OKTOBER 2024

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

MADE IN GERMANY

VOGEL IT MEDIEN

Eine Publikation von IT-BUSINESS SECURITY INSIDER

Powered by:

G DATA CyberDefense

TRUST IN GERMAN SICHERHEIT

Den Angreifern voraus

Unsere Experten-Workshops auf der it-sa 2024 für Ihren Wissensvorsprung.

22.10.24

- Angst vor dem Cyberangriff? Richtig vorbereiten – Vorfällen gelassener begegnen
- Angriffsabwehr als Service: Wie MXDR aktive Angreifer aufspürt

23.10.24

- Penetration Tests In der Praxis – Fallbeispiele aus realen Projekten
- Angriffsabwehr als Service: Wie MXDR aktive Angreifer aufspürt

24.10.24

- Cyber-Resilienz: Ohne sicherheitsbewusste Mitarbeitende keine Abwehrkräfte
- Angriffsabwehr als Service: Wie MXDR aktive Angreifer aufspürt

Jetzt anmelden

Falls Sie nicht vor Ort sein können, nehmen Sie einfach remote an den Workshops teil. Wir freuen uns auf Sie!

it sa

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

Bild: TeleTrusT

Liebe Leserinnen und Leser,

in einer Welt, die zunehmend von Digitalisierung geprägt ist, wird die Bedeutung von IT-Sicherheit immer offensichtlicher. Cyberangriffe, Datenlecks und digitale Bedrohungen sind nicht nur Schlagzeilen in den Nachrichten, sondern auch reale Herausforderungen, denen Unternehmen und Privatpersonen täglich gegenüberstehen.

Der aktuelle Stand der IT-Sicherheit in Deutschland zeigt, dass sowohl der öffentliche als auch der private Sektor zwar verstärkt in Sicherheitsmaßnahmen investieren, jedoch stetige Anpassung und Weiterentwicklung essentiell sind, um die Cyberabwehr zu stärken und die Resilienz gegen Angriffe zu erhöhen. Die Bedrohung durch Cyberkriminalität bleibt hoch.

In dieser Publikation möchten wir Ihnen einen umfassenden Überblick über die aktuellen Trends und Herausforderungen im Bereich der IT-Sicherheit bieten. Wir beleuchten nicht nur technische Lösungen, sondern auch organisatorische Ansätze und Best Practices, die Unternehmen und Organisationen dabei unterstützen können, ihre Sicherheitsarchitektur zu stärken.

Wir möchten betonen: IT-Sicherheit ist kein einmaliges Projekt, sondern ein fortlaufender Prozess, der enge Zusammenarbeit und vernetzte Koordination voraussetzt.

Im Namen von TeleTrusT wünsche ich eine interessante Lektüre. □

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.

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.

it-sa Expo&Congress

Besuchen Sie uns in **Halle 9 - Standnummer 9-503**

infodas
connect more. be secure.

SDoT Industry Gateway.

Effektiver Schutz sensibler Daten in Kritischen Infrastrukturen – militärisch & geheimdienstlich bewährt!

Das infodas SDoT Industry Gateway bietet dem privaten Sektor einen konsequenten Schutz vor steigenden Cyberattacken. Die Cross Domain Solution entspricht den höchsten Zertifizierungslevels und gewährleistet einen vollständig gesicherten und kontrollierten Datenaustausch zwischen verschiedenen Sicherheitsdomänen (IT/OT). Lösungen von infodas, einem Airbus Cyber & IT Tochterunternehmen, sind auf Militärniveau bewährt und für die Anforderungen des Industriesektors optimiert. Profitieren Sie von unserer 50-jährigen Erfahrung in der Absicherung höchster Geheimhaltungsstufen.

Let`s get in touch:
KRITIS Team
KRITIS@infodas.com

www.infodas.com | info@infodas.de

Vertrauen hat einen Namen

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

Träger des Vertrauenszeichens "IT Security made in Germany" (Stand 11.09.2024)

- Accellence Technologies GmbH
- AceBIT GmbH
- achelos GmbH
- Achtwerk GmbH & Co. KG
- ads-tec GmbH
- Adva Network Security GmbH
- agilimo Consulting GmbH
- aigner business solutions GmbH
- AirID GmbH
- Allgeier CyRis GmbH
- Alpha Strike Labs GmbH
- Alter Solutions Deutschland GmbH
- ANMATHO AG
- Anqa IT-Security GmbH
- Antago GmbH
- APRO Computer & Dienstleistung GmbH
- apsec Applied Security GmbH
- ASOFTNET
- arian IT Service GmbH
- ATIS systems GmbH
- Atruvia AG
- AUCONET Solutions GmbH
- AUTHADA GmbH
- authenton GmbH
- AWARE7 GmbH
- axilaris GmbH
- Bank-Verlag GmbH
- Bare.ID GmbH
- Bechtle GmbH & Co. KG
- Beta Systems IAM Software AG
- Biteno 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
- COGNITUM Software Team GmbH
- COMback Holding GmbH
- comcrypto GmbH
- comforte AG
- comtime GmbH
- Condition-ALPHA Digital Broadcast Technology Consulting
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- Cybersense GmbH
- dacoso GmbH
- dal33t GmbH
- DATAGROUP Cyber Security GmbH
- DATAGROUP Defense IT Services GmbH
- DATAKOM GmbH
- DATUS AG
- DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
- DERMALOG Identification Systems GmbH
- Detack GmbH
- DF Deutsche Fiskal GmbH
- DFN-CERT Services GmbH
- Digital Enabling GmbH
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- Dirk Losse Consulting
- ditis Systeme Niederlassung der JMV GmbH & Co.
- DoctorBox GmbH
- Dreyfield & Partner Deutschland GmbH
- DriveLock SE
- D-Trust GmbH
- EBRAND AG
- 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
- Green IT Services GmbH
- HDPnet GmbH
- HiScout GmbH
- HK2 Rechtsanwälte
- Hornetsecurity GmbH
- if(is) – Institut für Internet-Sicherheit
- Infineon Technologies AG
- INFODAS GmbH
- Inlab Networks GmbH
- INNOSYSTEC GmbH
- innovaphone AG
- Insentis GmbH
- INSYS MICROELECTRONICS GmbH
- intarsys GmbH
- intelliCard Labs GmbH
- isits AG International School of IT Security
- ISL Internet Sicherheits-lösungen GmbH
- ITConcepts PSO GmbH
- ITnovate UG

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 □

- ITSG GmbH
- itWatch GmbH
- keepbit IT-SOLUTIONS GmbH
- KikuSema GmbH
- KOBIL GmbH
- KraLos GmbH
- Kroll Strategieberatung GmbH
- LANCOM Systems GmbH
- LEIBOLD Sicherheits- und Informationstechnik GmbH
- limes datentechnik® gmbh
- Linogate GmbH
- LocateRisk UG
- MACONIA GmbH
- maincubes Holding & Service GmbH
- Maltego Deutschland GmbH
- MaskTech GmbH
- Materna Virtual Solution GmbH
- metafinanz GmbH
- MGR Integration Solutions GmbH
- Mitigant GmbH
- M&H IT-Security GmbH
- MTG AG
- MTRIX GmbH
- Mühlbauer ID Services GmbH
- NCP engineering GmbH
- ndaal GmbH & Co. KG
- Neosec GmbH
- NetComProtect
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- Nexis GmbH
- Nexis GRC GmbH
- nicos AG
- nicos cyber defense GmbH
- Nimbus Technologieberatung GmbH
- OctoGate IT Security Systems GmbH
- ondeso GmbH
- ONEKEY GmbH
- Opexa Advisory GmbH
- OTARIS Interactive Services GmbH
- O&O Software GmbH
- P3KI GmbH
- pen.sec AG
- PFALZKOM GmbH
- PHOENIX CONTACT Cyber Security 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
- Red Lion Europe GmbH
- retarus GmbH
- Robin Data GmbH
- Rohde & Schwarz Cybersecurity GmbH
- r-tec IT Security GmbH
- SAMA PARTNERS Business Solutions GmbH
- sayTEC AG
- Schönhofer Sales and Engineering GmbH
- SCHUTZWERK GmbH
- SC-Networks GmbH
- Sec2do GmbH
- Secorvo Security Consulting GmbH
- secrypt GmbH
- SECUDOS GmbH
- secunet Security Networks AG
- Secure Service Provision GmbH
- Securepoint GmbH
- SECURITYSQUAD GmbH
- secuvera GmbH
- SEPPmail – Deutschland GmbH
- sequrium GmbH
- SerNet GmbH
- signotec GmbH
- Skyflare GmbH
- Smartify IT Solutions GmbH
- 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
- TÜV Informationstechnik GmbH
- TÜV Rheinland i-sec GmbH
- TWINSOFT biometrics GmbH & Co. KG
- Uniscon GmbH
- UNIKI GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- VisionmaxX GmbH
- Voleatech GmbH
- water IT Security GmbH
- whitemacs GmbH
- Würzburger Versorgungs- und Verkehrs GmbH
- XignSys GmbH
- XnetSolutions KG
- Zertificon Solutions GmbH

NIS-2 in der Praxis: So gelingt die Umsetzung für Unternehmen

Cyberangriffe beeinträchtigen das gesellschaftliche Leben. Um Europa zu schützen, gibt es deshalb die NIS-2-Richtlinie. Doch wie gelingt die Umsetzung? Von Johannes Niederer, secunet Security Networks AG

NIS-2-Richtlinie: Europas Werkzeug gegen Cyberbedrohungen

Mit der NIS-2-Richtlinie soll ein hohes Cybersicherheitsniveau auf EU-Ebene geschaffen sowie der Binnenmarkt gestärkt werden. Die „EU Directive on Security of Network and Information Systems" versteht sich als eine Weiterentwicklung der ursprünglichen EU NIS-Richtlinie. Dabei geht es nicht nur darum, volkswirtschaftlich bedeutsame Unternehmen und kritische Einrichtungen vor Cyberangriffen zu schützen, ihnen sollen auch Leitlinien an die Hand gegeben werden, wie sie auf Angriffe reagieren können.

Nach der Veröffentlichung der NIS-2-Richtlinie am 27. Dezember 2022 folgte das Inkrafttreten am 16. Januar 2023 – seitdem läuft die Uhr für alle EU-Mitgliedsstaaten. Bis Oktober 2024 haben sie Zeit, die Richtlinie in nationales Recht umzusetzen.

In Deutschland existiert mittlerweile ein Gesetzentwurf der Bundesregierung mit dem Titel „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz), welcher zeitnah verabschiedet werden soll.

Wie bereiten sich Unternehmen am besten vor?

Unternehmen sollten zunächst prüfen, ob und wie sie von dem neuen Gesetz betroffen sein werden. Dazu empfiehlt sich eine Betroffenheitsanalyse mit den Parametern Sektor-Zugehörigkeit, Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme.

Betroffene Unternehmen sollten im nächsten Schritt eine sogenannte Gap-Analyse durchführen. Unternehmen, die bereits in der Vergangenheit verpflichtet waren, Maßnahmen zur Informationssicherheit umzusetzen (wie z. B. Betreiber kritischer Anlagen), sind gut vorbereitet und müssen mit geringen Anpassungen rechnen.

secunet bietet Unternehmen mit dem NIS-2-Check-up eine Standortbestimmung, die ihnen Aufschluss über ihre Compliance-Situation gibt und potenzielle Sicherheitslücken aufdeckt. Unternehmen müssen jetzt handeln – denn die NIS-2-Richtlinie kommt, daran führt kein Weg vorbei. ■

Was tun Sie bei einem Hackerangriff?

Entspannt bleiben – denn mit secunet sind Daten und Infrastruktur premiumsicher.

Wo Daten und IT-Infrastrukturen vor Cyberangriffen geschützt werden müssen, steht secunet bereit. Als IT-Sicherheitspartner der Bundesrepublik Deutschland bieten wir Behörden und Unternehmen Expertenberatung und premiumsichere Lösungen zum Schutz von Kommunikation und Daten.

secunet.com **protecting digital infrastructures**

secunet

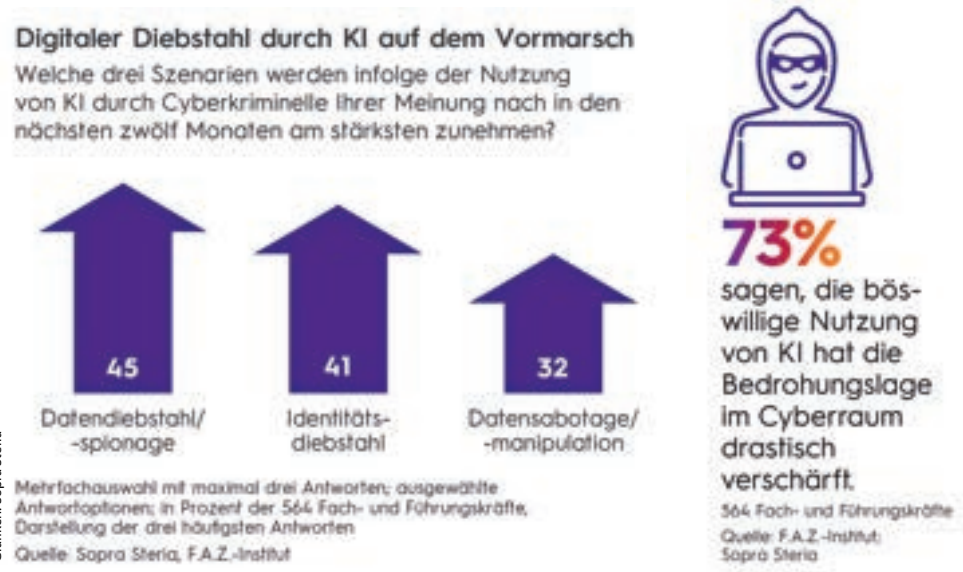
Cybersicherheit in Zeiten von Künstlicher Intelligenz

Rund zwei Drittel der Erwerbstätigen in Deutschland nutzen regelmäßig KI-Anwendungen im Arbeitsalltag. Eine Studie von Sopra Steria zeigt, dass sich eine Mehrheit der befragten Unternehmen und Behörden um das Bedrohungspotenzial von Cyberattacken sorgt.

Von Sophia Kos, IT-BUSINESS

Mit der Studie „Cybersecurity im Zeitalter von KI“ (Juni 2024) gibt Sopra Steria Einblicke in den Arbeitsalltag von 1.003 Erwerbstätigen sowie 564 Fach- und Führungskräften von Unternehmen und Behörden. Dabei zeigen die Ergebnisse, dass Künstliche Intelligenz längst im Berufsleben angekommen ist. Demnach verwenden circa zwei Drittel der Erwerbstätigen

Bild: everythingpossible - stock.adobe.com



Grafiken: Sopra Steria

ChatGPT und Co. zumindest teilweise, 37 Prozent arbeiten regelmäßig mit KI-Anwendungen. Die Befragten sorgen sich allerdings dennoch um die steigende Bedrohung durch Cyberattacken.

Drei Viertel der Unternehmen und Behörden sehen eine wachsende Bedrohungslage bezüglich Cyberkriminalität. Demnach plant jede dritte Organisation, in den kommenden 12 Monaten in eine KI-basierte Cybersecurity-Strategie zu investieren. Bereits jede vierte verwendet KI-gesteuerte Systeme zur Erkennung von Cyberangriffen.

„Cybersicherheit wird zwingend benötigt, um die Digitalisierung voranzutreiben, sensible Daten zu schützen, die Verfügbarkeit digitaler Assets zu garantieren und die Aufrechterhaltung des Geschäftsbetriebs zu sichern. Allerdings rüsten sich Cyberkriminelle mit KI weiter auf, so dass sich Unternehmen und Behörden neu aufstellen müssen", erklärt Olaf Janßen, Head of Cybersecurity bei Sopra Steria. Das Bedrohungspotenzial durch Cyberattacken in Unternehmen und Behörden hat deutlich zugenommen. Allein im vergangenen Jahr entstand der deutschen Wirtschaft durch lahmgelegte Computersysteme, Datenlecks sowie Lösegelderpressungen ein Schaden von 148 Millionen Euro, bestätigt der Branchenverband Bitkom. So wird durch den Einsatz von KI nach Ansicht der befragten Fach- und Führungskräfte die Bedrohungslage weiter zunehmen. In den kommenden 12 Monaten rechnen schon 45 Prozent mit mehr Datendiebstahl.

Dabei spielt speziell generative Künstliche Intelligenz (GenAI) eine große Rolle in Zeiten der Cybersecurity. „Cyberkriminelle nutzen diese, um ihre Attacken zu personalisieren und zu automatisieren. GenAI lässt den Enkeltrick 2.0 beispielsweise noch authentischer wirken und analysiert Beziehungen in sozialen Netzwerken, um Angriffe individueller zu gestalten. Mit Sprachmodellen (Large Language Models) können Websites derart angegriffen werden, dass eine KI von der Reaktion auf einen Angriff lernt und ihre Angriffsvektoren wie Phishing ⮑

oder das Ausnutzen von Sicherheitslücken für eine zweite, verbesserte Attacke anpasst", sagt Janßen.

Prävention statt Reaktion

Bei einer Mehrheit der befragten Fach- und Führungskräfte steigen angesichts der neuen Möglichkeiten die Bedenken, geht es um die Verschiebung der Kräfteverhältnisse in Richtung der Angreifer. So sind 71 Prozent der Meinung, dass Cyberkriminelle KI besser zum Angriff nutzen, als dies Unternehmen zur Abwehr tun. Im Gegenzug wächst bei den befragten Organisationen zeitgleich das Bewusstsein für eine KI-basierte Cybersecurity.

Demnach hat jede dritte Organisation erkannt, dass es auch für den Schutz von IT-Systemen neue Möglichkeiten gibt. 54 Prozent sehen ohne den Einsatz von KI künftig keine Chance mehr gegen Cyberangriffe. „Mit dem Einsatz

von KI in der Threat Detection können Unternehmen und Behörden zusätzlich eine auf dem Erkennen von Anomalien basierende Überwachung etablieren und so neuartige Angriffe früher aufspüren", kommentiert Janßen.

Schwachstelle Mensch

Dass auch im Zeitalter der Künstlichen Intelligenz der Mensch die größte Gefahr für erfolgreiche Cyberangriffe bleibt, zeigen folgende Ergebnisse: 43 Prozent der Fach- und Führungskräfte sehen unangemessene Reaktionen der Mitarbeitenden auf Phishing-Angriffe als größte Schwachstelle. Zusätzlich stellen falsche Reaktionen auf KI-gestütze Social-Engineering-Angriffe für 34 Prozent ein erhebliches Risiko dar. „Phising-E-Mails sind unter anderem deswegen so gefährlich, da sie kaum mehr als solche zu erkennen sind. Zielgruppengerechte Schulungen und konkrete Handlungsanweisungen sind unerlässlich", so Stefan Beck, Senior Manager im Team Cybersecurity bei Sopra Steria. „Das Einfallstor Mensch kann nie ganz geschlossen werden, so dass auch technische Elemente genutzt werden müssen. Durch entsprechende Tools landen Phishing-Mails nicht im Postfach, und der Klick auf einen Malware-Link führt nur in eine Sandbox."
Weitere unterschätzte Gefahren lauern in der ungeregelten Verwendung von KI-Anwendungen (26 Prozent) sowie nicht ausreichenden Regelungen und Sicherheitsbestimmungen für die Arbeit im Homeoffice (23 Prozent). Darüber hinaus gaben 65 Prozent der Erwerbstätigen an, KI-Tools im Beruf zu nutzen, allerdings informiert nur bei 41 Prozent der Arbeitgeber über Schulungen, Leitlinien und Empfehlungen. □

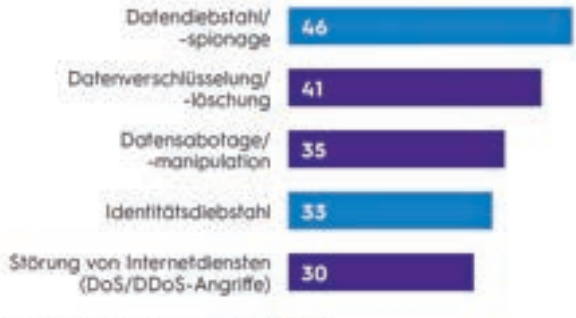
KI wird immer wichtiger

In welche Bereiche plant Ihre Organisation in den nächsten zwölf Monaten zu investieren, um die eigene Cybersecurity noch einmal zu erhöhen?

Mehrfachauswahl, in Prozent der 564 Fach- und Führungskräfte; ohne „weiß nicht/keine Angabe" (11%)
Quelle: F.A.Z.-Institut; Sopra Steria

Sorge vor Daten- und Identitätsdiebstahl

Welche drei Szenarien im Cyberraum verursachen Ihrer Ansicht nach derzeit den größten Schaden für Organisationen aus Ihrer Branche?



Mehrfachauswahl mit maximal drei Antworten, in Prozent der 564 Fach- und Führungskräfte. Darstellung der fünf häufigsten Antworten
Quelle: F.A.Z.-Institut; Sopra Steria

The future of Cloud-to-Site

Standortvernetzung neu gedacht – Vertrauen im Sinne von Zero Trust

In unserer weit vernetzten Welt funktioniert ohne verlässlichen Datenaustausch praktisch gar nichts mehr. Egal, ob im privaten Umfeld, im Job oder bei öffentlichen Einrichtungen – überall werden täglich Informationen auf unterschiedlichste Weise übertragen und müssen dabei natürlich auch abgesichert werden. Gerade letzteres stellt häufig die weitaus größere Herausforderung dar. Wie schafft man es im Zeitalter von Hackerangriffen und Cyberattacken, Daten wirklich sicher von A nach B zu schicken?

Diese Problematik löst NCP mit seinen Next Gen VPN Produkt-Innovationen zur it-sa 2024, die neue Maßstäbe in Sachen Flexibilität bei der Standortvernetzung setzen.
Gerade im Bereich der Standortvernetzung kommt es auf netzwerktechnischer Ebene für Unternehmen oder öffentliche Einrichtungen immer wieder zu IP-basierten Hürden und Überschneidungen. Durch die neue Cloud-to-Site-Funktion unseres NCP Secure Enterprise VPN Servers werden Eindeutigkeiten für sich überschneidende IP-Bereiche geschaffen. Dies ermöglicht auch bei der Vernetzung IP-technisch identischer Strukturen eine eindeutige Adressierbarkeit aller Netzwerkkomponenten.
Von besonderer Wichtigkeit ist dabei auch die weitreichende Kompatibilität mit allen Arten von Infrastrukturen. Schließlich verlagern manche Einrichtungen manche Teile ihrer Security-Strategie in die Cloud und nutzen dafür unterschiedliche Technologien/Konzepte wie SASE, SD-WAN, SSE, Single Sign-On durch SAML oder Zero Trust. Durch den softwarebasierten Security-Ansatz aller NCP-Produkte ist die Cloud-to-Site-Optimierung auch innerhalb von Cloud-Infrastrukturen vollständig anwendbar. Auf diese Weise erschließen sich gänzlich neue Anwendungsbereiche für Standortvernetzungen – egal, ob Cloud-to-Site, Site-to-Cloud oder klassisches Site-to-Site. Das zugriffsbasierte Vertrauen im Sinne von ZTNA wird hierbei ebenfalls gewahrt.

Modern Remote Access at its best

Zusätzlich dazu erweitern wir unsere moderne Next Gen VPN-Lösung um die Option des Application-Based-Split-Tunneling. Läuft ausnahmslos jeder Traffic des Unternehmens

durch den VPN-Tunnel, kann das schnell zu einer Überlastung des entsprechenden VPN-Servers führen. Gerade größere Datenbrocken wie Videos, die gleichzeitig aber in vielen Fällen keine sicherheitstechnische Relevanz haben, belasten den Server stark und vermindern die Geschwindigkeit, mit der tatsächlich schützenswerte Dokumente übertragen werden. Abhilfe schafft das Split-Tunneling, welches nun noch einfacher konfiguriert werden kann. Administratoren bestimmen nun mit wenigen Mausklicks, welcher Traffic durch den hochsicheren VPN-Tunnel geleitet werden soll – und das auf Anwendungsebene gemäß dem Zero-Trust-Prinzip! Das manuelle Pflegen langer IP-Adresslisten entfällt somit vollständig.

Features, die Admins & User freuen

Als weitere Messe-Neuheit präsentiert NCP auf der it-sa exklusiv die Verbesserung der REST-API in seinem Enterprise-Management. Manuelle Administrationsarbeit ist einer der größten Zeitfresser in der IT und steht zeiteffizientem Arbeiten im Weg. Daher sollten so viele Aufgaben wie möglich automatisiert ablaufen, um nach einmaliger Einrichtung keine Ressourcen mehr dafür binden zu müssen. So profitieren IT-Abteilungen nun von gänzlich neuen Automatisierungsmöglichkeiten im Rahmen des NCP-Enterprise-Managements. Manuelle Update-Vorgänge und weitere zeitraubende Aufgaben gehören damit der Vergangenheit an.

Daran anknüpfend stellen wir auf der Messe auch die Überarbeitung des grafischen Interfaces unserer Client- und Management-Komponenten vor. Diese kombinieren ein modernes Design mit noch einfacherer Bedienung – sowohl für IT-Admins als auch Endnutzer. ■

Weitere Informationen zu den VPN-Neuheiten von NCP erfahren Sie auf der it-sa 2024 an unserem Stand 7A-408!

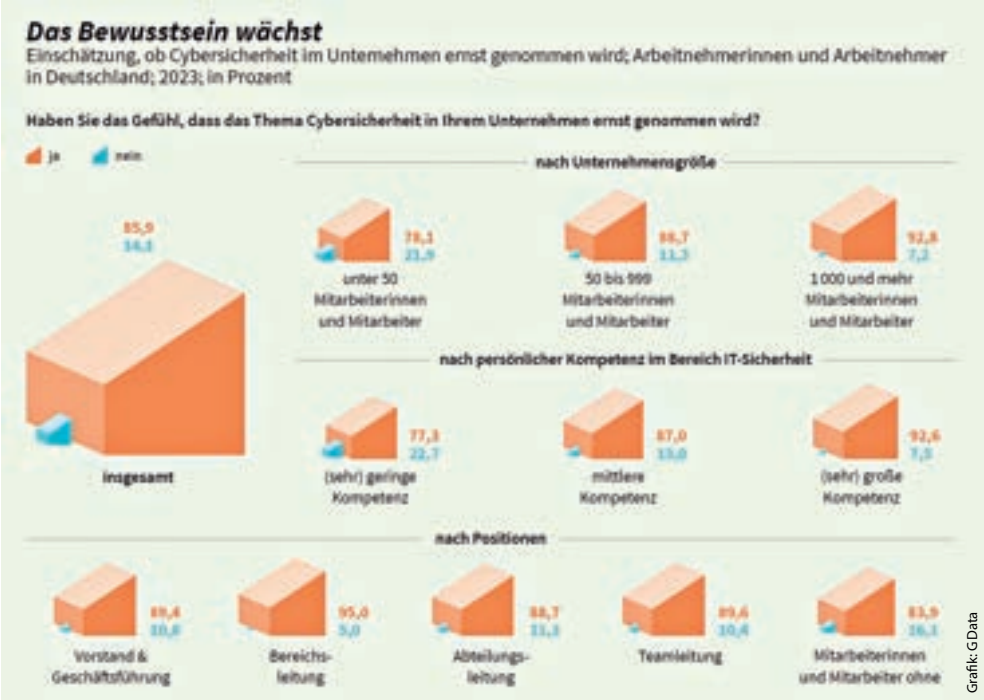
Cybersecurity: Immer noch keine Chefsache?

Cybersicherheit ist ein umfassendes Feld und darf bei der aktuellen Bedrohungslage nicht vernachlässigt werden. Viele Aspekte tragen zu einer ganzheitlichen Security-Strategie bei und sollten bei deren Planung berücksichtigt werden. G Data informiert mit Zahlen und Tipps.

Von Ira Zahorsky, IT-BUSINESS

Das Positive vorweg: Die Ergebnisse der Studie „Cybersicherheit in Zahlen" von G Data belegen, dass die IT-Sicherheit mehr in das Bewusstsein der Verantwortlichen rückt. Dies ist auch der medialen Aufmerksamkeit geschuldet, wenn Firmen Cyberkriminellen zum Opfer gefallen sind. Auch die ab Oktober verpflichtende NIS2-Richtlinie trägt dazu bei. Die Studie ergab

Bild: Sikov - stock.adobe.com



auch, dass die Awareness in Unternehmen mit mehr als 1.000 Mitarbeitenden größer ist, als in kleineren Unternehmen mit weniger als 50 Angestellten. Bei letzteren fehlt oft das Verständnis für IT-Sicherheitsmaßnahmen wie sichere Passwörter und Endgeräte, Softwareupdates und Datenschutz. In großen Firmen sind sowohl mehr Awareness als auch mehr Ressourcen vorhanden.

Eine große Bereitschaft, die IT-Sicherheit im Unternehmen zu erhöhen, ist dringend notwendig. „Jedes Unternehmen, unabhängig von Größe und Geschäftsfeld, ist ein potenzielles Ziel für Cyberkriminelle“, warnt Andreas Lüning, Vorstand und Mitgründer von G Data. „Die Gefahr besteht nicht nur für Großunternehmen, sondern auch für kleinere Betriebe, die oft den Irrglauben besitzen, nicht im Fokus von Angreifern zu stehen. Insbesondere als Teil einer Lieferkette von Großunternehmen müssen sie sich in der Verantwortung sehen, resilienter zu werden, um Teil einer Lieferkette zu bleiben.“ □

Cybersicherheit in Zahlen

Für die repräsentative Online-Studie „Cybersicherheit in Zahlen“ von G Data, Statista und brand eins wurden mehr als 5.000 Arbeitnehmer in Deutschland zur Cybersicherheit im beruflichen und privaten Kontext befragt.

Aktive Angriffsabwehr als Service mit Managed Extended Detection and Response

Als Cyber-Defense-Spezialist aus Deutschland steht G DATA für effektiven und umfassenden Schutz vor Cyberbedrohungen und einen vertrauensvollen Umgang mit Kunden. Auf der it-sa 2024 präsentiert die G DATA CyberDefense AG in Halle 7a, Stand 212 Managed Extended Detection and Response. Dank G DATA 365 | MXDR lösen Unternehmen gleich drei große Probleme bei ihrer Cyberabwehr: Fehlendes Spezialwissen, zu wenig Zeit und Personalmangel. Die Sicherheitslösung des deutschen Cyber-Defense-Experten sorgt für einen effektiven Rund-um-die-Uhr-Schutz.

Klassischer Virenschutz ist eine bewährte Sicherheitslösung in Unternehmen, die aber an ihre Grenzen stößt. Attacken sind heute oft individualisiert und dateilos, daher ist ein Virenschutz weniger effektiv. Es kommt darauf an, verdächtige Aktivitäten im Netzwerk frühzeitig zu entdecken und mit der richtigen Reaktion zu stoppen. Einen hundertprozentigen Schutz vor Cyberangriffen gibt es nicht, daher ist die schnelle Reaktion entscheidend für Unternehmen, um Schäden zu minimieren. G DATA 365 | MXDR leistet genau das. Die Reaktion erfolgt bei Managed Extended Detection and Response umgehend.

Überwachung rund um die Uhr durch G DATA

Die Überwachungsaufgaben übernimmt bei G DATA 365 | MXDR ein erfahrenes Analystenteam, das 24/7 im Einsatz ist. Die Expertinnen und Experten setzen unter anderem auf Threat Hunting für einen proaktiven Schutz vor Cyberangriffen. Das Team wertet die Sensorergebnisse aus, reagiert im Fall eines bestätigten Angriffs umgehend und isoliert zum Beispiel betroffene Endpoints. IT-Verantwortliche in Unternehmen werden über Vorfälle informiert.

Die Webkonsole bündelt alle relevanten Informationen und ermöglicht es Firmen-IT-Teams, Einsicht in Sicherheitsvorfälle und ergriffene Maßnahmen zu erhalten. Weiterhin führt das Analystenteam Root-Cause-Analysen (RCA) durch, um die Ursachen von Sicherheitsvorfällen zu identifizieren und daraus fundierte und für Kundinnen und Kunden verständliche Handlungsempfehlungen in deutscher Sprache abzuleiten.

Verlässlicher Partner

Durch die Nutzung von G DATA 365 | MXDR profitieren IT-Verantwortliche von der umfangreichen Expertise des deutschen Cyber-Defense-Spezialisten. Den Unternehmen stehen persönliche Ansprechpartner zur Seite, unterstützt von einem preisgekrönten 24/7-Support in deutscher Sprache. G DATA CyberDefense setzt auf eine direkte, persönliche Betreuung und nutzt eigens entwickelte Software zur Angriffserkennung, die kontinuierlich auf Basis von Kundenfeedback weiterentwickelt wird.

Beim Onboarding berät das Cyber-Defense-Unternehmen aus Bochum individuell und thematisiert aktiv das Thema Datenschutz. Dabei wird unter anderem festgelegt, auf welchen Endpoints welche spezifische Response ablaufen soll. Die Datenverarbeitung erfolgt ausschließlich auf Servern in Deutschland. Damit gelten die strengen deutschen Datenschutzrichtlinien. Der Schutz der Kundendaten sowie der Schutz vor Cyberbedrohungen stehen für G DATA CyberDefense an erster Stelle.

Kostenloses Workshop-Programm auf der it-sa

Mehr Informationen über das Aufdecken und Beenden von Cyberattacken, die passende Reaktion und wie Unternehmen ihre Resilienz gegen Angriffe steigern können, erhalten Interessierte auf der it-sa bei den kostenlosen Workshops von G DATA CyberDefense. Stefan Hausotte und Daniel Zessin referieren am 22. Oktober 2024 von 16 bis 17 Uhr, am 23. Oktober 2024 und am 24. Oktober 2024 jeweils von 11:30 bis 12:30 Uhr über „Angriffsabwehr als Service: Wie MXDR aktive Angreifer aufspürt“. Daneben bietet G DATA auf der it-sa in Nürnberg auch Workshops zu den Themen **Security Awareness** von Mitarbeitenden und den **Umgang mit IT-Sicherheitsvorfällen** an:

Unsere Experten-Workshops auf der it-sa 2024

22.10.24
- Angst vor dem Cyberangriff? Richtig vorbereiten – Vorfällen gelassener begegnen
- Angriffsabwehr als Service: Wie MXDR aktive Angreifer aufspürt

23.10.24
- Penetration Tests In der Praxis – Fallbeispiele aus realen Projekten
- Angriffsabwehr als Service: Wie MXDR aktive Angreifer aufspürt

24.10.24
- Cyber-Resilienz: Ohne sicherheitsbewusste Mitarbeitende keine Abwehrkräfte
- Angriffsabwehr als Service: Wie MXDR aktive Angreifer aufspürt

Interessierte finden G DATA CyberDefense vom 22. bis zum 24.Oktober 2024 auf der it-sa in Nürnberg in Halle 7a Stand 212.

Mehr Informationen über das G DATA Messeprogramm auf der it-sa, eine Anmeldemöglichkeit für die Workshops und kostenlose Messetickets hier:

Jetzt anmelden

Falls Sie nicht vor Ort sein können, nehmen Sie einfach remote an den Workshops teil. Wir freuen uns auf Sie!

Wege zu mehr Cloud-Sicherheit

Souveräne, öffentliche Cloud-Angebote ergeben sich aus Datenschutzgesetzen. Aufgrund der mangelnden Standardisierung dieser variieren die Angebote unter den Anbietern stark. Vor der Anwendung müssen I&O-Führungskräfte eine Sovereign-Cloud-Strategie auf drei Säulen aufbauen: Daten, Technologie und Betrieb.

Von Miguel Angel Borrega, Alessandro Galimberti, Ken Rothenberger und Rene Buest, Gartner

Für viele Unternehmen stellt die Cloud-Souveränität eine Herausforderung dar. Die Schwierigkeit besteht unter anderem darin, dass die Datenschutzverordnungen von Land zu Land variieren. Deshalb unterscheiden sich die Lösungen, um sensible Daten zu schützen, stark zwischen den Cloud-Anbietern.

Aktuell gibt es keine allgemein anerkannte Definition für den Begriff „Sovereign Cloud". Daher müssen I&O-Führungskräfte prüfen, ob ein Angebot mit der Bezeichnung „Souveräne Cloud" tatsächlich den Anforderungen des Unternehmens entspricht. Unternehmen, deren Souveränitätsanforderungen auf Infrastruktur- und Technologieunabhängigkeit beruhen, müssen bei der Einführung der Cloud meist auf Public-Cloud-Funktionen und Skalierung verzichten.


Bild: BalanceFormCreative - stock.adobe.com

Empfehlungen

- Definieren Sie zunächst, welche Souveränitätsanforderungen für Ihr Unternehmen relevant sind und zwar in jedem Land, in dem es tätig ist. So können Sie Ihre Cloud-Strategien für Souveränität umsetzen.
- Wählen Sie einen Anbieter, der sowohl die aktuellen als auch die zukünftigen Anforderungen der digitalen Souveränität bewertet.
- Führen Sie eine Auswirkungsanalyse durch, um zu bewerten, welche Cloud-Funktionen nach dem Wechsel möglicherweise entfallen.

Annahmen für die strategische Planung

Bis zum Jahr 2025 werden rund 30 Prozent der multinationalen Unternehmen mit Umsatzeinbußen, Markenschäden oder rechtlichen Schritten aufgrund von unkontrollierten digitalen Sicherheitsrisiken zu kämpfen haben. Bis 2028 werden über 50 Prozent der multinationalen Unternehmen Strategien zur digitalen Souveränität verfolgen. Momentan sind es weniger als 10 Prozent.

Viele Geschäftsprozesse und Unternehmensdaten werden auf Cloud-Plattformen bereitgestellt. Daher sorgen sich Unternehmen zunehmend über die Abhängigkeit von ausländischen Infrastrukturanbietern. Die Public-Cloud-Angebote der US-amerikanischen oder chinesischen Anbieter stimmen nämlich nicht immer mit den Datenschutz- oder Compliance-Anforderungen hierzulande überein. Die USA ist mit 83,7 Prozent Vorreiter bei der Bereitstellung von Cloud-Infrastrukturen. Die chinesischen Hyperscaler machen 13,6 Prozent aus. ⇨

Unternehmen, mit hohen Anforderungen hinsichtlich der Datensicherheit, wählen häufig Cloud-Anbieter mit privaten Clouds und lokalen Infrastrukturen, die lokal verwaltet und gesteuert werden. Denn diese Clouds gewähren den Schutz der sensiblen Daten, internen Prozesse und Abläufe. Der Nachteil einer privaten Cloud im Vergleich zu der öffentlichen Cloud kann darin bestehen, dass die Funktionen begrenzt sind. Die öffentlichen Clouds entwickeln sich stets weiter, doch aufgrund der vagen Souveränitätsdefinitionen, fällt es I&O-Führungskräften schwer, den passenden Anbieter zu finden.

I&O-Führungskräfte können die Anforderungen des Unternehmens bezüglich der Souveränitätsanforderungen passend bewerten, indem sie sich auf die folgenden drei Bereiche konzentrieren:

- Daten
- Betrieb
- Technologie

Daten-Souveränität

Der Rechtsrahmen und die Governance befassen sich mit der Anforderung der Datenhoheit – also mit der Frage, wie Daten mit den Gesetzen und Vorschriften des einheimischen Unternehmensstandorts in Einklang mit ausländischen Datenschutzverordnungen gebracht werden können. Kooperationen zwischen Public-Cloud-Anbietern und inländischen Partnern verbessern die betrieblichen Herausforderungen. Außerdem befassen sich einige Public-Cloud-Anbieter mit den länderspezifischen Anforderungen bezüglich der Souveränität.

Der Standort, an dem die Daten gespeichert und verarbeitet werden, ist ebenfalls von entscheidender Bedeutung, da gewährleistet werden muss, dass unbefugte Dritte keinen Zugriff auf die Daten erhalten.

Daher verfügen die meisten Anbieter über folgende Technologien und Fähigkeiten:

- Sichere Daten: Data at rest, Hardware-Sicherheitsmodule (HSM) mit Sicherheitszertifizierung wie FIPS, Data in use.
- Gewährleistung der Datenaufbewahrung: Definition und Implementierung von Richtlinien und Leitplanken, damit die Daten am gewünschten Standort gespeichert werden und keine Replikation oder Synchronisierung an anderen Standorten erfolgt.
- Kontrolle des Datenzugriffs durch Tools zur Identität, Audits, Landingzone.

Betriebliche Souveränität

Die Cloud-Souveränität garantiert, dass die Daten, Dienste und Infrastruktur am Zielstandort des Unternehmens verbleiben. Dadurch kann ebenso die betriebliche Souveränität gesichert werden. Denn es kann gewährleistet werden,

Bild: Rawf8 - stock.adobe.com

Die Public-Cloud-Angebote der US-amerikanischen und chinesischen Anbieter halten zusammen 97,3 Prozent Marktanteil weltweit. Ein Problem, da sie nicht immer mit den Datenschutz- oder Compliance-Anforderungen hierzulande übereinstimmen.

Private oder Public Cloud? Es gibt verschiedene Wege, eine sichere Cloud-Umgebung zu erreichen.

dass neben personenspezifischen auch sensible Daten sicher gespeichert wurden.

Technologische Souveränität

Unternehmen, die über eine technologische Souveränität verfügen, mindern das Risiko in den IT-Lieferketten. Kleinere und mittlere lokale Cloud-Anbieter, private Clouds und On-Premises-Systeme helfen den Unternehmen dabei, die technologische Unabhängigkeit zu gewährleisten.

Die Ausarbeitung einer souveränen Cloud-Stategie für Ihr Unternehmen

Lassen Sie sich bei der Ausarbeitung rechtlich von der Compliance- und Risikoabteilung beraten, wenn es um die Souveränitätsanforderungen Ihres Landes oder Ihrer Branche geht. Besonders für multinationale und branchenmäßig diversifizierte Unternehmen kann dies ein komplexes Unterfangen darstellen.

Vor- und Nachteile der Public Cloud und der Private Cloud

Die Vorteile der Public Cloud bestehen zweifelsohne in der Skalierbarkeit, Ausfallsicherheit, Innovation und der Funktionen. Public Clouds versuchen den Souveränitätsanforderungen zu entsprechen, doch die Souveränität kann nicht immer gewährleistet werden.

Die Private Cloud sticht hingegen durch ihre sichere Datenspeicherung hervor. Andererseits verfügt sie häufig über weniger Funktionen als die Public Cloud. □

Über die Autoren

Die Autoren Miguel Angel Borrega, Alessandro Galimberti, Ken Rothenberger und Rene Buest arbeiten als Analysten für das Marktforschungsunternehmen Gartner.

Kein Aufwand mehr bei E-Mail-Archivierung und -Verschlüsselung

Mit der Retarus Secure Email Platform lassen sich E-Mails revisions- und rechtssicher archivieren sowie ver- und entschlüsseln.

Laut IT-Branchenverband BITKOM gehen in deutschen Unternehmen täglich durchschnittlich 40 E-Mails pro Postfach ein. Dabei tauschen Mitarbeiter auch häufig sensible Informationen aus. Um vertrauliche Daten vor unbefugtem Zugriff zu schützen, müssen Unternehmen ihre E-Mail-Kommunikation bestmöglich absichern. Hierfür erhalten Unternehmen mit der cloudbasierten Retarus Secure E-Mail Platform alles Notwendige aus einer Hand.

Sicherer Datenspeicher für die Business-Kommunikation

Geschäftliche E-Mails müssen revisions- und rechtssicher archiviert werden. Gesetzliche Vorgaben wie Aufbewahrungspflichten sowie das E-Mail-Management sind dabei herausfordernd für Unternehmen. Hier kommt das Retarus Email Archive in Spiel. Als Baustein der Retarus Secure Email Platform speichert es den ein- und ausgehenden sowie auf Wunsch auch den internen E-Mail-Verkehr automatisch, zuverlässig und rechtskonform im Original-Raw-Format inklusive SMTP-Informationen. Im Archiv abgelegte Nachrichten sind unveränderbar und dank Vier-Augen-Prinzip vor unbefugtem Zugriff geschützt. Selbst bei großem Speicherumfang sind Nachrichten im Bruchteil von Sekunden auffindbar, unabhängig vom eingesetzten E-Mail-System. Das Archiv ermöglicht den Zugriff für bis zu zehn Jahre, danach erfolgt eine gesetzeskonforme Löschung.

Die Langzeitaufbewahrung von E-Mails mit Retarus Email Archive erfüllt zuverlässig die Datenschutzvorgaben der DSVGO sowie individuelle Branchenstandards und Compliance-Richtlinien. Die E-Mails werden in auditierbaren, hochverfügbaren und redundanten Retarus-Rechenzentren in Europa unveränderbar gespeichert und dabei durch eine hybride Verschlüsselung geschützt. Auch der Datentransfer von und zur IT-Infrastruktur des Kunden erfolgt verschlüsselt.

Sichere Ent- und Verschlüsselung von vertraulicher Kommunikation

Retarus Email Encryption schützt personenbezogene Daten ebenso wie wertvolles Firmen-Know-how. Die Lösung entschlüsselt eingehende Nachrichten zentral über die Cloud-Plattform, bevor sie im Originalformat im wiederum verschlüsselten Archiv abgelegt werden.

Zusätzlich reduziert die User Synchronization for Encryption (USE) von Retarus den Aufwand für Administratoren deutlich. Mit dieser Funktion lassen sich einzelne Nutzer, Gruppen, Schlüssel/Zertifikate sowie Richtlinien automatisiert verwalten. Der IT-Security-Admin definiert, welche Mitarbeiter oder Gruppen welche Schlüssel und Zertifikate benötigen und wie das individuelle Regelwerk aussehen soll. Anhand dieser kundenspezifischen Regelwerke werden vertrauliche Nachrichten inklusive aller Dateianhänge automatisch verschlüsselt. Administratoren werden über den Status der Synchronisation und die erstellten Schlüssel umgehend per E-Mail benachrichtigt. Dadurch behalten IT-Verantwortliche die volle Kontrolle über die verwendeten Schlüssel. Insbesondere große Unternehmen mit vielen Nutzern, IT-Systemhäuser und Distributoren senken dadurch ihren manuellen Aufwand und ihre Fehlerquote erheblich.

E-Mail-Rundumschutz aus einer Hand

Das Retarus Email Archive sowie Retarus Email Encryption sind Teil der cloudbasierten Retarus Secure Email Platform. Ihre umfassenden Sicherheitsmechanismen überprüfen ein- und ausgehende E-Mails auf Malware, Spam und Phishing.

Darüber hinaus umfasst die ganzheitliche Abwehrstrategie die Erkennung und Isolierung unbekannter Bedrohungen durch KI-gestützte Mechanismen und Sandboxing. Zum Funktionsumfang zählt außerdem die patentierte Retarus Patient Zero Detection, die bereits zugestellte Schad-E-Mails identifiziert. ■

Besuchen Sie Retarus auf der it-sa in Nürnberg in Halle 6 an Stand 306.

www.retarus.de

Auf NIS2-Mission

Bei der NIS2-Vorbereitung stehen deutsche Unternehmen erst einmal vor einem schwarzen Loch. Der Channel kann helfen, Unklarheiten zu beseitigen und die Kunden NIS2-konform zu machen.

Von Barbara Miletic und Ira Zahorsky, IT-BUSINESS

Bild: KI-generiert / Midjourney

Sei deinen Freunden nah, doch deinen Feinden näher – so ein berühmtes Zitat aus dem Film „Der Pate“. Angesichts der ernsten Cyberbedrohungslage gilt es auch für deutsche Unternehmen, potenzielle Cyberangreifer und -bedrohungen im eigenen IT-System genau auf dem Schirm zu haben – und im Notfall gekonnt reagieren zu können. Ein robustes Risiko- und Notfallmanagement liegt auch der Richtlinie NIS2 zugrunde. Dieses ist eine der Kernkriterien, um die Anforderungen des NIS2-Katalogs zu erfüllen. Ab 18. Oktober 2024 soll die NIS2-Richtlinie in nationales Recht umgesetzt werden. Die Uhr tickt. Wer meint, entsprechende Umsetzungen vernachlässigen zu können, soll mit knackigen Bußgeldern oder einer persönlichen Haftung (als Geschäftsführung) eines Besseren belehrt werden.

Doch wie gut ist Deutschland auf NIS2 vorbereitet? Wie weit sind Unternehmen in der Umsetzung, wo gibt es Stolpersteine? Welche Eckdaten sollten Geschäftsführer und Unternehmer dringend kennen?

NIS2 – Ich?

Bevor es also an die konkrete, praktische Umsetzung der NIS2-Anforderungen geht, ist eine vollständige Sicht auf den aktuellen Stand der Informationssicherheit im Unternehmen relevant. Hinzu kommt, „dass die Unternehmen enorm unter Zeitdruck stehen“, ergänzt Andreas Baresel, Vorstandsvorsitzender der Datagroup. Insbesondere die Umsetzung organisatorischer Maßnahmen stelle so manches Unternehmen vor Herausforderungen. Vernetzung lautet das richtige Stichwort, da auch die Bündelung von Lösungen und Kompetenzen essenziell ist.

Zusammenarbeit verschiedener Hersteller ist gefragt

Ein Beispiel einer Kompetenz- und Herstellerbündelung ist GData. Das Bochumer Unternehmen bietet, um dem Stand der Technik

Bild: Racle Fotodesign - stock.adobe.com

Gut für IT-Dienstleister: Bei der Umsetzung von NIS2 fällt viel Beratungsbedarf an.

und einem starken Notfallmanagement gerecht zu werden, Managed Endpoint Detection and Response (Managed EDR), Security Awareness Trainings und Incident Response (IR) im Portfolio an. Die Lösungen werden um die Einbruchserkennung von Cybersense oder durch Hard- und Softwarelösungen von Fortinet und Cisco ergänzt.

NIS2-fit: Webinare, Konzepte, Ansätze

Zunächst einmal geht es also für die IT-Dienstleister mit NIS2-Spezialisierung im Portfolio ⮑

Was ist die NIS2-Richtlinie?

Die NIS-Richtlinie gibt es bereits seit 2016. Ihr Ziel: die Gewährleistung eines hohen Sicherheitsniveaus für Netzwerke und Informationssysteme kritischer und sensibler Infrastrukturen in den EU-Mitgliedsländern. 2021 wurde damit begonnen, die NIS-Richtlinie zu überarbeiten. NIS2 trat am 16. Januar 2023 in Kraft und muss bis zum 17. Oktober 2024 in deutsches Recht umgesetzt werden.

darum, die Endkunden zu beraten und eine Bestandsanalyse zu machen. Die Datagroup bietet hierfür einen strukturierten Ansatz. Die Dienstleistungen sind modular aufgebaut, sodass sie flexibel an die individuellen Reifegrade und Bedürfnisse der Kunden angepasst werden können. Die NIS2-Services werden in vier zentralen Bereichen angeboten: Security Operation Center (SOC) zur Überwachung und Reaktion auf Sicherheitsvorfälle, Penetrationstests zur Identifizierung von Schwachstellen, Incident Response (IR) für schnelle Reaktionen auf Sicherheitsvorfälle und Consulting zur strategischen Beratung.

Ein weiterer Punkt auf der NIS2-Agenda, der von einem Großteil der Unternehmen noch angegangen werden muss, ist die Vorfallmeldung. Die Richtlinie verschärft die einzuhaltenden Meldezeiten noch einmal deutlich. Früh mit Umsetzungen zu beginnen, lohnt sich.

Ein 360-Grad-Blick auf die eigene IT-Sicherheit ist nicht nur mit der näher rückenden NIS2 elementar, sondern sollte grundsätzlich im Alltag integriert sein. Konzepte, um deutschen Unternehmen jeglicher Branche und Größe bei der Umsetzung von NIS2 unter die Arme zu greifen, gibt es im Channel. Spannend bleibt allerdings, was sie bei den scheinbar notwendigen Investitionen zum Zögern bringt.

Droht Verschiebung der Frist?

Deutschland hat zunächst das „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ (NIS2UmsuCG) im April 2023 im ersten Anlauf auf den Weg gebracht. Trotz eines Referentenentwurfs des Bundesinnenministeriums hat diese Umsetzung bislang noch nicht stattgefunden.

„Resilienz ist das Gebot der Stunde für alle“, erläutert René Hofmann, Geschäftsführer von Securepoint. „IT-Sicherheit muss als das verstanden werden, was sie ist: eine nachhaltige Investition in die Zukunft. Daraus entsteht Schutz für die Wirtschaft sowie die Gesellschaft und es können höhere Schäden durch Cyberangriffe verhindert werden. Was für Unternehmen gilt, gilt auch für Politik und Verwaltung.“ □

Wer ist betroffen?

Unternehmensgröße
„Mittlere Unternehmen“: 50 bis 250 Mitarbeiter, 10 bis 50 Mio. Euro Umsatz, Bilanzsumme kleiner als 43 Mio. Euro
„Große Unternehmen“: mehr als 250 Mitarbeiter, mehr als 50 Mio. Euro Umsatz, Bilanzsumme größer als 43 Mio. Euro

Sektorzugehörigkeit
Alle Unternehmen, die einer von achtzehn kritischen Branchen angehören: Energie, Transport, Bankenwesen, Finanzmärkte, Gesundheit, Trinkwasser, Abwasserwirtschaft, digitale Infrastrukturen, ICT Service Management, öffentliche Verwaltung und Weltraum sowie Post- und Kurierdienste, Abfallwirtschaft, Chemikalien, Lebensmittel, Herstellung bestimmter industrieller Produkte, digitale Dienste und Forschung

Was tun bei einem Vorfall?

Innerhalb von 24 Stunden muss ein Unternehmen einen potenziellen Sicherheitsvorfall gemeldet haben – auch an Feiertagen und Wochenenden. Regelmäßige Updates zu der Benachrichtigung nach 72 Stunden und nach 30 Tagen sowie ein Abschlussbericht innerhalb eines Monats gehören nun ebenfalls zum Pflichtprogramm.

ENGINSIGHT

MEHR SICHERHEIT
MEHR KONTROLLE

mit der All-in-one Cybersecurity-Software aus Jena

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

ALL-IN-ONE

+ IT-Inventarisierung
+ IT-Monitoring
+ Automatisierte Pentests
+ Schwachstellen-Scans
+ Konfigurations-Checks
+ Eventlog-Analyse
+ Intrusion Detection
+ Intrusion Prevention
+ Mikrosegmentierung
+ File Integrity Monitoring
+ **SIEM**

MADE IN GERMANY

jetzt kostenlos testen

ENGINSIGHT.COM

Model: Theresa von Enginsight

Nicht über Regulierung schimpfen, sondern handeln!

Die NIS2-Richtlinie soll das Cybersicherheitsniveau des EU-Wirtschaftsraums stärken – ein dringend nötiges Vorhaben. Wichtige und sehr wichtige Unternehmen müssen künftig ein strengeres Security-Regiment nachweisen, einschließlich ihrer Zulieferer. Dadurch betrifft die EU-Richtlinie auch Unternehmen jenseits der namentlich genannten Sektoren.

Von Dr. Wilhelm Greiner, IT-Fachjournalist

Bild: Leo Lintang - stock.adobe.com

Es ist eine der großen deutschen Erfolgsgeschichten: der Sicherheitsgurt. Seit 1974 ist er Pflichtbauteil in Neuwagen. Denn in Zeiten des Wirtschaftswunders und der Massenautomobilisierung hatte sich die Zahl der Verkehrstoten auf westdeutschen Straßen von 6.400 (1950) auf knapp 19.200 (1970) verdreifacht. Doch das lebensrettende Accessoire stieß anfangs auf wenig Akzeptanz („Ich stütz' mich einfach am Lenkrad ab!"). Deshalb folgte bald die Gurtpflicht (1976 in Westdeutschland, 1980 in der DDR), später kamen Airbags und viele weitere Maßnahmen.

Heute liegt die Zahl der Verkehrstoten in Deutschland trotz erheblich dichteren Verkehrs seit Jahren unter der 3.000er-Marke, darunter dank Gurt & Co. letztes Jahr nur 1.183 Pkw-Insassen. Manchmal muss der Mensch offenbar zu seinem Glück gezwungen werden.

Cybersecurity: „angespannte bis kritische Lage"

Jetzt ist es mal wieder so weit. Nur geht es diesmal nicht um Verkehrs-, sondern um Cybersicherheit, dem Raser und Drängler unter den Geschäftsrisiken. Der BSI-Lagebericht 2023 konstatiert „eine angespannte bis kritische Lage": „Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor."

Das BSI warnt vor dem „Ausbau cyberkrimineller Schattenwirtschaft", DDoS-Hacktivismus und hochprofessionellen Angreiferorganisationen (Advanced Persistent Threats, APTs). Doch allzu oft zotteln Privatleute, Unternehmen und Behörden bei Schutz- und Abwehrmaßnahmen auf der rechten Fahrspur dahin. Zudem klaffen immer neue Sicherheitslücken, nicht zuletzt in Angeboten von IT-Giganten wie Microsoft. Das Ergebnis findet, etwa in Form erfolgreicher Ransomware-Angriffe, fast schon täglich den Weg in die Nachrichten.

EU zieht die Reißleine

Anfang 2023 zog die EU die Reißleine und erweiterte mit der NIS2-Richtlinie (Network and Information Security Directive 2) den Einzugsbereich deutlich über deren Vorgänger NIS1 von 2016 hinaus: NIS1 zielt auf den Schutz kritischer Infrastrukturen (KRITIS), NIS2 aber auf alle Unternehmen und Organisationen, die laut EU für den Wirtschaftsraum „wesentlich" (im Amtsdeutsch: „sehr wichtig") oder zumin- ⇨

Bild: sheris9 - stock.adobe.com

Das Motto bei NIS2 lautet: Lieber anschnallen und durchstarten als im Straßengraben zu landen.

dest „wichtig“ sind, in 18 Branchen von Abfall bis Weltraum. Von ihnen fordert sie ein konsequentes Cyberrisikomanagement.

Wichtig: „NIS2 rückt die Bewältigung von Risiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu Lieferanten betreffen, ebenso in den Mittelpunkt wie die Cybersicherheit bei den betroffenen Einrichtungen selbst“, so Dennis-Kenji Kipker, Professor für IT-Sicherheitsrecht an der Hochschule Bremen. Die Richtlinie mache zunächst keine weiteren Einschränkungen, welche Unternehmen in diese Lieferkette fallen. Manch ein Unternehmen rast also auf einen regulatorischen Abgrund zu.

NIS2: Deadline 17. Oktober

Stichtag für die Umsetzung ist der 17.10.24. Bis dahin muss der deutsche Gesetzgeber NIS2 in nationales Recht überführt haben. Dies dürfte beim Stand der Dinge (Referentenentwurf) ein hektischer Endspurt werden. Betroffene Organisationen sind also ab 18.10. verpflichtet, sich auf der NIS2-Spur zu bewegen, aber noch fehlen gesetzliche Leitplanken.

„Wenn ein Unternehmen jetzt erst auf der sprichwörtlichen grünen Wiese anfängt, ist dieser Termin nicht zu halten“, sagt Tim Berghoff, Security Evangelist bei G Data. „Auch zwei Jahre wären dann schon eine extrem sportliche Ansage.“ Hier gilt also das altbewährte Motto: besser spät als nie!

Unternehmen mit ISO-27001-Zertifizierung können hingegen laut dem Experten „ein bisschen aufatmen“: Viele NIS2-Vorgaben zur Technik finden sich schon in ISO 27001. Diese sollte man besser erfüllen, sonst drohen hohe Bußgelder und Geschäftsführerhaftung.

Fazit

Deshalb heißt es nun: Anschnallen, Gas geben und durchstarten in Richtung Risikomanagement und Cybersecurity. Dies ist auch dann sinnvoll, wenn ein Unternehmen nicht als „wichtige“ Einrichtung gemäß NIS2 gilt oder keine 50, sondern nur 49 Beschäftigte hat. Denn ist ein Unternehmen erst einmal Opfer von Ransomware & Co. geworden, dann landet es schnell im Straßengraben. Und hat der Geschäftsführer dabei auf den Sicherheitsgurt verzichtet, dann nutzt es bekanntlich auch nichts, sich am Lenkrad abzustützen. □

In 10 Schritten zur NIS2-Konformität

Ob ein Unternehmen jetzt erst bemerkt, dass es von NIS2 betroffen ist, oder ob es – „Da stütz' ich mich einfach mit den Händen am Lenkrad ab!“ – bislang versäumt hat, sich mit dem Thema zu befassen: Das eBook von Security-Insider zeigt die zehn wesentlichen Schritte zur NIS2-Konformität auf und gibt zahlreiche Praxistipps.

ISX2024

IT-Security Digital Conference

www.isxconference.de

13. & 14. NOVEMBER
DIGITAL CONFERENCE

NEXTGEN IT-SECURITY – ONE STEP AHEAD OF CYBER CRIMINALS

- Mit Security Awareness Trainings planvoll Risiken senken – so geht's!
  Manuel König, KnowBe4
- Cyber-Angriffe und finanzielle Schäden: Prävention, Schutzmaßnahmen und Versicherungsoptionen für Unternehmen
  Sven Hillebrecht, ADLON Intelligent Solutions
- Zukunftssichere IT-Sicherheit – und welche Rolle spielen Mensch und KI?
  Martin Weiß, Sophos
- Sichere Nutzung von generativen KI-Anwendungen wie ChatGPT
  Georg Hermann, Netskope
- Neuer SASE Ansatz – Hybrid und Full-Meshed
  Daniel Bunzel, Check Point
- Cybercrime Insights – die neue Bedrohungslage
  Dr. Christian Reinhardt, SoSafe

KnowBe4 Human error. Conquered.
adlon Empowering Business with IT
SOPHOS
netskope
CHECK POINT
sosafe

GET YOUR VIP-TICKET!

EINE VERANSTALTUNG DER VOGEL IT AKADEMIE

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

OT und IT als Dreamteam

Bisher galt IT in der Industrie als „untypisch". Doch Industrie 4.0 wird immer unumgänglicher, genauso wie die digitale Vernetzung in der Fertigung. OT und IT werden zum Pflicht-Duo in der Produktionshalle – der Aufwand lohnt sich.

Von Barbara Miletic, IT-BUSINESS

Ransomware ist nach wie vor die häufigste Art von Cyberangriffen. Dazu wird sie immer mehr zum eigenen Businessmodell ausgebaut. Beliebtes Ziel ist die Industrie. Doch OT-Sicherheit (Operational Technology) betrifft viele weitere Marktsegmente. Angriffe auf OT zielen unter anderem auf die Lieferkette ab. Häufig werden sie ausgelöst durch geopolitische Probleme wie staatlich finanzierte Hacker oder politisch motivierte Akteure. Die ernste Bedrohung ihrer OT-¬Sicherheit ist den Unternehmen scheinbar bewusst. Sie räumen dem Schutz kritischer OT-Anlagen Priorität ein. Datensicherheit steht bei den Investitionen weit oben. Dadurch wollen sie versuchen, die Widerstandsfähigkeit ihrer technologischen Infrastruktur zu stärken.

Moderne Technologie veranlasst zum Umdenken

In KI-Zeiten stehen der Industrie große Veränderungen bevor, was eine Verzahnung von Security, Automatisierung und Edge Computing sinnvoll macht. Zunächst war OT für physische Prozesse wie Fertigung oder Energieversorgung zuständig. Heute sind eine digitale Vernetzung der Geräte und das Zusammenspiel mit der IT nicht mehr wegzudenken. KI hat hier ihren Spielraum, um zum einen Produktionsabläufe zu optimieren und zum anderen neue Dienstleistungen zu entwickeln. Hersteller überdenken zunehmend ihr Portfolio und erweitern dieses um neue KI-Funktionen oder schließen sich strategisch mit Partnern zusammen. □

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

Wie OT und IIoT besser geschützt werden können

Die Sicherheit im Analogen wie im Digitalen ist Grundvoraussetzung für den Erfolg der deutschen Industrie und gleichzeitig eine ihrer größten Herausforderungen. Die Cyberrisiken in der vernetzten Industrie sind enorm. Es ist höchste Zeit, neben der IT (Informationstechnologie) auch die OT (Betriebstechnologie) und das IIoT (Industrial IoT) besser zu schützen.

Von Dipl.-Phys. Oliver Schonschek

Bereits vor einigen Jahren warnte der Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV): In der Elektroindustrie sind viele Unternehmen nicht auf einen Cyberangriff vorbereitet. In einer Forsa-Umfrage im Auftrag des GDV gab fast die Hälfte (43 Prozent) der Unternehmen an, weder ein Notfallkonzept noch eine entsprechende Vereinbarung mit ihrem IT-Dienstleister zu haben. Eine ähnliche Situation musste der GDV auch im Maschinenbau feststellen: Kleine und mittelständische Maschinenbauer hatten große Lücken bei ihrer IT-Sicherheit. Zu viele Unternehmen wogen sich in falscher Sicherheit, mit unabsehbaren Folgen. 55 Prozent der Befragten gingen für ihr eigenes Unternehmen von einem geringen Risiko aus. Die IT-Sicherheit hat für viele Maschinenbauer dementsprechend keine Priorität, so das damalige Fazit des GDV.

Doch was hat sich geändert in den letzten Jahren? Mit voranschreitender Digitalisierung und der damit einhergehenden stärkeren Vernetzung nimmt die Zahl möglicher Angriffe stetig zu, warnt der Bundesverband der Deutschen Industrie e.V. (BDI). Im Jahr 2023 waren 72 Prozent der Industrieunternehmen von Diebstahl, Industriespionage oder Sabotage betroffen, wie der BDI mit Verweis auf eine Bitkom-Studie berichtet.

Die Industrie hält sich für sicherer, als sie es ist

Obwohl der noch lückenhafte Cyberschutz in der Industrie schon lange bekannt ist, ist das Bewusstsein für die eigenen Cyberrisiken in der deutschen Wirtschaft nicht wirklich ausgeprägt. Die eco-Studie „IT-Sicherheit 2024“ zeigt, dass die deutsche Wirtschaft sicherheitstechnisch immer noch unzureichend aufgestellt ist.

Zu diesem Ergebnis kommen, wie bereits in den Vorjahren, erneut die meisten der befragten Experten (76 Prozent). Die Cybersicherheit im eigenen Unternehmen schätzen die Experten hingegen eher optimistisch ein: 54 Prozent der Befragten sagen, das eigene Unternehmen sei sehr gut oder gut abgesichert, 31 Prozent bezeichnen sich als ausreichend abgesichert. Dennoch hatte jedes fünfte Unternehmen im letzten Jahr mindestens einen IT-Sicherheitsvorfall mit zum Teil erheblichen Schäden (vier Prozent), so der Verband der Internetwirtschaft eco.

Offensichtlich hat sich das Bewusstsein für die Cyberrisiken in der Industrie nicht deutlich verbessert. ⇨

So ist es leider auch nicht überraschend, dass die Absicherung von Produktions- und Industrieanlagen auch im Jahre 2024 nicht zu den wichtigsten Themen der Cybersicherheit gerechnet wird, wie die eco-Umfrage offenlegt.

Die vielen Cybervorfälle in der Industrie zeigen das echte Risiko

Gleichzeitig nehmen die Schäden für deutsche Unternehmen durch Cyberangriffe zu, wie die KPMG-Studie „e-Crime in der Deutschen Wirtschaft 2024" zeigt. Laut Studie sind betroffene Unternehmen am häufigsten Opfer von Phishing (53 Prozent), Attacken auf Cloud-Services (42 Prozent) sowie Datenlecks (37 Prozent). Computerkriminelle richten ihre Angriffe am häufigsten gegen Mailserver (39 Prozent) und Webserver (36 Prozent). Dabei nutzen sie auch Dienstleister der Unternehmen als Einfallstor für ihre kriminellen Handlungen. Mehr als die Hälfte (54 Prozent) der betroffenen Unternehmen erlebte Angriffe auf ihre eigenen Daten über die technische Infrastruktur von Dienstleistern, berichtet KPMG.

Beispiele für schwerwiegende Attacken auf die Industriebranchen muss man leider nicht lange suchen, ein prominenter Fall aus den letzten Jahren: Die Gruppierung LockBit erlangte Zugang zu den Systemen des Unternehmens Continental und exfiltrierte Daten in einer Gesamtmenge von rund 40 TB, die für 50 Millionen US-Dollar im Darknet angeboten wurden. Die geleakten Daten enthielten vertrauliche Informationen wie Strategiepläne, Korrespondenz und Kundendaten.

Es zeigt sich: Es muss deutlich mehr unternommen werden, um den Cyberrisiken im Industriebereich zu begegnen, denn die Industrie ist im Fokus vieler Cybercrime-Aktivitäten. Damit sich der Schutz für OT und IIoT verbessert, werden unter anderem die gesetzlichen Anforderungen verschärft, wie im nächsten Kapitel genauer betrachtet wird.

Verschärfung des Cybersicherheitsrechts

Die Umsetzung angemessener, risikobasierter Cybersicherheitsmaßnahmen ist für das Wirtschaften im Zeitalter der digitalen Transformation unerlässlich, wie der Bundesverband der deutschen Industrie (BDI) bekräftigt. Die nationalen und europäischen Gesetzgeber haben in zahlreichen Gesetzen neue und schärfere Anforderungen an Maßnahmen zur Reduktion des Cyberrisikos eingeführt. Die EU wird zum Beispiel verbindliche Cybersicherheitsanforderungen für Hardware- und Softwareprodukte mit vernetztem digitalem Element einführen, mit dem Cyber Resilience Act (CRA), mit klaren Folgen für notwendige Sicherheitsmaßnahmen im IoT und IIoT. Aus Sicht des BDI eine wichtige Entwicklung, denn der Cyber Resilience Act könne Betreiber Kritischer Infrastrukturen sowie besonders wichtige und wichtige Einrichtungen dabei unterstützen, ihre Risikomanagementmaßnahmen gemäß NIS2-Richtlinie umzusetzen. Wenn auf dem europäischen Markt nur noch cyberresiliente Produkte (Hard- und Software) verfügbar sind, dann erleichtert dies die Implementierung der Risikomanagementmaßnahmen erheblich, so der BDI.

Der Verband Deutscher Maschinen- und Anlagenbau (VDMA) verweist zudem auf die Bedeutung von NIS2: Die neue Richtlinie adressiert den Maschinen- und Anlagenbau als wichtigen Sektor. Unternehmen sind verpflichtet, sich bei der nationalen Behörde selbst zu registrieren. Wichtig ist es jedoch, dass sich die Industriebetriebe auch ihrer Betroffenheit durch die neuen Gesetze klar werden, auch und gerade bei der neuen EU-Cybersicherheitsrichtlinie NIS2. 24 Prozent der bei der VDMA-Studie „Industrial Security und Produktpiraterie 2024" befragten Unternehmen glauben, nicht von NIS2 betroffen zu sein. Jedoch ergab eine VDMA-Analyse, dass rund 90 Prozent es tatsächlich sind.


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

Die Absicherung von Produktions- und Industrieanlagen wird nicht zu den größten Sicherheitsthemen gezählt, trotz der offenkundigen Cyberrisiken bei Industrie 4.0, wie eine Umfrage des eco-Verbandes ergab.

Spezifische Leitlinien und Empfehlungen für die Umsetzung

Es reicht aber selbstverständlich nicht, gesetzlich mehr Sicherheit im OT und IIoT zu fordern, um das Risiko cyberkrimineller Angriffe auf die Industrie zu mindern. Die Industrieunternehmen müssen wissen, was konkret getan werden kann und sollte, gerade auch im Unterschied zur IT-Sicherheit, die in aller Regel deutlich fortgeschrittener in der Umsetzung ist als die OT-Sicherheit und die IIoT-Sicherheit. Doch es gibt bereits eine Reihe von Leitlinien und Standards, die speziell der Industrie in Fragen der Cybersicherheit helfen können. Zu nennen sind hier insbesondere

- ISA Standards and Publications / ISA Standards: ISA/IEC 62443 Series of Standards, Security for industrial automation and control systems
- NIST SP 800-82 Rev. 3 (Draft) Guide to Operational Technology (OT) Security
- ICS-Security-Kompendium des BSI
- Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen, Allianz für Cybersicherheit

Es geht nicht nur um die technische Sicherheit im OT und IIoT

Um Betriebs- und Produktionsunterbrechungen zu verhindern und die Einhaltung strenger, regulatorischer Vorschriften wie die EU-weiten Gesetzgebungen zu Cybersicherheit (NIS2 und CRA) zu gewährleisten, sind nachhaltige Investitionen in angemessene Schutzmaßnahmen unerlässlich, erklärt KPMG. Diese Maßnahmen umfassen aber nicht nur die Implementierung von OT-kompatiblen Security-Lösungen, sondern auch die kontinuierliche Aus- und Weiterbildung der Mitarbeitenden innerhalb der Produktion. Dadurch werde das Bewusstsein für Cybersicherheitsrisiken geschärft und sichergestellt, dass sie im Falle eines Angriffs angemessen reagieren können, wie das Wirtschaftsprüfungshaus erläutert. □

SuperApp „Made in Germany“

KOBIL myCity – die SuperApp für Städte und Kommunen

Digitale Technologien erleichtern den städtischen Alltag. Unter einer Voraussetzung: Sie müssen sicher und datenschutzkonform sein sowie die gesetzlichen Regularien erfüllen. Und: Sie sollten nicht nur Behördendienste umfassen, sondern auch andere Angebote. Daran scheitern viele Städte und Kommunen. Die Lösung bietet **Europas einziger SuperApp-Anbieter KOBIL aus Worms** mit einer App für alles: KOBIL myCity.

OneApp4All™ digitalisiert Behörden, Wirtschaft, Gesellschaft

KOBIL myCity ist eine SuperApp: OneApp4All™ – eine App für alles. Sie ist ein digitaler Marktplatz für Behördendienste und Angebote aus Wirtschaft und Gesellschaft. Zum Beispiel Shopping, Banking, sicheres Bezahlen und Chatten. Einmal authentifiziert, können Bürger alles nutzen, ohne die App zu verlassen. Die Bedienung ist einfach und barrierefrei.

In Istanbul nutzen die App über 5 Millionen Einwohner. Jetzt kommt sie nach Deutschland. Worms macht den Anfang. Weitere Städte werden folgen.

Bilder: KOBIL Gruppe

KOBIL myCity – die SuperApp für Städte und Kommunen

Sicher, datenschutz- und gesetzeskonform

Digitale Technologien brauchen Sicherheit und Vertrauen. Dafür sorgt KOBIL – führender Spezialist für Sicherheit und digitale Identitäten. Daten werden über 14 Schutzschichten übertragen. Sie liegen auf sicheren Servern in Deutschland. Die Bezahlung und der Dokumentenaustausch sind geschützt, der Chat ist verschlüsselt. KOBIL myCity erfüllt alle Sicherheits-, Datenschutz- und gesetzlichen Anforderungen.

Digitale Identität und BundID

Der Zugang zur SuperApp erfolgt über eine sichere, verifizierte Identität. Jeder weiß, mit wem er es zu tun hat. Die App wird mit der BundID kompatibel sein.

Mehr Bürgernähe, weniger Bürokratie

Von der App profitiert die ganze Stadt. Behörden werden effizienter und bürgernäher, Unternehmen treiben die Umsätze an. Sie brauchen keine IT-Kenntnisse und können Angebote mit wenigen Klicks selbst hinzufügen oder ändern. Das spart Geld, Zeit und baut Aktenberge ab.

Jede Stadt kann KOBIL myCity schnell und kostengünstig implementieren. ■

Erfahrungen aus Worms

Wirtschaft meets Verwaltung: Innovation für alle

Die SuperApp von KOBIL geht diesen Herbst in Worms live. Das ist Vorbild für ganz Deutschland. Egal ob Metropole oder Kleinstadt – alle können die App übernehmen und ihr eigenes Ökosystem schaffen.

Mitmachen – leicht gemacht

KOBIL liefert eine schlüsselfertige Plattform. Sämtliche Behörden, Unternehmen und kulturelle sowie Bildungseinrichtungen können sie nutzen. Die Angebote werden als MiniApp integriert. Eigene Investitionen in IT-Infrastruktur oder Fachpersonal sind nicht notwendig.

KOBIL und Worms: Ein perfekter Match

Das City-App Worms Projekt wurde öffentlich ausgeschrieben. KOBIL erhielt den Zuschlag. Heike Landwehr ist als Projektmanagerin Digitalisierung bei der Stadtverwaltung Worms für die Implementierung verantwortlich: *„Die Zusammenarbeit mit KOBIL verläuft sehr gut und vertrauensvoll. Alle Beteiligten sind extrem ehrgeizig. Wir haben es geschafft, gemeinsam ein neuartiges, hochinnovatives Projekt auf die Beine zu stellen."*

Ismet Koyun, CEO und Gründer, KOBIL Gruppe

Stimmen aus Worms

Die Vorfreude ist groß. Das sagen die Wormser über KOBILs SuperApp:

„Wir sind gerne dabei. Mit nur einem Klick findet man alle Geschäfte und Angebote in der Nähe."
Gernot Weber von Uhren und Schmuck Weber in Worms

„Wir wünschen uns, dass die App eine weitere gute Möglichkeit bietet, sich über Neuigkeiten, Veranstaltungen sowie ‚Aktuelles aus dem Rathaus' zu informieren."
Anja und Günter Hofmeister von Stahlwaren Lützenkirchen

„Mit der App können wir unsere Leidenschaft für Kaffee mit noch mehr Kunden und im Kreise anderer Geschäfte, Veranstalter und der Stadt teilen."
Alexander Pizzo, Kaffeeröster bei L'arte del caffé in Worms

Für eine sichere digitale Zukunft

KOBIL möchte allen Menschen nahtlosen Zugang zu digitalen Diensten mit höchsten Sicherheits- und Datenschutzstandards ermöglichen.

„Mit der OneApp4All™ schaffen wir die Brücke zu einer sicheren digitalen Zukunft."
Ismet Koyun, Gründer und CEO von KOBIL

Welche Gefahren mit KI verbunden sind

KI gilt als eine der Zukunftstechnologien. Auch in der Security sind die Erwartungen und Hoffnungen groß. Doch viele Unternehmen zögern und fürchten die Konsequenzen von KI für Datenschutz und Sicherheit. Die Cyberkriminellen hingegen setzen bereits auf KI und könnten einen gefährlichen Vorsprung erhalten. Die Bedenken der zögerlichen oder ablehnenden Unternehmen sind jedoch nicht unbegründet.

Von Dipl.-Phys. Oliver Schonschek

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

Künstliche Intelligenz ist der Trend, der im Jahr 2024 die IT-Branche am stärksten prägen wird, davon sind rund drei Viertel (73,6 Prozent) der IT-Entscheiderinnen und -Entscheider überzeugt, wie eine Studie von eco – Verband der Internetwirtschaft e. V. ergab. Der eco-Verband sieht insbesondere auch einen deutlichen Einfluss von KI auf die Security und empfiehlt: „Stärken Sie Ihre IT-Sicherheit mit KI-Anwendungen. KI kann Spam-Mails im Postfach oder ungewöhnliche Verhaltensweisen und Datenflüsse innerhalb der IT schneller und effizienter erkennen – und so Security-Verantwortliche frühzeitig vor Angriffen warnen. Unternehmen können so schneller Gegenmaßnahmen in die Wege leiten. Künstliche Intelligenz entlastet außerdem IT-Teams, die aufgrund von Personal- und Fachkräftemangel stark beansprucht sind, von Routineaufgaben."

So verlockend dies in Zeiten des Fachkräftemangels in der Security auch klingt, viele Unternehmen zögern bei KI. „ChatGPT, Gemini & Co. haben in deutschen Unternehmen noch einen schweren Stand", berichtete der Digitalverband Bitkom. Erst drei Prozent nutzen demnach generative KI bereits zentral im Unternehmen. Weitere sechs Prozent haben den Einsatz für das laufende Jahr geplant. Der Grund: Es herrscht eine große Unsicherheit, wenn es um den Einsatz von KI im Unternehmen geht.

Nicht alleine der Datenschutz bei KI macht Kopfzerbrechen

Wie groß die Unsicherheit bei Unternehmen, aber auch bei den einzelnen Nutzerinnen und Nutzern ist, zeigt eine weitere Umfrage des eco-Verbands: Zwei Drittel der Deutschen (66,3 Prozent) wollen ihre Daten selbst in anonymisierter Form nicht für das Training einer Künstlichen Intelligenz zur Verfügung stellen, dabei unterliegen anonymisierte Daten gar nicht dem Datenschutz nach DSGVO (Datenschutz-Grundverordnung).

Zudem lässt sich feststellen, dass den Anwenderinnen und Anwendern von KI-Lösungen der Aufbau eines reellen Vertrauensverhältnisses, basierend auf der Vertrauenswürdigkeit des KI-Anbieters, sehr wichtig ist, so die Anwender-Studie TrustKI des Instituts für Internet-Sicherheit – if(is). Offensichtlich besteht ohne den Nachweis der Vertrauenswürdigkeit ein Misstrauen gegenüber KI.

Dieses Misstrauen ist auch nicht unangebracht, denn mit der Nutzung von KI sind zahlreiche Risiken verbunden, zum einen durch Schwachstellen und Fehler in der KI selbst, aber auch durch den Missbrauch von KI, der auf Seiten der Cyberkriminellen stetig zunimmt.

Mit KI sind zahlreiche Risiken verbunden

Die von Bitkom befragten Unternehmen nannten Verstöße gegen Datenschutzvorgaben am häufigsten als Risiko (80 Prozent KI-Nutzer, 70 Prozent Gesamtwirtschaft). Zudem stehen für KI-Nutzer Fehler bei der Programmierung (70 Prozent, Gesamtwirtschaft 57 Prozent) und Haftungsverpflichtungen bei Schäden (69 Prozent, Gesamtwirtschaft 47 Prozent) weit oben. In der Gesamtwirtschaft machen die Unternehmen sich nach Datenschutzverstößen am meisten Sorgen über neue IT-Sicherheitsrisiken (69 Prozent, KI-Nutzer 58 Prozent) und Anwendungsfehler bei der KI-Nutzung (67 Prozent, KI-Nutzer 34 Prozent).

Wie folgenreich die genannten KI-Risiken sein können, zeigen auch die kritischen Bereiche, in denen Unternehmen KI einsetzen oder einsetzen würden: So sollen KI-Anwendungen explizit die Arbeit von Fachkräften übernehmen, wie die Studie eco Branchenmonitor Internetwirtschaft zeigt. Besonders in der industriellen Fertigung würden es 58,7 Prozent der Deutschen gerne sehen, wenn Technologien auf Basis von Künstlicher Intelligenz Aufgaben von Fachkräften übernehmen würden. ⮑

Auch im Transportwesen (38,5 Prozent) und im Finanzsektor (24,3 Prozent) soll KI durchaus verantwortungsvolle Aufgaben leisten. Kommt es hier aber zu Fehlern durch KI, sind die Konsequenzen für die Unternehmen und die betroffenen Personen hoch.

Schwachstellen von KI können kriminell ausgenutzt werden

Neben den auch schwerwiegenden Fehlern, zu denen der KI-Einsatz ungewollt beitragen kann, gibt es die absichtliche Ausnutzung der Schwachstellen von KI. Eine wichtige Übersicht zu den Schwachstellen im Bereich LLM (Large Language Models) liefert insbesondere „Top 10 for Large Language Model Applications" des Open Worldwide Application Security Project (OWASP).

Das National Institute of Standards and Technology (NIST) der US-Regierung hat zudem die Arten von Cyberangriffen identifiziert, die das Verhalten von KI-Systemen manipulieren. KI-Systeme können demnach versagen, wenn sie mit nicht vertrauenswürdigen Daten in Berührung kommen, und Angreifer nutzen dieses Problem aus. Angreifer können so Systeme der Künstlichen Intelligenz absichtlich verwirren oder sogar „vergiften", sodass sie nicht mehr richtig funktionieren.

Es gibt viele Möglichkeiten für Cyberkriminelle, die Daten zu manipulieren, wie das National Institute of Standards and Technology betont, sowohl während der Trainingsphase eines KI-Systems als auch danach, während die KI ihr Verhalten durch Interaktion mit der physischen Welt weiter verfeinert. Dies kann dazu führen, dass die KI eine „unerwünschte Leistung" erbringt. Da die zum Trainieren einer KI verwendeten Datensätze viel zu groß sind, als dass Menschen sie erfolgreich überwachen und filtern könnten, gibt es noch keine sichere Möglichkeit, die KI vor Fehlleistungen zu schützen, so NIST.

NIST unterscheidet insgesamt vier Haupttypen von Angriffen: Umgehungs-, Vergiftungs-, Datenschutz- und Missbrauchsangriffe:

- Umgehungsangriffe, die nach der Bereitstellung eines KI-Systems auftreten, versuchen eine Eingabe zu ändern, um die Reaktion des Systems darauf zu ändern.
- In der Trainingsphase kommt es zu Poisoning-Angriffen (Vergiftung) durch die Einführung beschädigter Daten.
- Datenschutzangriffe, die während des Einsatzes auftreten, sind Versuche, vertrauliche Informationen über die KI oder die Daten, auf denen sie trainiert wurde, in Erfahrung zu bringen, um sie zu missbrauchen.

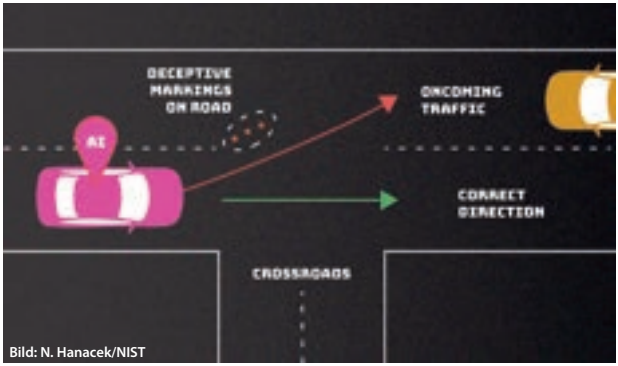


Bild: N. Hanacek/NIST

Ein KI-System kann versagen, wenn ein Gegner seine Entscheidungsfindung manipuliert. In diesem Beispiel führen fehlerhafte Markierungen auf der Straße dazu, dass ein fahrerloses, autonomes Auto möglicherweise in den Gegenverkehr gerät.

- Bei Missbrauchsangriffen werden falsche Informationen in eine Quelle, beispielsweise eine Webseite oder ein Online-Dokument, eingefügt, die dann von einer KI verarbeitet werden.

„Die meisten dieser Angriffe sind relativ einfach durchzuführen und erfordern minimale Kenntnisse des KI-Systems und begrenzte gegnerische Fähigkeiten", sagte Alina Oprea, Professorin an der Northeastern University. „Vergiftungsangriffe können zum Beispiel durch die Kontrolle einiger Dutzend Trainingsproben ausgelöst werden, was einen sehr kleinen Prozentsatz des gesamten Trainingssatzes ausmachen würde."

Trotz der erheblichen Fortschritte, die KI und maschinelles Lernen gemacht haben, sind diese Technologien anfällig für Angriffe, die spektakuläre Ausfälle mit schlimmen Folgen verursachen können, so die NIST-Studie.

KI ist ein Sicherheitsrisiko und kann selbst zum Gegner werden

Offensichtlich muss man KI als Sicherheitsrisiko einstufen, da Schwachstellen bestehen, die sich bösartig ausnutzen lassen. Zudem kann KI auch zum Angriffswerkzeug in Händen der Cyberkriminellen werden.

Ein Beispiel von vielen: Politisch motivierte Cyberangriffe erschöpfen sich nicht in Datendiebstahl oder im Lahmlegen digitaler Dienste, so das Bundesamt für Sicherheit in der Informationstechnik (BSI). Angreifer können sich in zunehmendem Maße die Möglichkeiten Künstlicher Intelligenz zunutze machen. Werkzeuge, mit denen Texte, Stimmen oder Bildmaterial geschaffen, verändert oder verfälscht werden können, sind immer leichter verfügbar und einfacher zu bedienen. Die Gefahr von Desinformation und Cybermobbing durch gefälschte Bilder oder Videos ist im Berichtszeitraum gestiegen, wie der Bericht zur Lage der IT-Sicherheit in Deutschland 2023 des BSI deutlich macht. □

Die Risikovielfalt bei der Nutzung von KI

Das EU-Parlament hat sich in Zusammenhang mit dem AI Act der EU ausführlich mit den Risiken durch einen Einsatz von KI befasst und nennt in diesem Zusammenhang (Auszug):

- Die Ergebnisse künstlicher Intelligenz hängen davon ab, wie sie konzipiert ist und welche Daten verwendet werden. Sowohl Daten als auch Design können absichtlich oder unabsichtlich verzerrt werden.
- Wird KI nicht ordnungsgemäß genutzt, so könnte sie beispielsweise bei Jobeinstellungen oder Kreditvergaben zu Entscheidungen führen, die durch ethnische Zugehörigkeit, Geschlecht oder Alter beeinflusst werden.
- Außerdem ergeben sich mögliche entscheidende Auswirkungen auf Privatsphäre und Datenschutz. KI kann beispielsweise für Gesichtserkennung oder Online-Tracking und Profiling von Einzelpersonen verwendet werden.
- KI kann dazu genutzt werden, extrem realistische, gefälschte Videos, Audioaufnahmen und Bilder zu erzeugen, die als „Deepfakes" bezeichnet werden. Diese Mechanismen können zu Polarisierung und Wahlmanipulation beitragen.
- KI-Tools, mit denen Menschen physisch in Berührung kommen oder die sogar in den menschlichen Körper implantiert werden, können hohe Sicherheitsrisiken darstellen, da sie missbraucht oder gehackt werden können.
- Ungleichgewichte beim Informationszugang könnten ausgenutzt werden. Auf der Grundlage des Online-Verhaltens einer Person oder anderer Daten kann ein Online-Anbieter beispielsweise ohne deren Wissen KI nutzen, um vorherzusagen, wie viel die Person zur Zahlung bereit ist.
- Ein weiteres Transparenzproblem besteht darin, dass es für die Menschen manchmal unklar sein kann, ob sie mit einer KI-Anwendung oder einer echten Person interagieren.

Wie Künstliche Intelligenz der Security helfen kann

Nicht nur Internetkriminelle können KI als Werkzeug nutzen, auch die Security-Abteilung kann von den besonderen Fähigkeiten der KI-Tools profitieren. Die Nutzung von KI in der Security ist nicht neu, sie findet bereits umfangreich statt, wird aber noch deutlich zunehmen.

Von Dipl.-Phys. Oliver Schonschek

KI-gestützte Angriffe werden von deutschen Unternehmen als größte Cyberbedrohung für dieses Jahr angesehen, so die Software-Analytiker von Capterra. Das Analystenteam untersuchte aber auch, in welchen Bereichen Unternehmen KI-gestützte Systeme nutzen, um sich

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

vor Angriffen zu schützen und welche Vorteile und Herausforderungen dies ihnen bringt.

Unternehmen investieren in KI für Security

Um Risiken, die durch Phishing oder unbeabsichtigtes Handeln von Mitarbeitern entstehen, entgegenzuwirken, haben laut der Studie KI-Investitionen in Cloud-Sicherheit (56 Prozent), E-Mail-Sicherheit (55 Prozent) und Netzwerksicherheit (47 Prozent) Priorität. Als KI-Vorteile für Security nannten die befragten Unternehmen die Möglichkeiten zur Verhaltensanalyse (Identifizierung von Anomalien und Mustern, die auf Bedrohungen hinweisen, 49 Prozent), Echtzeit-Monitoring (Erkennung von Bedrohungen, sobald sie auftreten, 48 Prozent) und Automatisierung (routinemäßige Sicherheitsaufgaben wie Warnungspriorisierung, Vorfallsreaktion und Patch-Management, 40 Prozent).
Auch das Beratungshaus PwC sieht eine klare Tendenz hin zu mehr KI-Nutzung für die Cybersicherheit. Sieben von zehn Unternehmen planen demnach, innerhalb des Jahres 2024 GenAI-Tools (Werkzeuge auf Basis generativer KI) für die Cyberabwehr einzusetzen.

KI ist schon heute Gegenstand der Security

Laut einer Umfrage von Gartner nutzen oder implementieren 34 Prozent der Unternehmen bereits Anwendungssicherheitstools für Künstliche Intelligenz, um die damit verbundenen Risiken generativer KI (GenAI) zu mindern. Mehr als die Hälfte (56 Prozent) der Befragten sagte, dass sie auch solche Lösungen planen. 26 Prozent der Umfrageteilnehmer gaben an, dass sie derzeit Technologien zur Verbesserung der Privatsphäre (PETs), ModelOps (25 Prozent) oder Modellüberwachung (24 Prozent) implementieren oder nutzen.
Doch nicht nur mehr Security für KI lohnt sich, auch mehr KI für die Cybersicherheit rechnet sich: Im vergangenen Jahr 2023 beliefen sich die durchschnittlichen Kosten für Datenschutzverletzungen für ein Unternehmen, das keine KI-gestützte Cybersicherheit einsetzt, auf 4,45 Millionen US-Dollar, so AltIndex.com. Bei Unternehmen, die dies taten, war dieser Wert um 40 Prozent oder 1,8 Millionen US-Dollar niedriger. Nach Angaben von AltIndex.com wird sich aufgrund dieser Erfolge der weltweite Markt für KI-Cybersicherheit voraussichtlich vervierfachen und bis 2030 einen Wert von 133 Milliarden US-Dollar erreichen.
Der Bericht des Capgemini Research Institute „Reinventing Cybersecurity with Artificial Intelligence“ unterstreicht diese Bedeutung von KI in der Cybersicherheit:

- Unternehmen halten es für zunehmend notwendig, die Cybersicherheit mit KI zu stärken – fast zwei Drittel glauben nicht, dass sie ohne KI kritische Bedrohungen erkennen können.
- Das Tempo der Einführung von KI in der Cybersicherheit nimmt zu – fast drei Viertel der Unternehmen testen KI in irgendeiner Weise in Anwendungsfällen der Cybersicherheit.
- Es gibt überzeugende Geschäftsgründe für den Einsatz von KI in der Cybersicherheit – drei von fünf Unternehmen geben an, dass der Einsatz von KI die Genauigkeit und Effizienz von Cyberanalysten verbessert.

Fazit

Viele Unternehmen nutzen Künstliche Intelligenz bereits in ihren Cybersicherheitsinitiativen oder planen die baldige Einführung, um Bedrohungsinformationen zu verbessern, Sicherheit, Orchestrierung, Automatisierung und Reaktion (SOAR) bereitzustellen, um das Sicherheitsmanagement zu verbessern, aber auch für die Cyberschulung. Offensichtlich hat KI in der Cybersicherheit eine große Zukunft, wenn die Security in der KI für mehr Schutz und Vertrauen sorgen kann. □

KI-Tools können Unternehmen zertifizieren

Sich ISO-zertifizieren zu lassen, das kostete die Unternehmen bisher viel Zeit und Geld. Deshalb verzichteten viele Klein- und Mittelunternehmer auf eine Zertifizierung. KI-Tools versprechen hier Abhilfe. Von Janne Siemens

Internet und Social Media ermöglichen es Unternehmen, sich mit Werbebotschaften direkt an ihre Zielkunden zu wenden. Im Wettbewerb um deren Aufmerksamkeit überbieten sie sich dabei förmlich: Jedes gibt (gefühlt) vor, das Günstigste, Beste, Kundenorientierteste, Innovativste usw. zu sein.

Im allgemeinen Marktgetöse Profil zeigen

Doch was steckt wirklich hinter den Werbeversprechen? Das können die Adressaten oft nicht beurteilen. Denn um in dem „Marktgetöse" überhaupt wahrgenommen zu werden, werden die Unternehmen, wie Dennis Berse, Geschäftsführer der Online Marketing-Agentur Adrock Marketing, Pfronten, betont, „mit ihren Selbstdarstellungen – speziell im Internet – stets schriller und lauter".

Doch wie können Klein-Unternehmen und Einzel-Unternehmer in diesem Umfeld ihre potenziellen Kunden noch davon überzeugen, dass sie wirklich kundenorientiert sind und ihnen eine Top-Qualität liefern – obwohl sie nicht

Bild: Funtap - stock.adobe.com

zu den Schreihälsen im Markt zählen? Insbesondere für Anbieter im B2B-Bereich stellt dies oft eine große Herausforderung dar; speziell dann, wenn sie sich gegen große etablierte Mitbewerber behaupten müssen, deren Marketingbudgets scheinbar unerschöpflich sind.

Zertifizierung als mögliche Problemlösung

Eine Option ist: Die eigene Organisation und ihre Leistung zertifizieren lassen – beispielsweise gemäß der Qualitätsnorm ISO 9001. „Gerade für kleine Unternehmen und Selbstständige bietet eine ISO-Zertifizierung große Vorteile", betont Reinhard Wanzek, Vorsitzender des Bundesverbands unabhängiger Zertifizierungsstellen (BVUZ), Bonn. „Denn sie signalisiert potenziellen Kunden: Der Anbieter legt Wert auf eine hohe Kundenorientierung und Qualität."

Das Problem war bisher das damit verbundene Procedere. „Als wir uns erstmals mit den Vorgaben der Norm ISO 9001 befasst haben, wurden wir von deren Komplexität fast erschlagen", erinnert sich Florian Kunze, Mitglied der Geschäftsleitung des Arbeitsbühnen-Anbieters Kunze GmbH, Bruckmühl: „Auch eine Investition von mehreren Tausend Euro für eine monatelange Beratung kam für uns nicht in Frage."

Bernd Brocher von der Vermakom GmbH, Würselen, die Notfallpläne für Auswanderer entwickelt, hatte dasselbe Problem: „Für uns war der Zertifizierungsaufwand bislang einfach zu groß."

Die Zahlen sprechen für sich: Von den vier Millionen KMU und Selbstständigen in Deutschland sind nur 50.000 zertifiziert. Der Grund: der hohe zeitliche und finanzielle Aufwand. Für eine ISO 9001-Zertifizierung müssen Solo-Unternehmer und Start-ups 5.000 Euro berappen, bei Unternehmen mit bis zu 10 Beschäftigten wird meist ein fünfstelliger Betrag fällig.

Nachweislich und sicher Qualität produzieren

Zertifizierungen werden in den nächsten Jahren immer wichtiger werden. Davon ist der Organisationsberater Klaus Doll, Neustadt an der Weinstraße, überzeugt: „Aufgrund der steigenden Zahl gesetzlicher Auflagen, die Unternehmen zu erfüllen haben, und weil die Marketingbotschaften speziell im Netz immer effekthascherischer werden, um möglichst viele Leads zu generieren." Deshalb werden Zertifizierungen, vermutet Doll, zu immer wichtigeren Differenzierungsmerkmalen im Wettbewerb werden – „sofern die Zertifikate von vertrauenswürdigen Zertifizierern stammen".

Sowohl die Kunze GmbH als auch die Vermakom GmbH nutzten ein KI-Tool für ihre ISO 9001-Zertifizierung. „Aus Zeit- und Kostengründen", erklärt Vermakom-Geschäftsführer Brocher. Und sein Kollege Florian Kunze von der Kunze GmbH ergänzt: „Wegen des bürokratischen Aufwands war uns klar: Wenn wir uns mit dem Thema Zertifizierung befassen, dann nur mit KI-Unterstützung." □

Digitale Souveränität bei IT-Sicherheitslösungen endlich ernst nehmen

Unternehmen und Behörden werden oft des „Greenwashings" und „AI-Washings" beschuldigt, nun auch des „Souveränitäts-Washings", indem sie digitale Souveränität und Datenschutz nur vortäuschen. Trotz Verfügbarkeit europäischer IT-Sicherheitslösungen setzen viele auf US-Anbieter, was problematisch ist. Open-Source-Technologien und europäische Standards bieten Lösungen gegen Abhängigkeit. Digitale Souveränität muss ernst genommen und praktisch umgesetzt werden. Von Elmar Eperiesi-Beck, Bare.ID

Bild: Funtap - stock.adobe.com

Unternehmen und Behörden werden zurecht verstärkt des „Greenwashings" bezichtigt, neuerdings auch des „AI-Washings". Ähnlich wie sich manche Organisationen Nachhaltigkeit oder den Einsatz von KI auf die Fahnen schreiben, obwohl es an der Umsetzung mangelt, achten sie vorgeblich auf die Sicherheit der Daten, ihrer eigenen wie der ihrer Kunden, und streben digitale Souveränität an.

Häufig aber kann in diesen Fällen eher von „Souveränitäts-Washing" die Rede sein, und ausgerechnet bei der Wahl von IT-Sicherheitslösungen machen sie es sich zu einfach, indem sie auf die bekannten US-Anbieter setzen. Dieser Umstand ist besonders im Lichte aktueller weltpolitischer Entwicklungen alles andere als begrüßenswert. Dabei stehen für nahezu alle Anwendungsbereiche der IT-Sicherheit Lösungen zur Verfügung, die sehr wohl digitale Souveränität und die Einhaltung hiesiger Datenschutzbestimmungen wie der DSGVO gewährleisten.

Digitale Souveränität – darum geht's

Kurz zur Erinnerung: Der Beauftrage der Bundesregierung für Informationstechnik definiert digitale Souveränität folgendermaßen: „‚Digitale Souveränität' beschreibt die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können. Dazu muss die Verarbeitung der für die Verwaltung notwendigen Daten durch zeitgemäße funktionale und vertrauenswürdige Informationstechnik gewährleistet werden." Für die öffentliche Verwaltung konstatiert der Bundesbeauftragte hingegen „hohe Abhängigkeiten zu einzelnen Technologieanbietern. Dies birgt die Gefahr, die Kontrolle über die eigene IT zu verlieren und u. a. Informations- und Datenschutz gemäß nationalen und EU-weit gültigen Vorgaben nicht mehr gewährleisten zu können." Im Wesentlichen geht es also darum, Abhängigkeit von einzelnen Technologieanbietern zu verhindern und technische Maßnahmen zu treffen, die geeignet sind, die Vorschriften für Informations- und Datenschutz einzuhalten.

Informations- und Datenschutz

Technische Maßnahmen, die geeignet sind, die Vorschriften für Informations- und Datenschutz einzuhalten, müssen vor allem sicherstellen, dass persönliche Daten nicht die EU verlassen und zudem die Auswertung dieser Daten durch Unbefugte anderweitig verhindern. Gerade bei IT-Sicherheitslösungen können viele Anbieter das nicht gewährleisten. Betrachten wir beispielsweise die Verwaltung von Logins und digitalen Identitäten, ist dies nahezu unmöglich, wenn die Identitäten im Klartext bei der im Drittland gehosteten Lösung vorliegen müssen. Dies ist ein grundsätzliches ⇨

Problem für alle Cloud-Dienste, bei IT-Sicherheitslösungen allerdings ist es als besonders problematisch zu betrachten. Unternehmen und Behörden in Deutschland sollten sich daher nicht nur zur Einhaltung von Vorschriften für Informations- und Datenschutz bekennen, sondern IT-Sicherheitslösungen wählen, deren Hersteller europäischen Datenschutzrechten unterliegen, die ausschließlich in Europa gehostet werden und auch hier entwickelt wurden.

Open Source und Standards gegen Anbieter-Abhängigkeit

Die Abhängigkeit von einigen wenigen IT-Anbietern ist ein alles andere als triviales Problem. Selbst wenn ein Anbieter zu Beginn einer Partnerschaft alle technischen und regulatorischen Anforderungen erfüllt, kann sich die Lage schnell ändern, wenn sich zum Beispiel die technischen Anforderungen des Kunden ändern oder ein neues Gesetz in Kraft tritt, das striktere Anforderungen an die Datenverarbeitung stellt. Insbesondere durch die Verwendung rein proprietärer Technologie machen es die meisten IT-Anbieter ihren Kunden nahezu unmöglich, kurz- oder auch nur mittelfristig auf einen anderen Anbieter umzusteigen.

Einen Ausweg bieten IT-Lösungen, die auf Open-Source-Technologie aufbauen und relevante Branchenstandards umsetzen, statt kom-

Bild: Artur - stock.adobe.com

IT-Lösungen, die auf Open-Source-Technologie aufbauen und relevante Branchenstandards umsetzen, bieten einen Ausweg aus der Abhängigkeit von einigen wenigen IT-Anbietern. Zudem sind sie vollkommen transparent und Anbieter-unabhängig entwickelt.

Für die öffentliche Verwaltung konstatiert der Beauftrage der Bundesregierung für Informationstechnik „hohe Abhängigkeiten zu einzelnen Technologieanbietern".

plett auf proprietäre Entwicklung zu setzen. Um wieder das Beispiel der Verwaltung von Logins und digitalen Identitäten zu wählen, steht mit dem Open Source IAM Framework Keycloak eine leistungsfähige und sichere Basis zur Verfügung, die sich jedoch im Eigenbetrieb als wenig benutzerfreundlich gestaltet. Glücklicherweise gibt es kommerzielle Anbieter, die den Lock-In vermeiden, indem sie die Open-Source-Basis nutzen und um eine Anwenderumgebung mit benutzerfreundlicher Admin-Oberfläche und weiteren Features anreichern. Sollte es aus irgendeinem Grund zu Unzufriedenheit mit dem Anbieter kommen, kann ein Kunde einfach auf die Open-Source-Basis umsteigen. Open-Source-Lösungen bieten zudem den Vorteil, dass sie ein größtmögliches Maß an Sicherheit bieten, weil sie vollkommen transparent sind und Anbieter-unabhängig entwickelt und kontrolliert werden.

Digitale Souveränität ernst nehmen

Um ein englisches Sprichwort zu verwenden, wird es Zeit „to put your money where your mouth is". Öl, Gas, Photovoltaik-Module, Hochleistungs-CPUs: Die Liste der Abhängigkeiten von unsicheren Lieferketten, die in Ländern bestenfalls zweifelhafter politischer Provenienz ihren Ursprung haben, ließe sich beinahe unendlich fortsetzen.

Es ist nicht absehbar, dass sich internationale Abhängigkeiten in Zeiten vielfältiger globaler Krisen von selbst verringern werden, und es gilt, die Fehler der Vergangenheit zu vermeiden. Daher ist es aktuell notwendiger denn je, dass Behörden und Unternehmen Worten Taten folgen lassen und die Gewährleistung digitaler Souveränität zu einem wichtigen Auswahlkriterium gerade für ihre IT-Sicherheitslösungen machen. □

Über den Autor

Elmar Eperiesi-Beck ist bei Bare.ID Teil des Managements und dort für Vertrieb und Strategie zuständig.

Schulungen sind mehr als ein Pflichtprogramm

Technik und Prozesse alleine können nicht sicherstellen, dass die neuen Vorgaben der EU-Regularien eingehalten werden. Die dritte Ebene „Mensch bzw. Personal" darf nicht fehlen. Hier werden insbesondere Maßnahmen zur Schulung und Sensibilisierung gefordert, die immer noch keine Selbstverständlichkeit sind.

Von Dipl.-Phys. Oliver Schonschek

Acht von zehn Unternehmen schulen Beschäftigte im Bereich der IT-Sicherheit, diese Meldung des Digitalverbands Bitkom ist auf den ersten Blick erfreulich. Doch die Details aus der Bitkom-Umfrage zeigen, dass beim Thema Security Awareness weiterhin Handlungsbedarf besteht: Nur jedes dritte Unternehmen (33 Prozent) schult grundsätzlich alle Mitarbeiterinnen und Mitarbeiter zu IT-Sicherheitsfragen, weitere 51 Prozent nur solche in bestimmten Positionen und Bereichen. 15 Prozent der Unternehmen führen hingegen überhaupt keine IT-Sicherheitsschulungen durch.

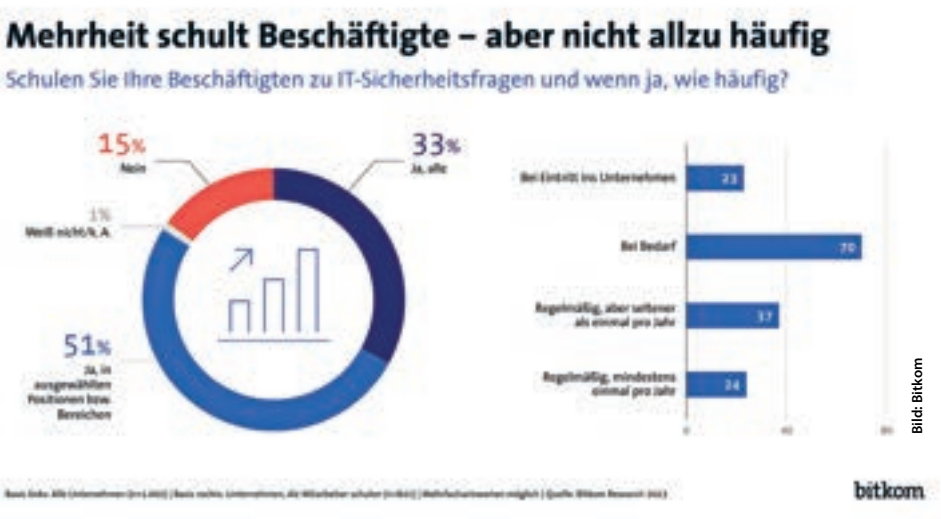
Eine weiteres Manko: Viele Unternehmen, die die gesamte oder zumindest einen Teil ihrer Belegschaft zur IT-Sicherheit weiterbilden, tun dies nicht regelmäßig. Nur rund jedes vierte dieser Unternehmen (24 Prozent) gibt an, mindestens einmal pro Jahr Schulungen durchzuführen. Weitere 37 Prozent bieten zwar regelmäßig entsprechende Schulungen an, diese finden aber seltener als einmal pro Jahr statt. 70 Prozent der Unternehmen geben zudem an, dass sie nur bei Bedarf die Beschäftigten schulen, 23 Prozent beim Eintritt ins Unternehmen.

Um den neuen Regularien zu entsprechen, sollte sich hier jedoch einiges ändern. Dabei sollte die Security Awareness aber nicht nur als Compliance-Bestandteil gesehen werden. „IT-Sicherheit beginnt bei den Menschen. Wer weiß, wie Cyberangreifer vorgehen, fällt nicht so leicht auf deren Tricks rein. Und regelmäßig geschulte Mitarbeiterinnen und Mitarbeiter können einen erfolgreichen Angriff frühzeitiger erkennen und so den Schaden für das Unternehmen begrenzen", erklärt Bitkom-Präsident Ralf Wintergerst.

Vorgaben für Security-Schulungen bei DORA

DORA (Digital Operational Resilience Act, digitale operationale Resilienz im Finanzsektor) enthält an die Unternehmensleitung die Forderung, angemessene Haushaltsmittel zuzuweisen und diese regelmäßig zu überprüfen, um den Anforderungen des Finanzunternehmens an die digitale Betriebsstabilität in Bezug auf die verschiedensten Ressourcen gerecht zu werden, einschließlich Schulungen zu IKT-Risiken und -Kompetenzen für alle einschlägigen Mitarbeitenden.

Zudem müssen die Mitglieder des Leitungsorgans regelmäßig Fachschulungen absolvieren, um ausreichende Kenntnisse und Fähigkeiten zu erwerben und auf dem neuesten Stand zu halten, damit sie IKT-Risiken und deren



Viele Unternehmen bilden im Bereich IT-Sicherheit nur einen Teil der Belegschaft weiter und das auch nur selten, so eine Bitkom-Umfrage.

Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten können. Weiterhin besagt DORA: Finanzunternehmen entwickeln Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen für digitale Betriebsstabilität, die im Rahmen ihrer Programme für die Mitarbeiterschulung obligatorisch sind. Diese gelten für alle Beschäftigten und die Geschäftsleitung.

NIS2 nennt sogar konkrete Schulungsthemen

Die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie) hat auch die Sensibilisierung zur Cybersicherheit und zu Cyberrisiken im Blick. So fordert NIS2: Die wesentlichen und wichtigen Einrichtungen sollen eine breite Palette grundlegender Praktiken der Cyberhygiene anwenden, darunter Sensibilisierung der Nutzer, Schulungen für ihre Mitarbeiter organisieren und das Bewusstsein für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken schärfen.

Zudem sollen die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen und allen Mitarbeitern regelmäßig entsprechende Schulungen anbieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben. Damit nennt NIS2 sogar konkrete Schulungsthemen, die bei der Security Awareness nicht mehr fehlen dürfen.

Es zeigt sich, dass die neuen Regularien für IT-Sicherheit und Datenschutz umfangreichen Handlungsbedarf für die betroffenen Unternehmen mit sich bringen – auf allen Ebenen: Technik, Prozesse und Personal. Dabei sollte klar sein, dass es nicht nur um Compliance geht, sondern immer um den Schutz von Daten, Systemen und insbesondere Menschen. □

Letzte Verteidigungslinie in Gefahr

Ransomware-Angriffe zählen seit Jahrzehnten zu den größten Cybersecurity-Gefährdungen. Doch gerade in den letzten Jahren haben die Attacken drastisch zugenommen. Zudem haben Hacker ein neues lukratives Ziel ausgemacht: die Backup-Dateien von Unternehmen. Dr. Yvonne Bernard, CTO bei Hornetsecurity, erklärt, welche Maßnahmen Unternehmen jetzt ergreifen müssen, um ihre Sicherungskopien vor böswilliger Manipulation zu schützen – und wie Immutable-Cloud-Speicher helfen kann.

Von Dr. Yvonne Bernard, Hornetsecurity

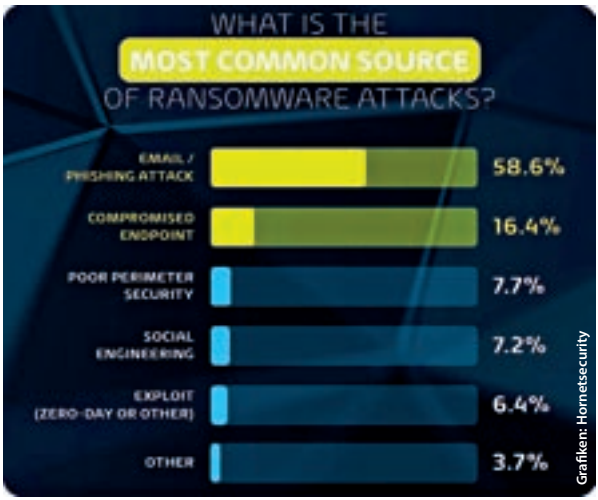
Bild: alphaspirit - stock.adobe.com

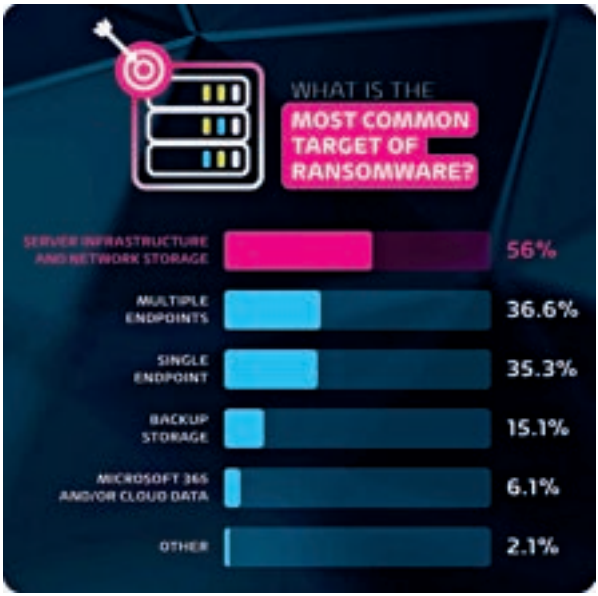
Es ist ein düsteres Bild, das sich aktuell zeichnen lässt. Immer mehr Unternehmen werden Opfer von Ransomware-Angriffen. Die Frage ist längst nicht mehr „Ob?“, sondern „Wann?“. Eine Ransomware-Studie von Hornetsecurity belegt, dass bereits jedes vierte Unternehmen von einem Angriff mit Erpressungssoftware betroffen war. In den letzten Jahren geht darüber hinaus die beunruhigende Tendenz immer mehr in Richtung Backups. Der Anteil dieser Angriffe liegt bereits bei 15 Prozent.

Gleichzeitig werden die Ransomware-Attacken immer intelligenter und gefährlicher. So kursieren im Darknet vermehrt Ransomware-as-a-Service-Angebote, mit denen Betrüger auch ohne Programmierkenntnisse und entsprechende IT-Infrastruktur erfolgreiche Erpressungskampagnen von einem „Dienstleister“ durchführen lassen können. Eine neue Dimension wurde jüngst mit der Ausbreitung generativer KI-Modelle – allen voran ChatGPT – erreicht. So gelang es IT-Sicherheitsforschern mithilfe des innovativen KI-Bots, mit minimalem Aufwand ausgeklügelte Ransomware zu entwickeln, die für die Opfer hohe Risiken bergen kann.

Sicherungskopien verstärkt im Visier

Bei den vermehrten Ransomware-Angriffen speziell auf Backups nutzen die Hacker Erpressungs-Software, um die auf den Speichermedien gesicherten Daten zu verschlüsseln oder den Nutzern den Zugriff zu versperren. Das ist besonders perfide, da ein Unternehmen gerade auf Sicherungskopien angewiesen ist, wenn die Daten in den Produktivsystemen verlorengehen oder beschädigt werden. Nur gegen ein Lösegeld sollen die Backups freigeschaltet oder wiederhergestellt werden. Geht die Zahlung nicht rechtzeitig ein, ⇨





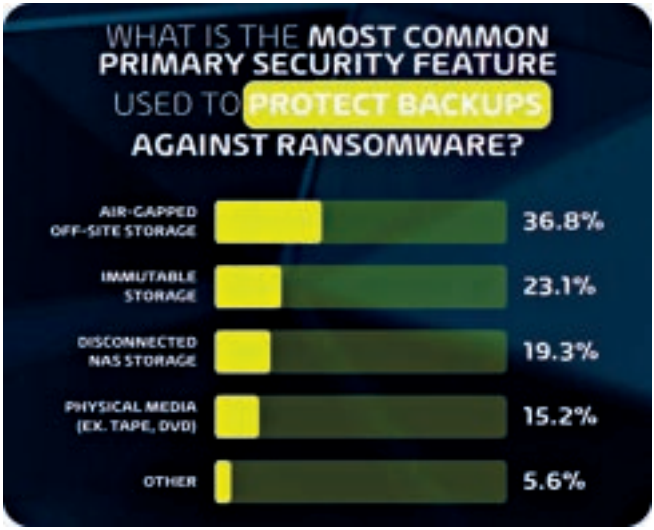
drohen die Angreifer damit, die Daten zu löschen, zu stehlen oder sensible Unternehmensinformationen zu veröffentlichen.

Aus diesem Grund entsteht für Unternehmen ein jährlicher finanzieller Schaden in Millionenhöhe. Längst sind sechs- oder siebenstellige Lösegeldforderungen an der Tagesordnung. Die Software erlaubt es den Hackern, ganze Arbeitsabläufe und -prozesse nachhaltig zu stören – oder gar die ganze IT eines Unternehmens zum Stillstand zu bringen. Gleichzeitig drohen der Verlust oder Diebstahl vertraulicher Unternehmensdaten. Kommen beispielsweise einem Kreditinstitut sensible Kundendaten abhanden, ist neben Schadensersatzforderungen auch mit einem dauerhaften Imageverlust und einer erhöhten Kundenfluktuation zu rechnen. So steigert sich der finanzielle Schaden exorbitant.

Erhöhter Druck durch NIS2-Vorgaben

Zeitgleich müssen sich die Unternehmen auf verschärfte gesetzliche Datenschutz- und Compliance-Vorgaben einstellen. Während bislang vorrangig die EU-Datenschutz-Grundverordnung (DSGVO/General Protection Regulation, GDPR) von 2018 maßgebend war, gilt es jetzt, die neue EU-Cybersicherheits-Richtlinie NIS2 (Network and Information Security) zeitnah umzusetzen.

Sie verschärft die Sicherheitsanforderungen an die Betreiber Kritischer Infrastrukturen (KRITIS). Erstmals werden auch kleine und mittelständische Einrichtungen in systemrelevanten Bereichen des öffentlichen Lebens – wie Gesundheit, Bildung und Behörden – adressiert. Da auch die Zulieferer NIS2 einhalten müssen, sind künftig fast alle Unternehmen und Organisationen von der neuen Richtlinie betroffen. Kommt es zu Datenschutz- und Compliance-Verstößen, sind die Verantwortlichen nun persönlich haftbar und können mit Strafen von bis zu 10 Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes belegt werden. Da die EU-Mitgliedstaaten nur noch bis Oktober 2024 Zeit haben, die Richtlinie umzusetzen, sollten die Unternehmen sich schleunigst daran machen, die erforderlichen Sicherheitsmaßnahmen zu implementieren.



Immutable Backups gegen Ransomware

Dies gilt auch für den Schutz der Backup-Dateien. Prinzipiell kann Ransomware aus unterschiedlichen Quellen stammen und auf verschiedenen Wegen übertragen werden. Ganz vorne rangieren Phishing-Mails, die infizierte Anhänge enthalten und zu einer Kompromittierung des gesamten Netzwerks führen können. Um diese Risiken zu mindern, kombinieren viele Unternehmen verschiedene Methoden, darunter Endpunkt-Sicherheit, Advanced Threat Detection and Response,

Patch-Management, Multi-Faktor-Authentifizierung (MFA) sowie Sicherheitsschulungen für die Mitarbeiter. Als zusätzliche Sicherheitsebene speziell für Sicherungskopien empfehlen sich Immutable Backups.

Immutability (Unveränderbarkeit) von Datensicherungen lässt sich mit mehreren Methoden erreichen. Zur Abwehr von Ransomware-Angriffen wird heute vor allem die WORM-Technik eingesetzt, die bereits in den späten 1970er-Jahren entwickelt wurde. WORM steht für „Write Once, Read Many", was bedeutet, dass eine Sicherungskopie nur einmal erstellt werden kann (Schreiben) und dann schreibgeschützt ist. Bei der Auswahl einer Backup-Lösung sollten die Unternehmen also ein Produkt bevorzugen, das die Unveränderlichkeit durch den Einsatz von WORM-Technologie unterstützt. Zur Speicherung der Daten können verschiedene Medien wie Speicherkarten und externe Festplatten oder externe Cloud-Dienste zum Einsatz kommen.

Besonders im Umgang mit virtuellen Maschinen (VM) werden Backup, Replikation und Wiederherstellung von Dateien vermehrt über Immutable-Cloud-Speicher durchgeführt. Backup-Lösungen, die einen Fokus auf die Nutzung von VMs legen, müssen dabei unterschiedliche Vorgaben erfüllen.

Einerseits ist es essenziell, dass eine Lösung den jüngsten Compliance-Vorschriften für Datensicherheit und Datenschutz entspricht. Andererseits sollte die Lösung möglichst breit anwendbar sein, sodass Unternehmen ihre Sicherheitskopien auf unterschiedliche Wege – wie beispielsweise Microsoft Azure, Amazon S3, lokale Festplatten oder auch Offsite-Backup-Server – ablegen können. Des Weiteren sollten Backup-Daten einfach für klar definierte Zeitspannen manipulationssicher aufbewahrt werden und sämtliche VMs über eine zentral und intuitiv zu bedienende Oberfläche überwacht und verwaltet werden können.

Bröckelt die letzte Bastion?

Im Zuge der steigenden Ransomware-Angriffe geraten Backup-Dateien als letztes Bollwerk gegen die Löschung und Manipulation wichtiger Unternehmensdaten zunehmend unter Beschuss. Aus diesem Grund sollten Unternehmen dazu übergehen, ihre Backups mit entsprechenden Lösungen abzusichern. Besonders unter Berücksichtigung der WORM-Technologie können Immutable-Cloud-Speicher mit modernen Lösungen möglichst effizient geschützt werden.

Unternehmen sollten sich also so schnell wie möglich um ihre Backups kümmern. Sind diese erst einmal verloren, ist der Schaden nicht mehr so leicht einzugrenzen. □


Bild: FotoStudio54

Über die Autorin

Dr. Yvonne Bernard ist CTO bei Hornetsecurity, einem weltweit führenden Anbieter von Cloud-basierten Sicherheits-, Compliance-, Backup- und Security-Awareness-Lösungen der nächsten Generation, die Unternehmen und Organisationen jeder Größe auf der ganzen Welt unterstützen. Das Flaggschiffprodukt 365 Total Protection ist die umfassendste Cloud-Sicherheitslösung für Microsoft 365 auf dem Markt.

Impressum

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

Geschäftsführer:
Tobias Teske, Günter Schürger

IT-BUSINESS

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

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

Account Management:
Besa Agaj/International Accounts (-112),
David Holliday (-193),
Stephanie Steen (-211)

SECURITY-INSIDER

Redaktion: Peter Schmitz/ps (-165) – Chefredakteur (verantwortlich für redaktionelle Inhalte),
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: Carin Böhm (Titel),
Jürgen Paukner, Johannes Rath, Udo Scherlin,
Gaby Weihmayer

EBV: Carin Böhm, Gaby Weihmayer

Anzeigen-Layout: Johannes Rath

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

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

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

Inserenten

TeleTrusT
Pioneers in IT security.

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

www.teletrust.de

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

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

www.teletrust.de/itsmig

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

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

Besuchen Sie TeleTrusT auf der it-sa in Halle 9 / Stand 9-245.

NG2000-Serie

Router - Made in Germany

Leistungsstarke Konnektivität mit DSL, 4G und 5G

Verfügbar bei unseren Distributionspartnern:

herweck

MICHAEL AG
Passion for ICT solutions

pilot
Computerhandels GmbH

SYSTEAM
Gesellschaft für Computersysteme mbH

TDT | Your experts in TELE COMMUNICATION

Weitere Infos unter **www.tdt.de**