterschiedlichen Quellen und in unterschiedlichen Größen (von Terabyte bis Zettabyte).

Die Produkte sayFUSE HCI, sayFUSE Backup und sayTRUST VPSC können auch alleine betrieben werden und stellen jede für sich eine hoch sichere und einzigartige Lösung in ihrem jeweiligen Einsatzgebiet dar. In Kombination verstärken sie einander und bilden eine ganzheitliche Lösung für die Anforderungen von heute und der Zukunft. sayFUSE HCI, sayFUSE Backup und sayTRUST VPSC bilden das Dreibein und sind die Säulen einer ganzheitlichen IT-Infrastruktur. ■

Security Operations Center: Wie der richtige Vertrag die Haftung reduziert

Wer als Dienstleister das Security Management für seine Kunden übernehmen will, sollte sich zuvor vertraglich absichern – und dabei einige Fallstricke kennen und umgehen. Hier unsere 5 Top-Tipps für SOC-Anbieter.

Von Rechtsanwalt Arne Trautmann

Bild: LALAKA/stock.adobe.com

Der Markt für Security Operations Center (SOC) as a Service ist stark wachsend und lukrativ. Hier können Dienstleister für ihre Kunden als externe Security-Experten tätig werden, deren Netzwerke und Systeme überwachen, auf Vorfälle reagieren, Bedrohungen analysieren, Angriffsmuster identifizieren und kontinuierlich entsprechende Gegenmaßnahmen ergreifen. Der Kunde erhält eine professionelle Leistung, die er inhouse so nicht oder jedenfalls nicht wirtschaftlich sinnvoll erbringen könnte. Das Systemhaus hat ein gut verkäufliches und vor allem skalierbares Produkt. Das alles geschieht in der Regel auf Basis eines Abo-Modells. Wie bei jeder Leistung muss auch hier ein Vertrag geschlossen werden – und natürlich gibt es Fallstricke, die es zu vermeiden gilt.

1. Legen Sie Wert auf ein gutes SLA

Kein Service ist 100-prozentig verfügbar, kein Techniker kann jederzeit sofort mit der Beseitigung eines Problems beginnen – oder gar dessen Beseitigung in bestimmter Frist zusagen. Es muss also definiert werden, was durch den SOC-Provider geschuldet ist, und zwar möglichst genau und vollständig. Diese Funktion erfüllt das Service Level Agreement (SLA). Hier werden Verfügbarkeiten und Reaktionszeiten definiert, aber auch, wie man diese misst und protokolliert. Ohne SLA ist häufig gar nicht klar, was genau eigentlich von wem wie geschuldet ist: SOC ist ja keine Leistung, die man „mittlerer Art und Güte“ (§ 243 Abs. 1 BGB) erbringen kann.

2. Kontrollieren Sie Ihre Haftung

Das SLA erfüllt noch eine sehr wichtige – oft aber übersehene – Funktion: Es begrenzt die Haftung des SOC-Providers. Das Haftungssystem des deutschen Zivilrechtes ist streng: Jede Vertragspartei haftet bereits bei leichter Fahrlässigkeit voll, also ohne Begrenzung der Summe. Dabei liegt das Risiko beim SOC-Provider, der ja die eigentliche Leistung erbringen muss – bei dem also auch viel schieflaufen kann. Die auf den ersten Blick einfachste Möglichkeit ist es, schlicht eine Haftungs-Höchstsumme in den Vertrag einzuführen.

Das ist aber nicht einfach. Denn die SOC-Verträge werden in aller Regel als Allgemeine Geschäftsbedingungen gewertet werden. Solche AGB dürfen aber nur in recht engen Grenzen von der gesetzlichen Grundkonzeption eines Vertrages abweichen – und die sieht eben eine volle Haftung vor. Aber hier hilft das SLA. Denn es definiert, was geschuldet ist und was nicht – und was nicht geschuldet ist, dafür kann man auch bei Nichterbringung nicht haften. Durch geschickte Bonus-Malus-Regelungen kann ein Graubereich definiert werden, in dem eine unterschrittene Verfügbarkeit oder Reaktionszeit zwar „schon“ eine Reduzierung der Vergütung triggert, aber „noch“ kein Mangel ist.

3. Sichern Sie die Skalierbarkeit der Leistungen

SOC-Services können nur dann preislich attraktiv und skalierbar angeboten werden, wenn sie nicht zu individuell ausgestaltet sind. Gleichzeitig entwickelt sich aber das Feld rasant weiter. Was gestern noch Stand der Technik war ist heute überholt. Neue Produkte, Bausteine und Leistungen müssen eingeführt, alte geändert oder abgemanagt werden. Deshalb darf der SOC-Vertrag nicht statisch sein.

Nun lässt sich jeder Vertrag durch eine Vereinbarung der Parteien ändern. Das nutzt aber einem SOC-Provider nichts, der 90 Prozent seiner Kunden zu einer solchen Vereinbarung bewegen kann, bei 10 Prozent der Kunden aber einen alten Vertrags- und Leistungsstand parallel zum aktuellen Stand betreiben muss. Der Vertrag muss daher entsprechende Mechanismen vorsehen, nämlich in der Regel eine AGB-sichere Klausel, die Vertragsänderungen unter bestimmten Bedingungen mit angemessener ⇨

Ankündigungsfrist erlaubt. In jedem Fall muss das Thema im Vertrag geregelt und in der Praxis – ausgesprochen sorgfältig – gemanagt werden.

4. Widerstehen Sie dem Lock-in

Aus Sicht des Providers ist es verlockend, Kunden per „Lock-in" zu binden, also einen Wechsel des Anbieters zu erschweren. Das ist bei komplexen Dienstleistungen auch gar nicht übermäßig schwer. Ich rate aber ab: Reisende soll man nicht aufhalten und Kunden, die nur per Zwang beim Anbieter bleiben, sind keine gute Referenz. Zuletzt führt ein übertriebener Lock-in häufig zu unangenehmen und nur selten zielführenden Rechtsstreitigkeiten. Stattdessen sollte der SOC-Vertrag klare Regelungen vorsehen, wie nach Vertragsbeendigung die Leistungen zu einem anderen Anbieter überführt oder auch inhouse erbracht werden können. Dazu gehören Festlegungen betreffend die Übergabe von Dokumentationen, Datenexporten in interoperablen Formen und ein geordneter Übergabeprozess. Es spricht übrigens nichts dagegen, sich das als Anbieter vergüten zu lassen.

Bild: Trautmann

Der Autor

Rechtsanwalt Arne Trautmann ist seit 2009 als Außensozius bei der SNP Schlawien Partnerschaft mbB Rechtsanwälte Steuerberater in München und Sofia tätig. Zu Trautmanns Schwerpunkten gehört das Vertragsrecht im Tech-Bereich. Lesenswert ist auch sein Blog zu diesem Thema: https://vertrags.blog/

5. Und natürlich: Compliance und Datenschutz

Natürlich bleiben auch SOC-Verträge von Anforderungen der Compliance und des Datenschutzes nicht verschont. Es ist Wesen der Dienstleistung, dass Zugang zu sensiblen und geschützten Daten gewährt wird. Häufig sind das nicht nur die des Kunden, sondern auch von dessen Kunden und Geschäftspartnern. Der SOC-Vertrag muss daher oft begleitet werden von einem Auftragsverarbeitungs-Vertrag nebst Dokumentation der technisch-organisatorischen Maßnahmen oder eines umfassenden Datenschutzkonzeptes.

Gerade große Kunden können und wollen keine Sourcing-Entscheidungen ohne ein grünes Licht ihrer Compliance-Abteilung treffen. Ein souveränes Handling der datenschutzrechtlichen Anforderungen und notwendigen Dokumentationen ist somit ein echtes Sales-Tool gerade im Up-Market.

Fazit: Alter Wein in neuen Schläuchen?

Wie so häufig: Viele Tipps und Ratschläge für die sinnvolle Gestaltung von SOC-Verträgen klingen wie alter Wein in neuen Schläuchen. Und sind sie auch: SOC-Leistungen sind in gewisser Weise ja auch „nur" ein neuer Mix von vorher bekannten Leistungen in sinnvoller Verpackung. Also: Alter Wein vielleicht, aber neu gemischt. □

Sicherheitsbaustein Cyberversicherung

Die Cyberversicherung ist Teil eines umfassenden Risikomanagements. Welche Voraussetzungen müssen Unternehmen für einen Abschluss erfüllen? Welche Leistungen bekommen sie dafür? Wie können Dienstleister unterstützen?

Von Ira Zahorsky, IT-BUSINESS

„Cyberangriffe werden unversicherbar", orakelte Mario Greco, Chef des Zurich-Versicherungskonzerns, Ende vergangenen Jahres. Welche Unternehmen brauchen überhaupt eine Cyberversicherung? Eigentlich alle. Dem Allianz Risk Barometer 2023 zufolge, bereiten Cybergefahren den Unternehmen zum zweiten Mal in Folge mit die größten Sorgen. Die jährlichen finanziellen Schäden in Deutschland bezifferte der Bitkom mit 203 Milliarden Euro. 200.000 Euro pro Schadenfall nennt die Cyber-Direkt-Studie „Risikolage 2022". Dass die Versicherungskonzerne deshalb die Prämien im vergangenen Jahr um 50 bis 100 Prozent erhöht haben, wundert daher nicht. Denn digitale Bedrohungen sind schwer kalkulierbar. Auch für die Unternehmen. Speziell für kleinere Unternehmen kann ein Vorfall das finanzielle Aus bedeuten.

Bei großen Unternehmen ist eine Cyberversicherung inzwischen Standard. Kleine und mittelgroße Firmen sehen oft nur die Kosten, die eine solche Versicherung verursacht. Denn es geht nicht nur um die Beiträge. Auch die Voraussetzungen, die von den Versicherern gefordert werden, kosten Geld. Bedenkt man aber, dass die Absicherungsmaßnahmen sowieso zu einem zeitgemäßen Risikomanagement gehören, relativiert sich der finanzielle Aufwand einer Cyberversicherung wieder.

Vorgaben der Versicherungsgesellschaften

Goethes Weisheit „Was man Schwarz auf Weiß besitzt, kann man getrost nach Hause tragen" passt bei Versicherungen nicht immer. Im Schadensfall versuchen sich die Konzerne vor der Zahlung zu drücken, wenn die vereinbarten Voraussetzungen nicht zu 100 Prozent erfüllt wurden. Die verpflichtenden Kriterien für den Abschluss einer Cyberversicherung sind zahlreich, aufgrund des schlecht kalkulierbaren Risikos aber für die Versicherungen essentiell. Viele Anträge werden abgelehnt, wenn das Schutzniveau nicht hoch genug ist. Im Gegenzug kann ein sehr hohes Schutzniveau die Beiträge im Rahmen halten. Zu den Vorgaben der Versicherungsgesellschaften zählt unter anderem, dass die Daten durch regelmäßige Backups gesichert werden müssen. Auf den Zugangsgeräten der (remote) Mitarbeitenden muss die aktuellste Version eines Antivirenprogramms installiert sein. Für die Identitäts- und Zugriffsverwaltung ist zumindest die Multifaktor-Authentifizierung (MFA) vorgeschrieben. Best Practice bei der Rechtevergabe im Identity Access Management ⇨

(IAM) ist das Least-Privilege-Prinzip, also entsprechende Rechte nur denjenigen einzuräumen, die sie für die Arbeit benötigen. IAM ist auch die Grundlage einer Zero-Trust-Strategie. Ein weiterer Baustein ist Extended Detection & Response (XDR). Wichtige Punkte im Risikomanagement sind PEN-Tests und, da der Mensch eine große Schwachstelle darstellt, die regelmäßige Mitarbeiterschulung. Versicherungsunternehmen fordern außerdem belegfähige Daten und automatische Messungen. Sonst wird im Schadensfall unter Umständen nicht gezahlt. Zudem nötig ist ein Fahrplan zur Schadensbegrenzung, sollte eine Cyberattacke erfolgreich sein.

Nur eine finanzielle Absicherung?

Welche Schäden deckt eine Cyberversicherung ab? Das sowie die Beitragsprämie sind abhängig vom vereinbarten Leistungsumfang. Grundsätzlich können unter anderem folgende Aspekte versichert werden:

- Wiederherstellung der IT-Systeme und Daten
- IT-Forensik (Entfernung der Schadsoftware)
- Lösegeldzahlungen bei Ransomware-Angriffen
- Gewährleistung der Geschäftskontinuität
- Kompensation des Umsatzausfalls
- Rechtskosten, auch Gerichtskosten
- Einkommensverluste
- Drittschäden (Schadenersatzforderungen)

Noch wichtiger als die finanzielle Absicherung ist im Schadenfall inzwischen die Hilfe von Incident-Response-Experten der Versicherungen. Diese hochqualifizierten Security-Spezialisten unterstützen das IT-Team vor Ort bei der Identifizierung der Ursache, der Eindämmung und Beseitigung des Schadens sowie der Wiederherstellung der IT-Systeme und Daten.

In Zeiten des Fachkräftemangels, der auch in der IT-Security vorherrscht, kann diese Hilfe die Rettung für ein Unternehmen sein. Auch ein eigener Incident-Response-Plan, der Rollen und Aufgaben klar verteilt, ist im Fall der Fälle hilfreich. Die Versicherung kann auch die Kommunikation mit den zuständigen Behörden übernehmen und sich um Presse- und Öffentlichkeitsmaßnahmen kümmern.

Unterstützung durch Lösungsanbieter und Dienstleister

Doch nicht alle Schäden können abgesichert werden. Der Vertrauensverlust bei den Kunden sowie der Reputationsverlust bei Geschäftspartnern sind hier an erster Stelle zu nennen. Zu bedenken ist auch, dass sich andere Cyberkriminelle die geleakten Daten im Darkweb für eine „Zweitverwertung“ beschaffen. Hat das Unternehmen nicht vorgesorgt, wird es erneut Ziel

Eine Cyberversicherung kann Unternehmen durch ihre Vorgaben bereits im Vorfeld auf Sicherheitslücken aufmerksam machen sowie im Krisenfall unterstützen. Dennoch kann sie nicht alle Schäden abdecken und ist deshalb nur ein Teil einer umfassenden Sicherheitsstrategie.

eines Angriffs. Nicht von der Hand zu weisen ist auch, dass sich Ransomware-Angreifer gezielt Unternehmen mit einer Cyberversicherung als Opfer aussuchen, da sie hier ihre Chance auf eine Zahlung, meist in Kryptowährung, besser einschätzen.

Security-Lösungsanbieter und -Dienstleister können ihre Kunden auf unterschiedliche Weise unterstützen. Bei der Beratung sollte ein Fokus auf die Software-Automatisierung gelegt werden. Denn vor allem bei KMU ist die Personaldecke oft dünn und die IT-Verantwortlichen betreuen die IT-Security quasi nebenher mit. Automatisierungen filtern hier beispielsweise nur die wirklich wichtigen Security-Vorfälle heraus. Ebenso erleichtert entsprechende Software mittels automatisierter Reportings die Prüfungsverfahren der Versicherung und bietet dieser Transparenz.

Zahlreiche Anbieter haben Security Operations Center (SOC) als Dienstleistung im Portfolio. Ein SOC-Team kümmert sich um die Entwicklung eines Notfallplans und wertet auch den Erfolg der Reaktion auf Vorfälle aus. Weiterhin übernehmen Security-Hersteller inzwischen oft Awareness Trainings für die Mitarbeitenden des Kunden. Investitionen in eine gute Sicherheitsstruktur lohnen sich auf jeden Fall, verhindern sie doch bestenfalls, dass der Schaden gar nicht erst entsteht. □

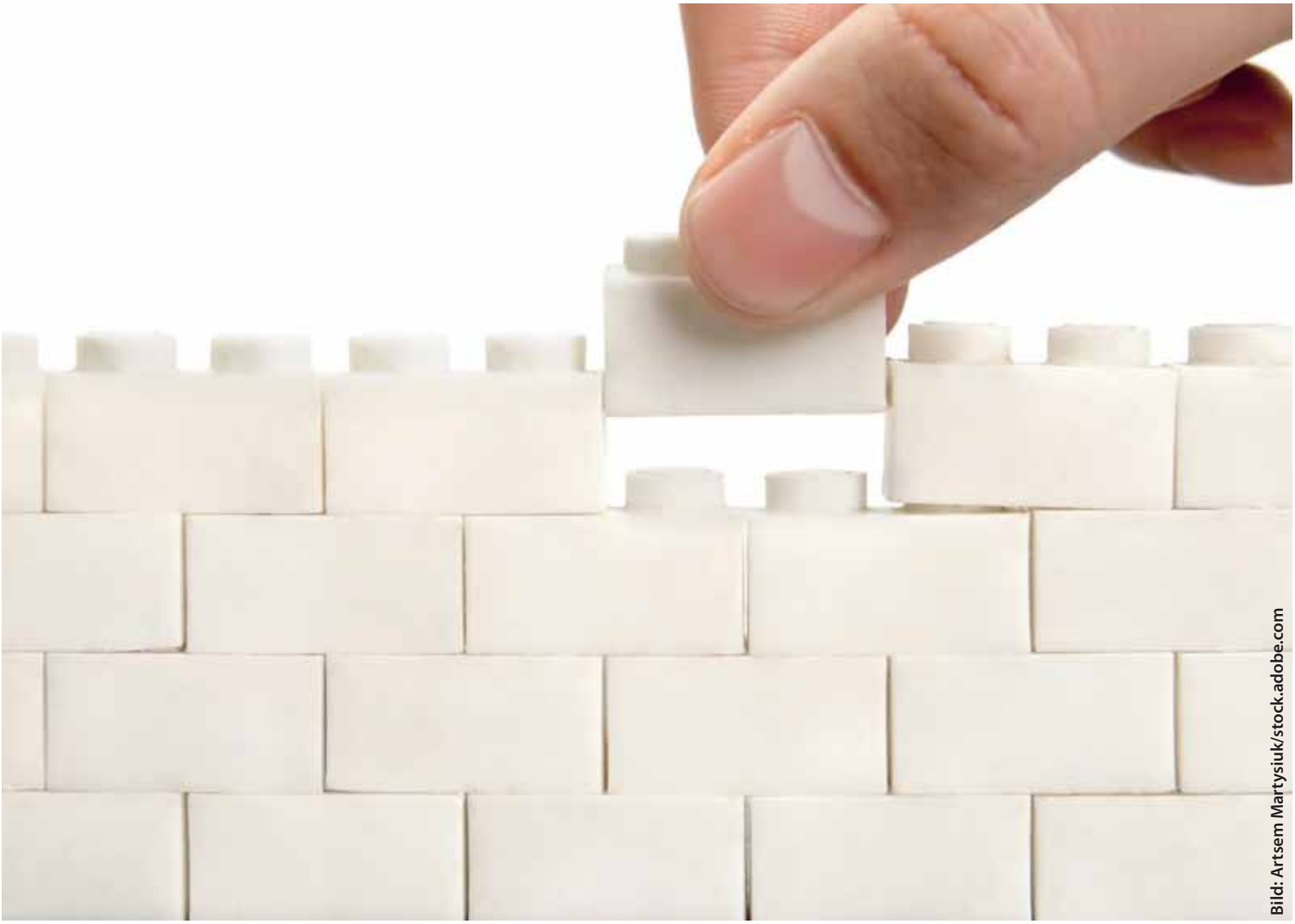


Bild: Artsem Martysiuk/stock.adobe.com

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:
Werner Nieberle, Günter Schürger, Tobias Teske

IT-BUSINESS

Redaktion: Sylvia Lösel/sl (-144) – Chefredakteurin, Heidi Schuster/hs (-122) – CvD/ltd. Redakteurin

Co-Publisher: Lilli Kos (-300)
(verantwortlich für den Anzeigenteil)

Account Management:
Besa Agaj/International Accounts (-112), Stephanie Steen (-211)
eMail media@vogel-it.de

SECURITY-INSIDER.DE

Redaktion: Peter Schmitz/ps (-165) – Chefredakteur, Jürgen Paukner/jp – CvD

Co-Publisher: Markus Späth (-138)

Key Account Management:
Brigitte Bonasera (-142), Vitalis Donhauser (-179), Philipp Emering (-129), Hannah Lamotte (-169)

Anzeigendisposition: Mihaela Mikolic (-204)

Grafik & Layout: Brigitte Krimmer, Johannes Rath, Udo Scherlin, Carin Böhm (Titel)

EBV: Carin Böhm, Brigitte Krimmer

Anzeigen-Layout: Johannes Rath

Adressänderungen/Vertriebskoordination:
Thomas Kragler (-301)
eMail vertrieb@vogel-it.de

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

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

Die wichtigsten Angebote des Verlages sind **IT-BUSINESS, eGovernment Computing, BigData-Insider, Blockchain-Insider, CloudComputing-Insider, DataCenter-Insider, Dev-Insider, IP-Insider, Security-Insider** und **Storage-Insider.**

Inserenten

Enginsight GmbH	Jena	https://www.enginsight.com/de/	26
G DATA Software AG	Bochum	https://www.gdata.de	14, U2
Insentis GmbH	Geisenheim	https://insentis.com	40
NCP engineering GmbH	Nürnberg	https://www.ncp-e.com/de/	20, U4
retarus GmbH	München	https://www.retarus.com/de/	44
sayTEC AG	München	https://www.saytec.eu	50
Securepoint GmbH	Lüneburg	https://www.securepoint.de	8
TDT AG	Essenbach	https://tdt.de/de/	32
Vogel IT-Akademie	Augsburg	https://www.vogelitakademie.de	5


NCP
Zero Trust
Cyberbedrohungen, Homeoffice und technologische Strategien wie SASE, Single Sign-On, SD-WAN oder Zero Trust stellen IT-Abteilungen vor Herausforderungen.
Schützen Sie Ihr Unternehmen mit der NCP Secure Enterprise Lösung und sichern Sie auch moderne Cloud-Technologien wie SD-WAN, SASE, SAML/SSO und Zero Trust durch zukunftssichere VPN-Technik ab.
Besuchen Sie NCP in Halle 7A – Stand 412!
Mehr Infos auf unserer Webseite!
NCP my access
SecurITy made in Germany
www.ncp-e.com