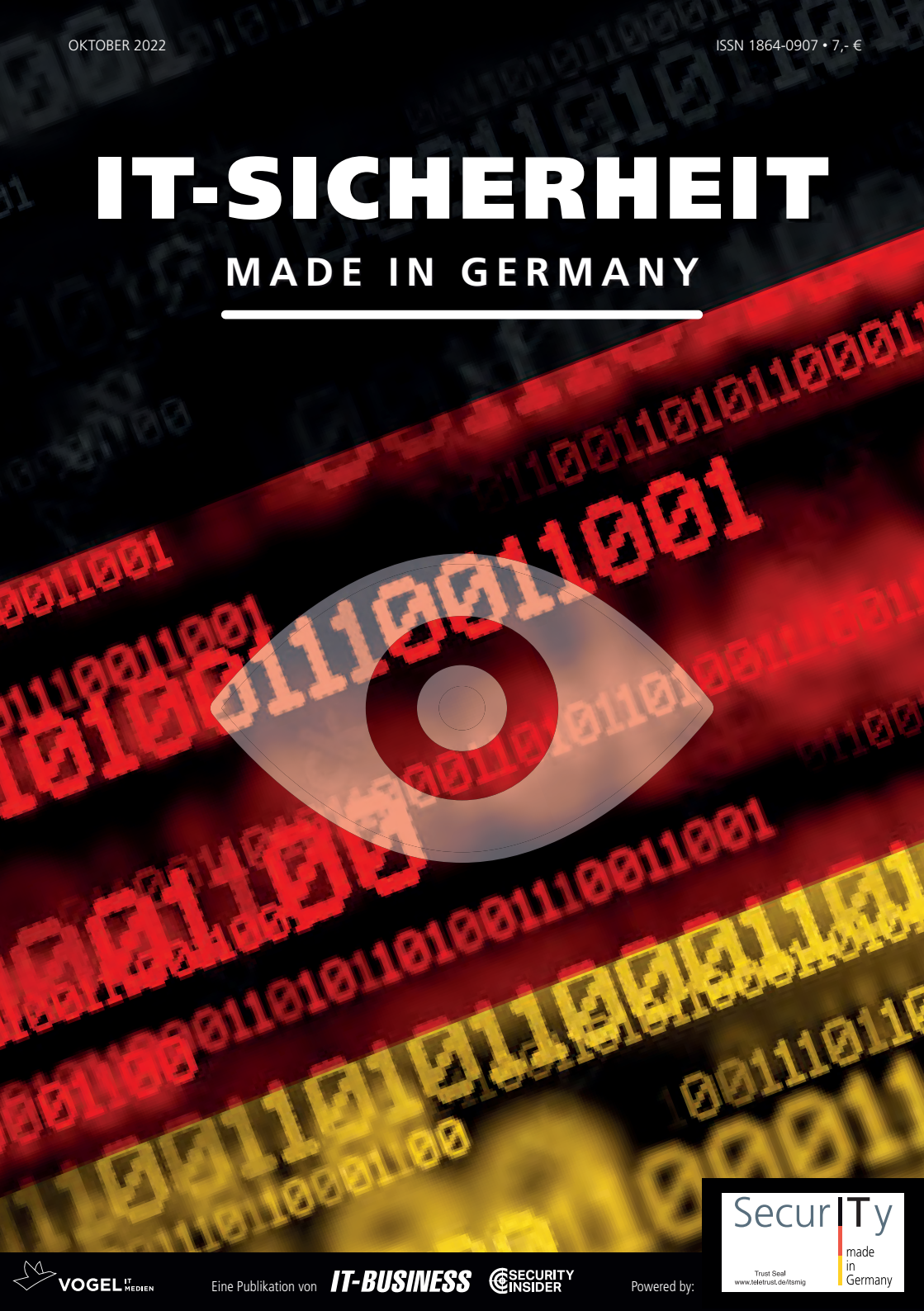
OKTOBER 2022

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

MADE IN GERMANY



VOGEL IT MEDIEN

Eine Publikation von IT-BUSINESS SECURITY INSIDER

Powered by:

G DATA academy

G DATA auf der it-sa

Besuchen Sie uns zwischen dem 25. und 27. Oktober in Halle 7A (Stand 7A-311). Wir freuen uns auf Sie!

DAS SECURITY UPGRADE FÜR IHR TEAM

Mit unseren Online-Trainings lernen Mitarbeitende, wie sie den digitalen Alltag sicher machen.

Es bedarf einer Umsetzungsstrategie


Bild: TeleTrusT

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

Liebe Leserinnen und Leser,

globale Krisen wie die Pandemie, die Lieferketten-Schwierigkeiten sowie der Krieg in der Ukraine haben die IT- und damit die IT-Sicherheitsbranche in den vergangenen zwei Jahren vor diverse Herausforderungen gestellt.

Die digitale Transformation in Deutschland stagniert in einigen Bereichen nach wie vor, schreitet aber voran. Zugleich wächst das Risiko von Angriffen. Diese Cyber-Angriffe werden breiter gefächert, raffinierter und professioneller und richten Milliardenschäden an. Die IT-Kriminalität erfährt eine zunehmende Industrialisierung und dies nicht erst seit dem Krieg in der Ukraine.

IT-Sicherheit kann nur durch ein zielgerichtetes und langfristiges Vorgehen erfolgreich umgesetzt werden. Es bedarf einer Umsetzungsstrategie, die Ziele definiert, Maßnahmen priorisiert und festlegt sowie eine Aufgabenverteilung zwischen Politik und Industrie vornimmt. Die Politik ist aufgerufen, Impulse zu setzen und langfristig zu unterstützen. Europa muss seine Konkurrenzfähigkeit neu erlangen und erhalten. Als Bundesverband IT-Sicherheit wünschen wir uns entsprechende Schwerpunktsetzungen.

Die notwendigen Abwehrtechnologien und Werkzeuge sind vorhanden, werden aber in der Praxis oft noch zu wenig oder nicht konsequent eingesetzt. Als Verband aktualisieren wir beispielsweise im TeleTrusT-Arbeitskreis "Stand der Technik in der IT-Sicherheit" fortlaufend die gleichnamige Handreichung. Dabei sind wir bestrebt, Unternehmen, Anbietern und Dienstleistern Hilfestellung bei der Bestimmung des "Standes der Technik" zu geben.

Die vorliegende Publikation vermittelt Einblicke in ausgewählte Themen, die uns derzeit fachlich und politisch beschäftigen. Die Beiträge zielen auf grundsätzliche Fragen ab, mit denen sich IT-Verantwortliche befassen sollten: Sicherheitskonzepte für die Digitalisierung des Mittelstandes, Security Awareness, Managed Security, Security im Public-Sektor und vieles mehr. Die Publikation gibt Orientierung und fasst die wichtigsten Maßgaben für die IT-Sicherheit zusammen.

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.

Trust Seal
www.teletrust.de/itsmig

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

ISXQIV/22

IT-Security Virtual Conference

» 23. NOVEMBER DIGITAL

www.isxconference.de

JETZT ANMELDEN!

IT-SECURITY IN THE **NEW CYBERCRIME WORLD**

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

HIER GEHT ES ZUR WEBSITE

» JETZT TICKET SICHERN

Eine Veranstaltung der VOGEL IT AKADEMIE

Vertrauen hat einen Namen

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

Von Dr. Holger Mühlbauer und Jürgen Paukner

Träger des Vertrauenszeichens "IT Security made in Germany" (Stand 15.09.2022)

- Accellence Technologies GmbH
- AceBIT GmbH
- achelos GmbH
- Achtwerk GmbH & Co. KG
- ads-tec GmbH
- aigner business solutions GmbH
- akquinet enterprise solutions GmbH
- Allgeier IT Solutions GmbH
- ANMATHO AG
- Antago GmbH
- AOE GmbH
- apsec Applied Security GmbH
- ASOFTNET
- asvin GmbH
- ATIS systems GmbH
- Atruvia AG
- AUCONET Solutions GmbH
- AUTHADA GmbH
- AWARE7 GmbH
- axilaris GmbH
- Bank-Verlag GmbH
- BAYOOSOFT GmbH
- Bechtle GmbH & Co. KG
- Beta Systems IAM Software AG
- Biteno GmbH
- Blue Frost Security GmbH
- Bosch CyberCompare
- Build38 GmbH
- Bundesdruckerei GmbH
- CBT Systems & Services GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- certgate GmbH
- CERTIX IT-Security GmbH
- CGM Deutschland AG
- Cherry GmbH
- CHIFFRY GmbH
- Cognitec Systems GmbH
- COGNITUM Software Team GmbH
- COMback Holding GmbH
- comcrypto GmbH
- comforte AG
- Communisystems-Care GmbH
- comtime GmbH
- Condition-ALPHA Digital Broadcast Technology Consulting
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- Crashtest Security GmbH
- CryptoMagic GmbH
- Cryptshare AG
- cv cryptovision GmbH
- Cybersense GmbH
- dacoso data communication solutions GmbH
- dal33t GmbH
- DATAKOM GmbH
- datenschutzklinik
- DATUS AG
- DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
- DELIT AG
- DERMALOG Identification Systems GmbH
- Detack GmbH
- Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG
- DFN-CERT Services GmbH
- Digital Enabling GmbH
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- dinext. pi-sec GmbH
- ditis Systeme Niederlassung der JMV GmbH & Co.
- DoctorBox GmbH
- DRACOON GmbH
- Dreyfield & Partner Deutschland GmbH
- DriveLock SE
- D-Trust GmbH
- e-ito Technology Services GmbH
- eCom Service IT GmbH
- ecsec GmbH
- EgoMind GmbH
- enclaive GmbH
- Enginsight GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- essentry GmbH
- FAST LTA GmbH
- floragunn GmbH
- FSP GmbH
- FZI Forschungszentrum Informatik
- GBS Europa GmbH
- G DATA CyberDefense AG
- Generation Secure GmbH
- genua GmbH
- glacier advisory & coaching
- GORISCON GmbH
- Hanko GmbH
- HDPnet GmbH
- HiScout GmbH
- HK2 Rechtsanwälte
- Hornetsecurity GmbH
- IDEE GmbH
- if(is) – Institut für Internet-Sicherheit
- Infineon Technologies AG
- INFODAS GmbH
- Inlab Networks GmbH
- inlyse GmbH
- INNOSYSTEC GmbH
- innovaphone AG
- INSYS MICROELECTRONICS GmbH
- intelliCard Labs GmbH
- Intelligent Minds UG
- IoT Inspector GmbH
- isits AG International School of IT Security
- ISL Internet Sicherheitslösungen GmbH
- ITConcepts PSO GmbH
- ITSG GmbH
- itWatch GmbH
- keepbit IT-SOLUTIONS GmbH
- KikuSema GmbH
- KnowledgeRiver GmbH

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

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

Die Liste der zertifizierten deutschen Unternehmen wächst beständig. Die aktuelle Liste der Unternehmen, denen die Nutzung des Vertrauenszeichens derzeit eingeräumt wird, können Sie einsehen unter: www.teletrust.de/itsmig/zeichentraeger/ □

- KOPRAX Systemhaus GmbH & Co. KG
- LANCOM Systems GmbH
- LEIBOLD Sicherheits- und Informationstechnik GmbH
- limes datentechnik® gmbh
- Linogate GmbH
- LocateRisk UG
- m3 management consulting GmbH
- maincubes one GmbH
- MaskTech GmbH
- MATESO GmbH
- Matrix42 AG
- MB Connect Line GmbH Fernwartungssysteme
- Mentana Claimsoft GmbH
- MGR Integration Solutions GmbH
- MH-IT + Service GmbH
- M&H IT-Security GmbH
- MTG AG
- MTRIX GmbH
- Mühlbauer ID Services GmbH
- NCP engineering GmbH
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- NETZWERK Software GmbH
- Nexis GmbH
- NG Guard Technology GmbH
- nicos AG
- nicos cyber defense GmbH
- Nimbus Technologieberatung GmbH
- OctoGate IT Security Systems GmbH
- ondeso GmbH
- Opexa Advisory GmbH
- OPTIMA Business Information Technology GmbH
- OTARIS Interactive Services GmbH
- P3KI GmbH
- pen.sec AG
- PFALZKOM GmbH
- PHOENIX CONTACT Cyber Security GmbH
- PHYSEC GmbH
- Pix Software GmbH
- PPI Cyber GmbH
- PRESENSE Technologies GmbH
- Primary Target GmbH
- procilon GmbH
- PSW GROUP GmbH & Co. KG
- Pyramid Computer GmbH
- QGroup GmbH
- QuoIntelligence GmbH
- real-cis GmbH
- Resility GmbH
- retarus GmbH
- Rhebo GmbH
- RheinByteSystems GmbH
- Robin Data GmbH
- Rohde & Schwarz Cybersecurity GmbH
- r-tec IT Security GmbH
- SAMA PARTNERS Business Solutions GmbH
- sayTEC AG
- SBE network solutions GmbH
- Schönhofer Sales and Engineering GmbH
- SCHUTZWERK GmbH
- SC-Networks GmbH
- Secomba GmbH
- Secorvo Security Consulting GmbH
- secrypt GmbH
- SECUDOS GmbH
- secunet Security Networks AG
- Securepoint GmbH
- secuvera GmbH
- sequrium GmbH
- SerNet GmbH
- signotec GmbH
- Skyflare GmbH
- SL.IS Services GmbH
- Smartify IT Solutions GmbH
- Softline AG
- SoSafe GmbH
- SRC Security Research & Consulting GmbH
- Steen Harbach AG
- Steganos Software GmbH
- suresecure GmbH
- SVA System Vertrieb Alexander GmbH
- syracom consulting AG
- TDT AG
- TE-SYSTEMS GmbH
- Tech-Prax GmbH
- teamwire GmbH
- Teligencia UG
- Tenzir GmbH
- TG alpha GmbH
- TMB Service GmbH
- Trufflepig IT-Forensics GmbH
- TrustCerts GmbH
- TrustSpace
- TÜV Informationstechnik GmbH
- TÜV Rheinland i-sec GmbH
- TWINSOFT biometrics GmbH & Co. KG
- UMH Systems GmbH
- Uniki GmbH
- Uniscon GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- virtual solution AG
- VisionmaxX GmbH
- VMRay GmbH
- Voleatech GmbH
- Vulidity GmbH
- WMC Wüpper Management Consulting GmbH
- Würzburger Versorgungs- und Verkehrs GmbH
- XignSys GmbH
- XnetSolutions KG
- zeroBS GmbH
- Zertificon Solutions GmbH

Vorbereitung auf den Angriffsfall: Kostenloses Whitepaper hilft beim Aufbau von Incident Response Readiness

Um im Falle eines Cyberangriffs adäquat reagieren zu können, benötigen betroffene Unternehmen vor allem eines: die bestmögliche Vorbereitung. Da Hacker in der Lage sind, sich mit extrem hoher Geschwindigkeit in gekaperten Netzwerken auszubreiten, muss in dieser Situation schließlich schnellstmöglich gehandelt werden. Die besten Voraussetzungen für eine Erfolg versprechende Gegenreaktion lassen sich durch den Aufbau einer Incident Response Readiness schaffen.

Die Incident Response Readiness stellt Ihre bestehenden technischen und nichttechnischen Maßnahmen zur Bewältigung von Cyberangriffen auf den Prüfstand. Ziel: Schnelle und effiziente Reaktionsfähigkeit im Angriffsfall. Um diese Reaktionsfähigkeit zu erreichen, müssen unter anderem Notfallpläne und Playbooks für typische Incidents erstellt werden. Zudem ist es notwendig, geeignete IT-Security-Komponenten zu implementieren und an die Anforderungen des jeweiligen Unternehmens anzupassen. Darüber hinaus sollte festgelegt werden, welche Personen im Angriffsfall für welche Aufgaben zuständig sind.

Angriffe eindämmen und den Normalbetrieb wiederherstellen

Wer derartige Vorkehrungen trifft, kann im Angriffsfall schnell die richtigen Maßnahmen ergreifen, um Attacken einzudämmen und den Normalbetrieb wiederherzustellen. So können finanzielle Schäden und Reputationsverluste minimiert werden. Um Unternehmen einen Überblick über notwendige Vorkehrungen zu geben, haben die Cyber-Defense-Spezialisten der r-tec IT Security GmbH auf Basis ihrer Erfahrung ein Whitepaper zum Thema Incident Response Readiness erstellt. Das Dokument enthält unter anderem eine Checkliste, die einen ersten Überblick über die zu ergreifenden technischen und nichttechnischen Maßnahmen gibt. Zudem wird erläutert, wie typische Angriffe und Standard-Incident-Response-Prozesse ablaufen. ■

Interessierte können das Whitepaper auf der r-tec-Website kostenlos downloaden:
r-tec.net/whitepaper-irr

Garantierte Reaktionszeiten. Umfassende Vorbereitung.

Incident Response Service

Im Ernstfall einen kompetenten Partner schnell an Ihrer Seite

Mit unserem Incident Response Service stellen wir sicher, dass Ihrem Unternehmen im Ernstfall die richtigen Ressourcen und Kompetenzen zur Verfügung stehen, um Angriffe effektiv einzudämmen. Sie zahlen eine feste monatliche Pauschale und wir bieten Ihnen dafür einen Bereitschaftsdienst mit garantierten Annahme- und Reaktionszeiten. Durch einen im Vorfeld von uns erarbeiteten Maßnahmenplan sparen Sie im Ernstfall wertvolle Zeit.

r-tec.net/irs

"Ohne IT-Sicherheit ist Digitalisierung gefährlich"


Bild: TeleTrusT

André Kudra ist im Vorstand des Bundesverbandes für IT-Sicherheit (TeleTrusT) und CIO beim Digitalisierungsdienstleister esatus. Nicht nur in diesen beiden Funktionen beschäftigt er sich mit IT-Sicherheitsfragen. Besonderes Augenmerk legt er darauf, wie Unternehmen jeder Größe in Deutschland ein mehr als nur akzeptables Niveau an IT-Sicherheit erlangen können.

Herr Kudra, was umfasst das Label "IT Security Made in Germany" und wie ist dieses in den europäischen und den weltweiten Kontext einzuordnen?

Dr. André Kudra: Das Vertrauenszeichen "IT Security made in Germany" (ITSMIG) ist in erster Linie eine Selbstverpflichtung von TeleTrusT-Mitgliedern. Ein Unternehmen verpflichtet sich unter anderem, dass seine Produkte keine Backdoors enthalten und dass seine IT-Sicherheitsforschung und -entwicklung in Deutschland stattfindet. ITSMIG ist markenrechtlich geschützt und interessierte Verbandsmitglieder bekommen es auf Antrag und Konformitätserklärung zeitlich befristet gestattet. Gleichermaßen gibt es von TeleTrusT noch "IT Security made in EU" (ITSMIE). Dieses Label ist besonders für Mitglieder geeignet, die ihren Hauptsitz in der EU aber nicht in Deutschland haben. Die Selbstverpflichtung ist ein leichtgewichtiger Vorgang, der mit hoher Signalwirkung und starkem Reputationseffekt einhergeht.

Andere Labels sind beispielsweise die "EU Cybersecurity Certification Schemes" der European Union Agency for Cybersecurity (ENISA) oder die global bekannten und anerkannten "Evaluation criteria for IT security" gemäß ISO/IEC 15408-1:2022 – die sogenannten "Common Criteria". Diese erfordern das Durchlaufen eines umfassenden Zertifizierungsprozesses. Das ist ein erheblich größerer Aufwand für Unternehmen, die solch ein Label für sich beziehungsweise ihre Produkte beanspruchen wollen. Das ist nichts für nebenbei. Perspektivisch wäre es wünschenswert, dass einfach mehr Produkte ganz automatisch gemäß des "Security by Design"-Prinzips sicherer werden – ob zertifiziert oder nicht.

Wie schaffen Unternehmen die Balance zwischen Security und Innovationsfreiheit?

Nur weil man innovativ ist, bedeutet es nicht, dass man sich an nichts zu halten hat und jegliche Sicherheitsanforderungen erst einmal

ignorieren kann. Bei allem Innovationsgeist sollte man gesunden Menschenverstand walten lassen und das "Security by Design"-Prinzip beherzigen. Ein gewisser Experimentierrahmen ist grundsätzlich nützlich und wird vom Gesetzgeber explizit gewünscht und bereitgestellt. Gelebte Praxis ist das zum Beispiel in den BMWK-Schaufensterprojekten "Sichere Digitale Identitäten". Technische Innovationen stellen uns oft vor gesellschaftliche und regulatorische Herausforderungen, ein plakatives Beispiel ist autonomes Fahren. Da muss man die Implikationen von Beginn an abwägen, das geht nicht als "Wild-West-Innovation" – jedenfalls nicht hierzulande. Das ist in diesem Fall besonders eingängig, haben wir es doch mit unmittelbaren Auswirkungen im physischen Raum zu tun – Safety-kritisch, nicht "nur" Security. Von Innovationen dieser Kategorie sind in den nächsten Jahren noch viel mehr zu erwarten.

Wie gehe ich es als mittelständisches Unternehmen an, wenn ich Security bei Digitalisierungsprojekten integrieren möchte?
Ja, leider sieht es immer noch so aus, dass man die Wahlfreiheit hat, ob man möchte oder nicht. An dieser Einstellung muss sich grundlegend etwas ändern.

Was ist dabei zu bedenken?
Solche "Digitalisierungsprojekte" sollen im Regelfall bestehende Prozesse durch IT-Unterstützung optimieren und eine beschleunigte Abwicklung ermöglichen. Es ist dann nicht damit getan, einen überfrachteten Prozess einfach in digitale Abläufe zu gießen und irgendwie IT-Sicherheit anzuflanschen. Abläufe überdenken, Ergebnisse bewusst machen, Rollen und Verantwortlichkeiten glattziehen, IT-Ausgestaltung planen. Da muss überall der IT-Sicherheitsgedanke mit drin sein: Welche Daten brauche ich? Kommen Daten aus externen Quellen? Wohin fließen Daten? Wer hat aktuell Zugriff darauf? Wer sollte ihn haben? Welche IT-Systeme aus dem Bestand sind betroffen? Welche relevanten und gegebenenfalls sicherheitsgeprüften Tools haben wir schon im Einsatz? Das hat zig Implikationen für das IT-Sicherheitskonzept, das es hoffentlich schon gibt. Und ganz grundsätzlich gilt für alle Unternehmen, die davon ausgehen, dass sie noch gar nicht digitalisiert sind: Ganz elementar muss die Leitungsebene sich bewusst machen, wie bedeutsam die IT aktuell schon für den Unternehmenserfolg ist. Häufig sind die IT-Abhängigkeiten bereits viel größer als bekannt oder man zu akzeptieren bereit ist. E-Mail geht nicht? Der Betrieb steht. Digitalisierung heißt nicht, dass man den ganzen Betrieb "auf digital" umbaut. Die Digitalisierung ist meist längst da, ob man will bzw. wollte, oder nicht.

Bei allem Innovationsgeist sollte man gesunden Menschenverstand walten lassen und das "Security by Design"-Prinzip beherzigen.

Wo liegen die Herausforderungen? Wie meistere ich diese?
Wenn die Entscheidung für "mehr IT-Sicherheit" getroffen ist, sollte die ansonsten oft als Showstopper geltende Budgetfrage keine Herausforderung mehr sein. Im Umkehrschluss bedeutet dies: IT-Sicherheit kostet Geld und die Mittel müssen bereitstehen.
Es ist zu hoffen, dass die eigene IT-Abteilung oder der IT-Dienstleister des Vertrauens die IT-Security als ein Thema auf ihrer Agenda sehen. Leider ist das oft nicht der Fall. Wenn die Awareness da ist, scheitert es häufig am ⇨

Predelivery Logic: E-Mail-Workflows leicht gemacht

Mit der Predelivery Logic von Retarus lassen sich E-Mails analysieren, optimieren oder umleiten und der Workflow automatisieren – noch bevor die Nachricht die Unternehmensinfrastruktur erreicht. Als Teil der Retarus Secure Email Platform leistet der Service einen entscheidenden Beitrag zur Automatisierung und Beschleunigung von Geschäftsprozessen.

retarus

Unternehmen mit komplexen oder hybriden E-Mail-Infrastrukturen müssen heutzutage eine immer größere Menge an Nachrichten sinnvoll verwalten und absichern. Hier versprechen Cloud-Komplettlösungen für Business-E-Mail einen klaren Wettbewerbsvorteil. So bietet etwa die Retarus Secure Email Platform nicht nur Schutz vor Cyberangriffen, die frühzeitige Erkennung unbekannter Bedrohungen sowie Lösungen für Verschlüsselung und Archivierung, sondern auch innovative Infrastruktur-Services wie die Predelivery Logic. Alle Services sind flexibel, skalierbar und ziehen geringe Kosten sowie keinen Wartungsaufwand nach sich. Bei der Datenverarbeitung setzt Retarus gezielt auf Local Processing. Alle Daten werden DSGVO-konform in selbst betriebenen, auditierbaren Rechenzentren in Deutschland verarbeitet.

Automatisierte Kontrolle des Mailverkehrs

Mit der Predelivery Logic bietet Retarus einen innovativen Werkzeugkasten, mit dem sich der eingehende E-Mail-Verkehr dank individueller Regelwerke einfach verwalten lässt. Flexible Kombinationsmöglichkeiten aus Bedingungen und Aktionen ermöglichen nahezu unbegrenzte Einsatzszenarien. Dabei spielt es keine Rolle, ob das Unternehmen seine E-Mail-Infrastruktur on-premises oder als Cloud Service betreibt. Mit der Predelivery Logic werden E-Mails schon zum Zeitpunkt der Interaktion mit der Retarus Enterprise Cloud, also noch bevor sie an die eigene Infrastruktur zugestellt werden, nach individuellen Regeln analysiert, optimiert und gegebenenfalls umgeleitet.

Individuelle Regelwerke für innovative Vorselektion

Der Funktionsumfang der Retarus Predelivery Logic reicht deutlich über den einer Policy Engine hinaus. Denn neben einem

User-abhängigen Routing unterstützt der Service bei der Automatisierung von Geschäftsprozessen. Da E-Mails basierend auf Inhalt oder Sprache weiterverarbeitet werden können, lassen sich etwa Nachrichten an Funktionspostfächer, die zuständige Landesgesellschaft oder die jeweilige Abteilung automatisch vorsortieren. Es ist auch möglich, E-Mails vollautomatisch und regelabhängig zu bearbeiten – vom Umschreiben der Adresse bis hin zum Hinzufügen eines Schlagworts in der Betreffzeile.

Konsequente Umsetzung von Compliance-Richtlinien

Zudem erlauben es die Regelwerke, E-Mails nach landesspezifischer Herkunft zu identifizieren und automatisch entsprechende Maßnahmen einzuleiten, etwa wenn das Unternehmen aufgrund der aktuellen politischen Lage, aus Sicherheitsgründen oder aufgrund interner Compliance-Vorgaben alle Nachrichten aus bestimmten Regionen vorsorglich isolieren möchte. So lassen sich je nach Konfiguration zum Beispiel E-Mails in die User-Quarantäne leiten. Per Retarus Email Live Search können Administratoren dabei den Weg einer Nachricht durch die gesamte Verarbeitungskette nachvollziehen.

Einheitlicher Auftritt nach außen

Individuelle Regelwerke lassen sich auch für den Outbound-Kanal festlegen. Ob Spin-off, Carve-out, Unternehmenszukäufe, Fusionen oder Rebranding – idealerweise treten Mitarbeiter bereits zum Stichtag mit dem korrekten Firmennamen auf. In solchen Fällen kann die Unternehmensbezeichnung oder -Domain automatisch überprüft und bei Fehlerhaftigkeit umgeschrieben werden.

Umfassender Support

Als zentralen Self-Service stellt Retarus die Predelivery Logic über ein webbasiertes Administrationsportal (EAS) bereit. Alle Regeln lassen sich dort transparent anlegen und verändern. In die eigentliche E-Mail-Infrastruktur des Unternehmens wird dazu nicht eingegriffen. Zudem stehen die Retarus-Experten Kunden bei der Umsetzung individueller Regelwerke für eine effiziente E-Mail- und Workflow-Automatisierung jederzeit beratend zur Seite. So lassen sich Probleme durch Zeitmangel oder noch unklare Organisationsstrukturen vermeiden sowie Maßnahmen mit geringem Aufwand umsetzen. ■

Besuchen Sie Retarus vom 25. bis zum 27. Oktober auf der it-sa in Nürnberg in Halle 7 an Stand 502.

www.retarus.com

fachlichen Knowhow. Denn IT-Security-Experten befassen sich tagtäglich mit der Materie und halten sich auf dem neuesten Stand. Das geht normalerweise nicht neben dem IT-Admin- oder DevOps-Job, zumindest nicht während der regulären Arbeitszeit. Diese Fachexpertise für das Vorhaben verfügbar zu machen, ist eine Herausforderung, meist geht das nur über externe Beratung. Zum Glück kann man sein Projekt mit höchstqualifiziertem Personal aus einer florierenden IT-Sicherheitsbranche adäquat unterstützen und aufwerten. Der Bundesverband IT-Sicherheit zählt aktuell rund 400 Mitglieder. Zusätzlich sind die eigenen Mitarbeiter IT-sicherheitstechnisch zu schulen bzw. explizit zu qualifizieren, damit die IT-Sicherheit nachhaltig als Querschnittsthema im Unternehmen etabliert wird.

Eine grundlegendere Herausforderung ist oft, dass die IT-Organisation an sich in einem desolaten Zustand ist. Das fängt bei der Transparenz an, was überhaupt im Unternehmen an IT im Einsatz ist. Ein entsprechendes Verzeichnis, neudeutsch "IT-Asset Repository", das so automatisch wie möglich aktuell gehalten wird, ist essenziell. Nur dann funktioniert ein Patch- und Schwachstellenmanagement, das als Basis-Security gilt. Wenn mit einem Digitalisierungsvorhaben etwas neu geschaffen werden soll, muss die sichere Integration in die Bestands-IT gewährleistet sein. Idealerweise sind dabei vorhandene IT-Sicherheitsrichtlinien und die Liste gemäß Technology Roadmap zu bevorzugender IT-Produkte zu berücksichtigen. Ganz allgemein gesprochen: Die elementaren IT-Hausaufgaben sind zu erledigen, sonst greifen IT-Sicherheitsbemühungen ins Leere bzw. haben massive Lücken.

Wie sicher ist der deutsche Mittelstand bereits? Wo gibt es Lücken?

Eine pauschale Aussage kann man hier nicht treffen. Bei vielen Mittelständlern haben die dauernden, medienwirksamen IT-Sicherheitsvorfälle auch auf Entscheidungsträgerebene ein starkes Bewusstsein geprägt, welchen Stellenwert IT-Sicherheit hat. Besser noch, die Erkenntnis wurde in Handlungen überführt und es wird in IT-Sicherheit investiert. Der Regelfall dürfte dies allerdings noch nicht sein. Der deutsche Mittelstand ist notorisch unterfinanziert in Sachen IT-Investitionen gemäß der gängigen Devise: "Die IT kostet viel zu viel Geld!" Und diese Aussage bezieht sich nicht nur auf die IT. Ein althergebrachtes (eher anachronistisches) Sprichwort aus der IT-Sicherheitsbranche trägt mehr als ein Körnchen Wahrheit: "Die IT-Sicherheit ist die hässliche kleine Schwester der IT." Wo es bereits an der Bereitschaft mangelt, die simple IT-Ausstattung gesund zu finanzieren, werden die Mehrkosten für ernsthaft sichere IT kaum willig getragen werden. Es bleibt zu hoffen, dass die Sensibilisierung durch alle externen Umstände zu einem Umdenken führt und regulatorische Anforderungen, wie beispielsweise die NIS-Richtlinie, die Hürden für den Betrieb unsicherer IT drastisch erhöhen.

Multicloud-Szenarien machen umfassende Security-Maßnahmen nicht einfacher: Wie können Unternehmen das Komplexitätsrad zurückdrehen und trotzdem innovativ bleiben?

Die Komplexität in der IT zu reduzieren, ist immer eine gute Idee, denn in einfacheren Systemen ist Sicherheit leichter zu bewerkstelligen. Cloud und die Multicloud sind oft komplexitätstreibend, aber sie gehen werden uns erhalten bleiben. Jeder IT-Entscheidungsträger muss sich bewusst machen, was eine – gegebenenfalls sogar extensive – Cloud-Nutzung für sein Unternehmen bedeutet. Die Vorteile bezüglich Flexibilität und Geschwindigkeit sind einerseits immens. Die kritischen Verfügbarkeitsabhängigkeiten und in anderen Jurisdiktionen gesetzlich angeordneten Dateneinsichtsrechte

für Geheimdienste wiegen andererseits schwer. Größte deutsche Unternehmen haben dies akzeptiert und bereits vor Jahren eine "Cloud first"-Strategie ausgelobt und umgesetzt. Der Mittelstand ist da deutlich verhaltener, vielfach auch sehr Cloud-kritisch eingestellt. Doch die Cloud wird auch im Mittelstand ankommen, und zukünftig wird sich dieser damit auch leichter tun. Aktuell sind in Deutschland und Europa starke Bestrebungen im Gange, europäische Cloud-Alternativen zu schaffen, die echte Datensouveränität ermöglichen. Die bekannteste Initiative ist Gaia-X, an der sich auch bekannte deutsche IT-Serviceprovider, Webhoster und Rechenzentrumsbetreiber beteiligen. Letztere sind in ihren Cloud-Angeboten immer besser geworden und bieten für viele Anwendungsbereiche sehr gut gangbare Wege. Weniger bekannt in der Öffentlichkeit sind bisher die „Important Projects of Common European Interest“ (IPCEI) der Europäischen Kommission. Mit dem IPCEI-CIS, wobei der Annex für "Cloud Infrastructure and Services" steht, wird angestrebt, die Cloud der Zukunft zu schaffen. Diese soll den bekannten Plattformen aus West und Ost Paroli bieten können und insbesondere europäischen Organisationen eine sichere und vertrauensvolle Cloud-Nutzung ermöglichen.

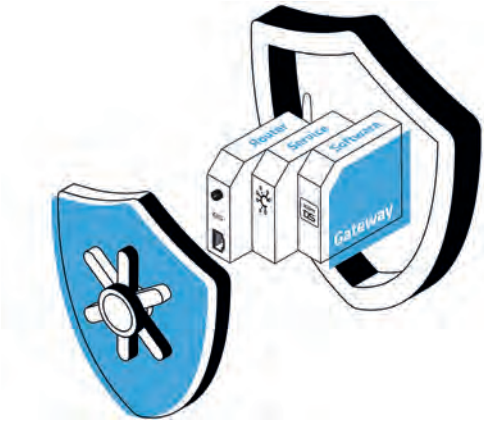
Welche neuen Herausforderungen stellen sich für Unternehmen angesichts vermehrter Cyberangriffe und geopolitischer Veränderungen?

Die multiplen Krisen mit globalen Auswirkungen liefern externe Faktoren, die für jedes Unternehmen entscheidungsrelevant geworden sind. Vertrauen und Stabilität sind schlagartig viel wichtiger geworden, denn vieles, auf das sich bisher alle blind verlassen haben, ist nun infrage gestellt. Bekomme ich die gewohnten (IT-)Produkte in akzeptablen Zeiträumen und zu vertretbaren Konditionen? Wie stabil ist unsere Versorgung mit bezahlbarer Energie? Werde ich für meine Produkte und/oder Dienstleistungen noch Abnehmer haben? Ist meine IT gegen Angriffe von staatlich gestützten Angreifern ausreichend geschützt? Besonders bei der letzten Frage wird sich kaum ein Unternehmen zu einem beherzten "Ja!" hinreißen lassen. Vielmehr bleibt ein mulmiges Gefühl, dass alles schon viel zu sehr abhängig von der IT ist. Deren Sicherheitszustand ist selbst von Experten nur mit größeren Anstrengungen zu bewerten, schon gar nicht von den Security-Laien in den IT-Abteilungen. Eine belastbar sichere IT verursacht hohe Aufwände, sie erfordert moderne Technik und hochqualifiziertes Personal. Es wäre besser, wenn deutsche Unternehmen hier aus dem Vollen schöpfen könnten und in den letzten Jahrzehnten schon sicher und nachhaltig digitalisiert hätten. Dies nicht zu tun, ist nun definitiv keine Option mehr. Gefordert sind effiziente Lösungen, die in den Unternehmen schnell Wirkung entfalten.

Ein von Staat und Wirtschaft gemeinsam organisiertes und betriebenes Security Operations Center sollte allen Organisationen, die IT betreiben, zur Verfügung stehen.

Die IT-Sicherheitsbranche steht bereit. Ein von Staat und Wirtschaft gemeinsam organisiertes und betriebenes Security Operations Center (SOC) sollte allen Organisationen, die IT betreiben, zur Verfügung stehen. Vergleichbar mit der Flugsicherung, ohne die ist die Luftfahrt ja auch nicht denkbar. Alle sind aufgerufen, die IT-Sicherheit als den Erfolgsfaktor zu erkennen, der er ist. □

30 Jahre IT & OT Expertise „Made in Germany“



INSYS icom ist Digitalisierungsexperte für industrielle Datenkommunikation. Mit unseren Lösungen bilden wir die Brücke zwischen IT und OT. Sie sind somit häufig das zentrale Gateway in der Kommunikation von geschlossenen und sicheren Netzwerken nach außen in das freie Internet. Daher hat die Sicherheit unserer Lösungen die oberste Priorität.

Die aktuell rasant steigenden Energiepreise halten die Industrie dazu an, sich noch stärker auf einen wirtschaftlichen Betrieb zu fokussieren. Das Aufrechthalten der Energiewirtschaft und Produktionsketten darf an modernen Fernwartungslösungen nicht scheitern, weshalb die Bundesregierung mit dem IT-Sicherheitsgesetz 2.0 weitere Maßnahmen zur Stärkung der Cybersicherheit in Deutschland fordert. Im Mittelpunkt: die sichere Vernetzung von IT und OT in kritischen Infrastrukturen (KRITIS).

Viele Bestandskunden von Systemhäusern fallen in die neu vorgeschriebene Sicherheitsgesetzkategorie und genau das eröffnet, über das Kerngeschäft IT-Dienstleistungen hinaus, Chancen für neue Lösungen und Servicepakete.

INSYS icom wird als bewährter Industrie-Router-Hersteller, oft als Teil von Modernisierungs- und Fernwartungsprojekten, in KRITIS-Bereichen eingesetzt. Seit 30 Jahren ist das Regensburger Unternehmen in den Applikationsbereichen Fernwartung, Fernsteuerung, Überwachung von Zuständen und Vernetzung von Daten unterwegs. Industrietaugliche „Made in Germany“-Lösungen, zu denen zuverlässige Router, Software-Applikationen und Fernwartungs-Services gehören, bieten maximale Sicherheit und Flexibilität. Lösungen für Anforderungen in Bezug auf Langlebigkeit, Performance und IT-Sicherheit werden aus einer Hand geboten.

INSYS icom Router sind ausgestattet mit dem auf Linux entwickelten, gehärteten Betriebssystem icom OS.

Ergänzende Lösungen, wie der Fernwartungsdienst „icom Connectivity Suite – VPN“, ermöglichen die kontinuierliche Steuerung und Datenerfassung von Geräten. Der Betrieb in ISO27001-zertifizierten Data Centern und die einfache Bedienbarkeit sorgen für bestmögliche Sicherheit auch für „Nicht IT-Profis“.

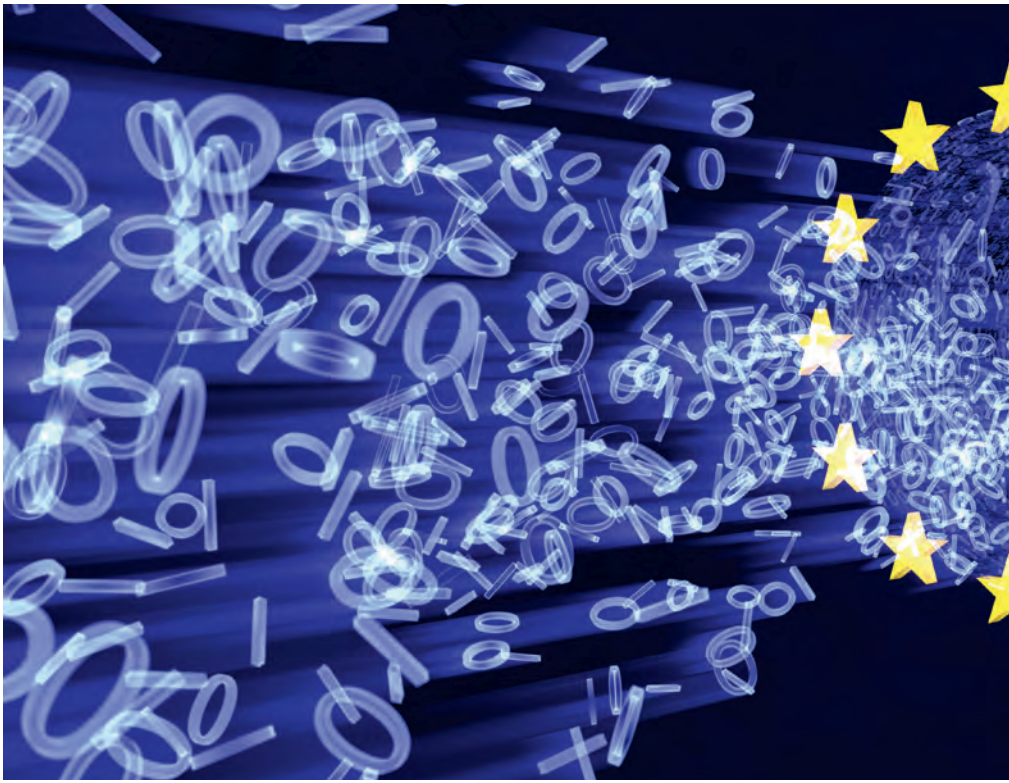
Mit dem Anspruch, „Immer eine Spur voraus“ zu sein, setzt INSYS icom kontinuierlich neue Technologiestandards. Ein respektvoller, partnerschaftlicher und verantwortungsbewusster Umgang mit Kunden, Partnern und Lieferanten ist für uns dabei nicht nur unabdingbar, sondern auch unser Erfolgsrezept – ebenso wie der gegenseitige Wissensaustausch.

Fernwartung und Remote Access in Betrieben können mit den Industrie-Routern von INSYS icom sicher durchgeführt werden. Die Produkte erfüllen alle Anforderungen des IT-Sicherheitsgesetztes 2.0, erprobt im Einsatz bei zahlreichen Kunden aus den kritischen Infrastrukturen – komplett in Deutschland entwickelt und in Europa produziert. Somit sind Sie bestens gerüstet für die steigenden Anforderungen an die IT-Sicherheit. ■

Security als Fundament der digitalen Souveränität

Die von der EU gewünschte digitale Souveränität ist mehr als Datenhoheit, man muss auch technologisch souverän sein. Das gilt besonders im Bereich der Cybersicherheit. So kann es ohne eine unabhängige Security keine zuverlässige Kontrolle über die eigenen Daten geben. Erst die Datensicherheit ermöglicht die Datenhoheit. Doch wie steht es um die Souveränität der Security in der EU?

Von Dipl.-Phys. Oliver Schonschek



Die Konferenz „Aufbau der digitalen Souveränität Europas“ unter der Französischen Präsidentschaft im Rat der Europäischen Union hatte die Bestandsaufnahme der in den letzten Jahren erzielten Fortschritte zum Ziel und sollte einen Denkanstoß sowie Impulse für den weiteren Aufbau der digitalen Souveränität Europas geben. Im Mittelpunkt der Konferenz stand die Fähigkeit der Europäischen Union, ihre Zukunft im digitalen Zeitalter souverän zu gestalten, insbesondere ihre wirtschaftlichen Interessen und Werte zu verteidigen und ihre Autonomie zu sichern.

Die Stärkung der digitalen Souveränität und der Datenhoheit von Unternehmen sind zentral für die Innovations- und Wettbewerbsfähigkeit der Wirtschaft. Dies bestätigt auch die Studie „Digitale Souveränität“, die das ZEW Mannheim im Auftrag des Bundesministeriums für Wirtschaft und Energie erstellt hat. Der Verbesserung der digitalen Souveränität für die deutsche Wirtschaft messen rund 70 Prozent der befragten Unternehmen aus dem Verarbeitenden Gewerbe und der Informationswirtschaft langfristig eine große Bedeutung bei. Für eine höhere digitale Souveränität erachten die Unternehmen die Datenhoheit als zentral: 90 Prozent der Unternehmen aus der Informationswirtschaft und 84 Prozent der Unternehmen im Verarbeitenden Gewerbe gaben an, dass sie für das eigene Unternehmen eine besondere Bedeutung hat.

Bild: mixmagic/stock.adobe.com

Die Säulen der digitalen Souveränität

Um zu bewerten, wie es um die digitale Souveränität in der EU steht, müssen die Elemente, die zu der Souveränität beitragen, betrachtet werden. So basiert digitale Souveränität auf Datensouveränität und technologischer Souveränität.

Datensouverän zu sein ist die Fähigkeit, informiert und selbstbestimmt zu entscheiden, wie und von wem Informationen über die eigene Person oder Institution, eigene Handlungen oder Produkte erhoben, verarbeitet und weitergegeben werden.

Technologische Souveränität beschreibt den Anspruch und die Fähigkeit, Schlüsseltechnologien international auf Augenhöhe mitzugestalten, so das BMBF (Bundesministerium für Bildung und Forschung). Sie ist die Voraussetzung, um in einem härter werdenden internationalen Technologiewettbewerb nicht in Abhängigkeiten zu geraten und damit wirtschaftliche und politische Gestaltungsfähigkeit zu verlieren. Dies kann auch erfordern, Lösungen und Produkte in strategisch relevanten Feldern in Europa selbst zu entwickeln und zu produzieren, ⇨

Wenn die Kür zur Pflicht wird – Angriffserkennung für KRITIS-Unternehmen

Mit der Verabschiedung des IT-Sicherheitsgesetzes 2.0 müssen alle KRITIS-Betreiber ab dem 1. Mai 2023 nach § 8a Absatz 1a Systeme zur Angriffserkennung einsetzen – ohne Ausnahme.

Von Alexander Maringer, Senior Security Consultant bei TÜV Rheinland

150 Jahre

TÜVRheinland®
Genau. Richtig.

Mit einer Angriffserkennung können Cyber-Attacken frühzeitig erkannt und potenzielle Schäden reduziert werden. Wichtig: Die zu verwendenden Systeme müssen kontinuierlich die notwendigen Informationen erfassen und automatisch auswerten. Ferner sollen sie Störungen vermeiden bzw. auf Störungen aktiv reagieren. Folglich müssen die Systeme sowohl detektieren als auch reagieren können.

Die Angriffserkennung sollte auf einem mehrschichtigen Ansatz basieren – ein zentrales Element ist die Analyse der Log-Daten. Diese Aufgabe kann von einem SIEM („Security Information and Event Management“) on-premise oder „as-a-service“ übernommen werden. Hier stellt sich die Frage, ob ein einziges System für IT und OT verwendet wird, oder ob man sich aufgrund der unterschiedlichen Anforderungen der beiden „Welten“ für zwei spezialisierte Systeme entscheidet. Die kontinuierliche Anpassung der Erkennungsmechanismen zur Vermeidung von False-Positives ist bedeutend für die Effektivität eines solchen Systems.

Je nach Unternehmensgröße kann ein „Security Operations Center“ (SOC) im Eigenbetrieb oder „as-a-service“ (SOCaaS – insbesondere für kleinere Unternehmen) notwendig werden, um die Anforderung der Reaktion auf Störungen umzusetzen. Durch

die Beauftragung eines outgesourcten SIEMs (inkl. Logserver) werden die Anforderungen der Funktionstrennung und manipulationssicheren Protokollierung erfüllt, da die Systeme außerhalb des eigenen Zugriffs sind. Ferner wird bei einem SOCaaS weniger Expertise und kein 24/7-Schichtbetrieb im eigenen Haus benötigt.
Wir unterstützen Sie in allen oben genannten Fragestellungen und begleiten Sie auch gerne bei der Lösungsimplementierung. ■

Interview mit Anja Daniela Favuzzi, Head of Sales bei der TÜV Rheinland i-sec GmbH.

1. Cybersecurity und TÜV Rheinland – wie passt das zusammen?

Seit 150 Jahren steht TÜV Rheinland für mehr Sicherheit und Qualität im Zusammenspiel von Mensch, Technik und Umwelt. In einer zunehmend digitalen Welt bedeutet das zwingend, das Thema Cybersecurity immer mitzudenken. Und tatsächlich nimmt die Betrachtung von Cybersicherheitsaspekten auch im klassischen Prüfgeschäft von TÜV Rheinland stetig zu.

2. Mit welchen Herausforderungen kommen Ihre Kund*innen auf Sie zu?

Unternehmen, die der sogenannten „kritischen Infrastruktur“ zugerechnet werden, sind mit regulatorischen Anforderungen der KRITIS-Verordnung konfrontiert. Die Erfüllung dieser Anforderungen und der Schutz vor Ransomware-Angriffen sind aktuell die beiden größten Herausforderungen für unsere Kund*innen. Parallel macht vielen Kund*innen der sich verschärfende Mangel an Fachkräften in der Cybersecurity und der daraus resultierende Bedarf an externer Unterstützung zu schaffen.

3. Welche Lösungsansätze bieten Sie hier an?

Wir unterstützen unsere Kund*innen bei einer umfassenden Cybersecurity-Strategie und erarbeiten einen konkreten Fahrplan hin zu einem „cyber-resilienten“ Unternehmen. Dabei werden vorgegebene Budgets und alle aktuellen Security-Maßnahmen berücksichtigt. Wir führen Penetrationstests, Phishing- und Red-Teaming-Kampagnen durch und simulieren Hackerangriffe auf das Unternehmen. Dabei betrachten wir neben der IT (Information Technology) auch die OT (Operational Technology) von Industrieunternehmen.

4. Wie richtet sich der TÜV Rheinland künftig zum Thema Cybersecurity aus?

Große Dynamik sehen wir in der industriellen Automatisierung und Steuerung durch den Einsatz von 5G Edge Computing und KI-gesteuerten Systemen sowie in dem zunehmenden Shift der Infrastrukturen und Systeme in die Cloud. Gerade im Hinblick auf hybride Infrastrukturen sind gut durchdachte Securitylösungen unverzichtbar. Wir liefern mehr Sicherheit und Qualität im Zusammenspiel von Mensch, Technik und Umwelt. ■

www.tuv.com/cybersecurity

etwa, wenn sie auf dem globalen Markt nicht mit den aus europäischer Sicht notwendigen Eigenschaften und Fähigkeiten verfügbar sind.

Die Konferenz „Aufbau der digitalen Souveränität Europas" sah als eine zentrale Säule für die digitale Souveränität die „Europäische Union als schützende Macht": Die EU muss die Sicherheit von Bürgerinnen und Bürgern, öffentlichen Diensten und Unternehmen im Cyberspace stärken und eine industrielle Datenstrategie entwickeln, die gegen extraterritoriale Gesetze resistent ist.

Aber auch aus einem anderen Grund ist die technologische Souveränität der Cybersicherheit elementar für die digitale Souveränität. Erst mit einer zuverlässigen Datensicherheit kann Datenkontrolle und Datensouveränität überhaupt gelingen. Nur wer zum Beispiel Daten sicher verschlüsseln kann, hat die Kontrolle darüber, wer auf die Daten zugreifen kann und wer nicht.

Die Souveränität der Cybersicherheit

Gerade im Bereich der Cybersicherheit ist die technologische Souveränität somit von entscheidender Bedeutung. Mit der Digitalisierung von Wirtschaft und Gesellschaft wachsen zugleich deren Verwundbarkeit und das Missbrauchspotenzial im digitalen Raum, so das BMWi (Bundeswirtschaftsministerium). Cybersicherheit und IT-Sicherheitstechnologien, mit denen sich Cyberangriffe abwehren lassen, stellen demnach einen zentralen Aspekt der Digitalen Souveränität eines Staates und eines Unternehmens dar.

Auf dem Weg zu einem digitalen Europa: Das Ziel der digitalen Souveränität erfordert eine unabhängige Cybersicherheit.

Digitale Souveränität hat für die Cyber- und Informationssicherheit eine wesentliche Bedeutung, so die Bundesregierung mit Blick auf die Cybersicherheitsstrategie 2021. Sichere Technologien und Lösungen sowie entsprechende Fähigkeiten, die Chancen und potenziellen Risiken digitaler Technologien erkennen und bewerten zu können, seien wesentliche Voraussetzungen für die digitale Souveränität. Ein hohes Cybersicherheitsniveau trage so zur Stärkung der digitalen Souveränität von Bürgerinnen und Bürgern, Wirtschaft, Wissenschaft und Staat bei. Auf europäischer Ebene bedeute digitale Souveränität eine stärkere wirtschaftliche und sicherheitspolitische Vernetzung mit strategisch wichtigen Partnern, um Abhängigkeiten zu mindern und die politische Handlungs- beziehungsweise Gestaltungsfähigkeit zu bewahren.

Die Bundesregierung will mit mehreren Bausteinen eine Souveränität in der Cybersicherheit erreichen. Dazu gehören die anwendungsorientierte Forschung und Entwicklung sowie der Forschungstransfer, die Cybersicherheit als Qualitätsmerkmal „Made in Germany", die staatlichen Fähigkeiten zur Beurteilung neuer Technologien, die Beauftragung europäischer Anbieter, die Eigensicherung der Verwaltung sowie eine gemeinsame Vision und Strategie der EU für Cybersicherheit und europäische digitale Souveränität.


Bild: TeleTrusT

„Technologische Souveränität im Bereich IT-Sicherheit schaffen – für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft", so eine TeleTrusT-Forderung in der „IT-Sicherheitsagenda 2029". Im Bild: TeleTrusT-Vorstandsvorsitzender Prof. Dr. Norbert Pohlmann.

Forderungen aus der Security-Branche

Noch ist das Ziel einer souveränen Cybersicherheit aber nicht erreicht. Deutschland und Europa müssen angemessen und souverän die digitale Zukunft gestalten können, so der Bundesverband IT-Sicherheit e.V. (TeleTrusT). Für die nächsten beiden Legislaturperioden des Deutschen Bundestages hatte TeleTrusT eine IT-Sicherheitsagenda 2029 aufgestellt.

Darin finden sich Forderungen wie „Technologische Souveränität im Bereich IT-Sicherheit schaffen – für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft" und „Mehr IT-Sicherheitstechnologie ‚Made in Germany' in der Praxis", aber auch „Verbot der Kompromittierung von IT-Sicherheit, keine Backdoors, Staatstrojaner oder geschwächte Verschlüsselung".

Rechtsanwalt Karsten U. Bartels LL.M., stellvertretender TeleTrusT-Vorstandsvorsitzender, erklärte dazu: „Wenn wir eine technologische und digitale Souveränität Deutschlands und Europas wollen, muss die Politik in den nächsten zwei Legislaturperioden die IT-Sicherheit massiv stärken."

Dies betont auch der Digitalverband Bitkom: Sowohl national als auch auf EU-Ebene werde viel in Cybersecurity-Forschung investiert. Dies allein sei jedoch nicht ausreichend, um dem Ziel digitaler Souveränität näher zu kommen: Hierfür brauche es neben einheitlichen rechtlichen Rahmenbedingungen in der EU auch einen berechenbaren Nachfragemarkt. Dieser sei Grundvoraussetzung dafür, dass die staatlichen Forschungsausgaben tatsächlich zu zielgerichteten Investitionen der Industrie und damit einer Stärkung der digitalen Souveränität Deutschlands und Europas führten.

Wer also digitale Souveränität und Datenhoheit in der EU erreichen will, muss auch die betreffende Cybersicherheitsbranche in Deutschland und in der EU stärken. Dies findet sich auch in der Cybersicherheitsstrategie 2021, sie besagt: Durch die Förderung deutscher und europäischer Anbieter sowie die Weiterentwicklung eigener Kompetenzen in der Erforschung neuer Cybersicherheitsrisiken wird das souveräne Handeln Deutschlands im Cyberraum sichergestellt.

Cybersicherheit ist somit ein Fundament der digitalen Souveränität, die sich ohne eine souveräne Security nicht erreichen lässt. Noch sind die Arbeiten am Fundament aber nicht abgeschlossen, das sollte man im Hinterkopf behalten, wenn man das Gebäude der digitalen Souveränität plant. □

„Sicherer VS-Arbeitsplatz“: Mobil und hochsicher mit Verschlusssachen arbeiten

Nicht zuletzt durch die Umsetzung des Onlinezugangsgesetzes (OZG) werden in Behörden immer mehr Prozesse und Abläufe ins Digitale verlegt. Dabei müssen jedoch höchste Sicherheitsanforderungen beachtet werden, insbesondere wenn klassifizierte Dokumente und Informationen bearbeitet werden. Der IT-Sicherheitsexperte Rohde & Schwarz Cybersecurity ermöglicht mit R&S®Trusted Endpoint Suite öffentlichen Institutionen und geheimschutzbetreuten Unternehmen, Arbeitsplätze so abzusichern, dass VS-NfD-eingestufte Informationen einfach gespeichert und bearbeitet werden können. Die innovative Sicherheitslösung erhielt dafür vom Bundesamt für Sicherheit in der Informationstechnik (BSI) die VS-NfD-Zulassung als „Sicherer VS-Arbeitsplatz“.

ROHDE&SCHWARZ

Der sichere VS-NfD-Arbeitsplatz überzeugt auch mit Flexibilität bei der Hardware: Benutzer können bereits vorhandene Endgeräte nutzen und es muss gemeinhin keine zusätzliche Hardware angeschafft werden. Darüber hinaus ermöglicht das zentrale und intuitive Managementsystem eine leichte Administration. Nicht zuletzt, da für alle Komponenten der Plattform nur eine Smartcard benötigt wird. Das verringert den Administrationsaufwand und bietet höchste Sicherheit bei gleichbleibender Produktivität.

Zwei Komponenten für umfassenden Schutz

Der VS-NfD-Arbeitsplatz auf Basis von R&S®Trusted Endpoint Suite besteht aus zwei Komponenten auf einer vereinheitlichten Softwarearchitektur: R&S®Trusted VPN Client und R&S®Trusted Disk. R&S®Trusted VPN Client schützt die Netzwerkkommunikation einer Client-Plattform (Windows-Laptop, -Tablet) mit einem Behörden- oder Unternehmensnetzwerk über ein nicht vertrauenswürdiges Netzwerk wie zum Beispiel

dem Internet. Für zusätzliche Sicherheit sorgt der „Always On"-Modus. Nutzer befinden sich so zu keinem Zeitpunkt ungeschützt in einem nicht vertrauenswürdigen Netzwerk – egal ob im Büro oder auf Dienstreise im Hotel, Zug oder Flugzeug. R&S®Trusted VPN Client setzt eine Zero-Trust-to-OS-basierte VPN-Lösung um, bei der kein Vertrauen in potenziell unsichere Komponenten wie einem Betriebssystem bestehen muss. Die sogenannte Rot-Schwarz-Trennung (Netzwerktrennung zwischen roten Verschlusssache-Daten und dem schwarzen Internetverkehr) findet außerhalb des Betriebssystems statt, sodass selbst bei Schwachstellen und Sicherheitslücken im Betriebssystem ein Abfluss von eingestuften Daten verhindert werden kann. Mit einem umfassenden Schnittstellenmanagement kann komfortabel und zentral gesteuert werden, welche USB-Geräte Mitarbeitende anschließen dürfen – auch ein vollständig restriktiver Modus (Default Block) ist möglich.

Die Festplattenverschlüsselung R&S®Trusted Disk schützt sensible Daten mit einer sicheren und transparenten Verschlüsselung in Echtzeit ohne Produktivitätseinschränkung sogar im Falle von Verlust oder Diebstahl vor unbefugtem Zugriff. Neben den Daten verschlüsselt R&S®Trusted Disk auch das komplette Betriebssystem und die temporären Daten. Selbst der Zugriff auf mobile Datenträger wie USB-Sticks oder externe Festplatten kann geschützt werden. Die moderne Zufallszahlgenerierung ebenso wie eine flexible Umschlüsselung nach Zeit und Datenmenge garantieren die stetige Aufrechterhaltung des hohen Sicherheitsniveaus.

Optional mit zusätzlichen Schutzfunktionen

Für zusätzlichen Schutz des VS-NfD-Arbeitsplatzes sorgt die virtuelle Umgebung zum sicheren Surfen im Web, R&S®Browser in the Box, der die Sicherheitslücke „Internet" schließt, indem er eine digitale Quarantäne für Angriffe ermöglicht: Schadsoftware wird isoliert, bevor sie überhaupt zur Ausführung kommt. Dieser Mechanismus schützt auch vor Angriffen via E-Mail-Anhängen oder Webkonferenzen mit Mikrofonnutzung und Webcam-Unterstützung. R&S®Browser in the Box wurde im Juli 2022 bei den Network Computing Awards zum „Softwareprodukt des Jahres" sowie zum „Produkt des Jahres" gekürt.

Für eine VS-NfD-konforme E-Mail- und Datenverschlüsselung kann R&S®Trusted Endpoint Suite außerdem um GnuPG VS-Desktop® erweitert werden. ■

Cyberresilienz in der EU

Die Forderung nach Cyberresilienz ist nicht neu, aber sie erscheint wichtiger denn je. Die Abhängigkeit von digitalen Diensten steigt, die Bedrohungslage verschärft sich nicht nur im Internet. Regierungen sind ebenso gefordert wie die Wirtschaft.

Von Dipl.-Phys. Oliver Schonschek

Bild: S.Gvozd/stock.adobe.com

Die laufende Diskussion und die umfassende Betrachtung zur Cyberresilienz in Europa sind wichtig und notwendig, aber die Zeit drängt.

Vor dem Hintergrund des russischen Angriffskrieges auf die Ukraine will die Bundesinnenministerin Nancy Faeser Deutschlands Cyberfähigkeiten ausbauen: „Wir sehen angesichts des russischen Angriffskriegs gegen die Ukraine, wie sehr die äußere und die innere Sicherheit miteinander zusammenhängen. Das gilt gerade für die Cybersicherheit." Faeser macht deutlich: „Die Zeitenwende, die wir erleben, erfordert deutliche Investitionen in unsere Cyber- und Informationssicherheit. Das hat besondere Priorität für uns. Wir modernisieren die nationale Cybersicherheitsarchitektur und bauen das Bundesamt für Informationssicherheit zur Zentralstelle aus. Die Cyberbefugnisse der Sicherheitsbehörden werden wir weiterentwickeln."

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ruft Unternehmen, Organisationen und Behörden dazu auf, ihre IT-Sicherheitsmaßnahmen zu erhöhen. Das BSI hat seinen Eigenschutz und seine Krisenreaktion gestärkt und hat dazu das Nationale IT-Krisenreaktionszentrum aktiviert. Darüber hinaus hat das BSI auch seine Zielgruppen, darunter die Bundesverwaltung, Betreiber Kritischer Infrastrukturen und weitere Organisationen und Unternehmen sensibilisiert und zu einer erhöhten Wachsamkeit und Reaktionsbereitschaft aufgerufen.

Alle diese Maßnahmen bedeuten letztlich, dass es nun darum geht, die Cyberresilienz herzustellen. Das BSI definiert Resilienz als die Fähigkeit eines Systems, mit Veränderungen umgehen zu können. Resilienz bedeutet demnach Widerstandsfähigkeit gegen Störungen jeder Art, Anpassungsfähigkeit an neue Bedingungen und eine flexible Reaktion auf Veränderungen mit dem Ziel, das System aufrechtzuerhalten.

Das Ziel lautet deshalb, nicht nur die Cybersicherheit Deutschlands und der EU insgesamt zu stärken, sondern in Zukunft eine Cyberresilienz zu erreichen und aufrechtzuerhalten. Die Cyberresilienz würde dann automatisch dazu führen, dass zum Beispiel die Cybersicherheit gestärkt wird.

Quelle: Peter Jülich

Bundesinnenministerin Nancy Faeser: „Die Zeitenwende, die wir erleben, erfordert deutliche Investitionen in unsere Cyber- und Informationssicherheit."

Der Weg zur Cyberresilienz in der EU

„Um unsere Resilienz zu erhöhen, müssen wir gemeinsame europäische Cybersicherheitsstandards für Produkte (insbesondere vernetzte Objekte) und Dienstleistungen etablieren, die auf unserem Markt platziert werden", erklärte Thierry Breton, EU-Kommissar für den Binnenmarkt, bereits im September 2021. „Dies wird der Zweck des angekündigten European Cyber Resilience Act sein. Ich bin der Meinung, dass dieses Gesetz auch eine verteidigungspolitische Dimension haben sollte, um Synergien zu maximieren, indem beispielsweise ⇨

Die Vorteile für Systemhäuser in der Zusammenarbeit mit ITSMIG-Unternehmen

In einer immer komplexer werdenden IT-Landschaft mit globalen Lieferketten und einer unüberschaubaren Anzahl an Zulieferern für IT-Produkte stellt sich zurecht die Frage, wie sich die Sicherheit der einzelnen Komponenten und deren Prozesse in der gesamten Wertschöpfungskette sicherstellen lassen.

Von Tobias Eder und Niels Lerch, INFODAS GmbH

Längst sind digitale Dienste und zugehörige Infrastrukturen elementare Grundlagen unseres Lebens und der Funktionsfähigkeit unserer Gesellschaft und des Staates geworden. Die DIGITALE NACHHALTIGKEIT bietet hier die Antwort, indem sie beschreibt, wie eine solide, sichere und interoperable digitale Infrastruktur erreicht werden kann, um damit verbindliche und beständige Grundlagen für künftige Generationen zu schaffen.

TeleTrusT setzt mit dem Vertrauenszeichen „IT Security made in Germany“ (ITSMIG) an dieser Stelle an und hat einen Standard geschaffen, der Unternehmen mit Sicherheitsbewusstsein einen Orientierungspunkt für vertrauenswürdige IT gibt.

Nicht nur müssen die mit dem ITSMIG ausgezeichneten Unternehmen den Unternehmenshauptsitz in Deutschland haben, ebenso muss die IT-Sicherheitsforschung und -entwicklung des Unternehmens in Deutschland stattfinden. Besonders hervorzuheben ist dabei, dass das Unternehmen vertrauenswürdige IT-Sicherheitslösungen anbietet, welche keine versteckten Zugänge enthalten dürfen.

Wie stark der Fokus auf **Vertrauenswürdigkeit** liegt, wird noch einmal dadurch betont, wenn man bedenkt, dass der aktuell gültige Koalitionsvertrag vorsieht, nur noch **vertrauenswürdige** Unternehmen beim Ausbau kritischer Infrastrukturen zu beteiligen. Gleiches gilt auch für den **vertrauenswürdigen** Aufbau der digitalen Verwaltung. Auch in Zukunft möchte man ein tiefgreifendes Sicherheitsbewusstsein durch die Verwendung von **vertrauenswürdigen** IT-Sicherheitslösungen fördern.

Mit Hinblick auf die DIGITALE NACHHALTIGKEIT bedeutet dies, die Berücksichtigung der Vertrauenswürdigkeit, sichere

Ihre Sicherheit ist unser Auftrag.

infodas auf einen Blick.

Unabhängiges Familien-Unternehmen gegründet 1974 in Köln

Branchenfokus auf Cybersicherheit im Öffentlichen Sektor und Kritischen Infrastrukturen

Niederlassungen in Köln, Berlin, Bonn, München, Hamburg

Hochsicherheits-Produkte & Consulting

Lieferketten, Security-by-Design sowie Digitale Souveränität. Grundsätzlich lässt sich **Vertrauenswürdigkeit** in der IT an drei Kernaspekten ablesen.

1) Am Produkt: Es macht genau das, was es soll und nicht mehr. Nachgewiesen durch umfassende (BSI-) Zulassungen oder (Common Criteria-) Zertifizierungen sowie mittels umfangreicher technischer Prüfungen, gemäß allgemein anerkannter Sicherheitskriterien.

2) Anhand ihrer Lieferketten: Es wird nur das verbaut, was verbaut sein muss und nicht mehr. Sichere, zuverlässige Lieferketten sind unerlässliche Schlüsselfähigkeiten, um vertrauenswürdige IT herzustellen und über den Lebenszyklus hinweg aufrechterhalten zu können.

3) In der Vertrauenswürdigkeit des Unternehmens selbst: Das Unternehmen hat sich ausreichend Vertrauen erarbeitet, ggf. durch Erfüllung von ISO-Standards, BSI-Zertifizierungen oder als geheimschutzbetreutes Unternehmen.

Hierfür gilt es, ein übergreifendes Ökosystem aufzubauen, welches erlaubt, dass Hersteller, Dienstleister und Nutzer **vertrauenswürdige** IT-Systeme effizient und sicher produzieren sowie einsetzen können.

Bei der Nutzung eines ITSMIG-Unternehmens kann das sicherheitsbewusste Systemhaus einen ersten Ansatz dieser beschriebenen Nachhaltigkeit sicherstellen und so zumindest auf mittelfristige Sicht auch günstiger wirtschaften. Zusammen mit einem Management des Restrisikos hätten so aufgebaute, vertrauenswürdige IT-Systeme ein belegbar geringes und beherrschbares Risiko über den gesamten Lebenszyklus hinweg.

Die INFODAS GmbH ist langjähriger Träger des Zeichens „IT Security made in Germany“, weist sich gerade an ihrem hohen Grad der Vertrauenswürdigkeit im Sinne der DIGITALEN NACHHALTIGKEIT aus und verbunden mit ihrer umfangreichen Kompetenz mit Hochsicherheitsanwendungen zeigt sie sich als bevorzugter Partner von Systemhäusern und KRITIS-Unternehmen. ■

verteidigungsbezogene Anforderungen berücksichtigt werden können."

Der Appell des EU-Kommissars Breton gilt heute noch mehr denn je: „Angesichts von Cyberbedrohungen kann die Europäische Union keine Kompromisse eingehen und muss gemeinsam mit ihren Mitgliedstaaten alles tun, um unsere Widerstandsfähigkeit zu erhöhen. Um unsere Industrie, unsere öffentlichen Dienste, unsere Infrastrukturen, unsere Sicherheit und Verteidigung zu erhalten."

Im März 2022 hat die EU-Kommission eine öffentliche Konsultation eingeleitet, um die Ansichten und Erfahrungen aller relevanten Parteien zum bevorstehenden europäischen Rechtsakt zur Cyberresilienz einzuholen. Die öffentliche Konsultation sollte bis zum 25. Mai 2022 laufen. Die Ergebnisse werden in den Gesetzgebungsvorschlag der EU-Kommission einfließen, der in der zweiten Hälfte dieses Jahres erwartet wird.

Quelle: EC - Audiovisual Service

Thierry Breton, EU-Kommissar für den Binnenmarkt: „Angesichts von Cyberbedrohungen kann die Europäische Union keine Kompromisse eingehen und muss gemeinsam mit ihren Mitgliedstaaten alles tun, um unsere Widerstandsfähigkeit zu erhöhen."

Das Gesetz zur Cyberresilienz soll dann den bestehenden EU-Rechtsrahmen ergänzen, der die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) und das Gesetz zur Cybersicherheit sowie die künftige Richtlinie über Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit in der gesamten Union umfasst (NIS 2).

Konkrete Vorschläge und Forderungen für die Cyberresilienz

Verbände und Branchenvertreter haben sich bereits zu den in ihren Augen notwendigen Maßnahmen in der aktuellen Lage geäußert. Angesichts der veränderten geopolitischen Situation infolge des Ukraine-Konfliktes fordert zum Beispiel der Bundesverband IT-Sicherheit e.V. (TeleTrust) von Politik, Regulierern und Betreibern weitreichende IT-Sicherheitsmaßnahmen und Investitionen zur Verbesserung der nationalen Sicherheit und der Versorgungssicherheit.

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

TeleTrust fordert daher eine engagierte nationale Kraftanstrengung von Politik, Regulierern und Betreibern zur Verbesserung der Cybersicherheit und der nationalen Sicherheit, insbesondere:

- Beschleunigung der Energiewende und schnelle Digitalisierung mit einem sehr hohen Security Level

- Nachschärfung des IT-Sicherheitsgesetzes auf ein höheres Sicherheits- und Vertrauensniveau
- Strengere Prüfung der Umsetzung des höheren Sicherheitslevels durch Auditoren bei Versorgungsunternehmen (KRITIS)
- Pragmatische, unbürokratische Unterstützung und Förderung der KMU bei der Bewältigung der IT-Sicherheitslage
- Wirksame Absicherung der Industrieproduktion und digitaler Industrie-Netzwerke, einschließlich Logistik und Supply Chain
- Beachtung der Vertrauenswürdigkeit von IT-Sicherheitslösungen bei Kaufentscheidungen
- Verbesserung des Qualifizierungsniveaus des Personals in Bezug auf IT-/OT-Sicherheit

Der Digitalverband Bitkom sieht neben den Bestrebungen auf EU-Ebene auch die notwendige Kooperation mit weiteren Verbündeten. „Die Kriege der Zukunft werden hybrid geführt: im digitalen Raum gleichermaßen wie in der Luft, zu Wasser oder an Land. Auf diese neue Form der Kriegsführung müssen sich Wirtschaft, Staat und Gesellschaft einstellen", so Bitkom-Präsident Achim Berg. Es sei essenziell, die hiesige Wirtschaft und die kritischen Infrastrukturen vor digitalen Angriffen zu schützen, so Berg. „Cybersicherheit muss für den NATO-Raum und seine Partner gesamtheitlich gedacht werden. Wir brauchen eine Cyber-NATO."

So fordert der Verband der führenden europäischen Telekommunikationsbetreiber (European Telecommunications Network Operators, ETNO) „eine stärkere europäische Koordinierung in einer heiklen Zeit". Da Anbieter von IKT-Produkten und -Diensten, die zu einem integralen Bestandteil von Kommunikationsnetzen werden, am besten in der Lage seien, ihre eigenen Schwachstellen zu erkennen, sei ihre Rolle bei der Bekämpfung von Cyberbedrohungen von größter Bedeutung. ETNO fordert daher den Rat der EU auf, die Notwendigkeit einer besseren Zuordnung der Verantwortung für das Risikomanagement in digitalen Infrastrukturen entlang der IKT-Lieferkette zu prüfen.

Quelle: Secunet

Steffen Heyde, Leiter der TeleTrust-Arbeitsgemeinschaft „Smart Grids / Industrial Security": „Die neue geopolitische Lage, ausgelöst durch den Ukraine-Konflikt, ist Zäsur und Zeitenwende auch für die IT-Sicherheit in Deutschland."

Die NIS-2-Richtlinie sei das beste Instrument, um die noch bestehende Lücke in der Lieferkettensicherheit zu schließen, wenn ihr Anwendungsbereich IKT-Lieferanten kritischer Netzwerkkomponenten einschließen würde. Es sei noch nicht zu spät, da die Richtlinie noch verhandelt wird. Dies würde die allgemeine Widerstandsfähigkeit kritischer Netzwerke und wesentlicher Dienste, demokratischer Institutionen und Prozesse sowie der wirtschaftlichen Sicherheit in Europa insgesamt stärken.

Die laufende Diskussion und die umfassende Betrachtung zur Cyberresilienz sind wichtig und notwendig. Gleichzeitig drängt die Zeit durch die sich immer weiter verschärfende Bedrohungslage. Deshalb bleibt zu hoffen, dass zum Beispiel der European Cyber Resilience Act ohne Verzögerung verabschiedet wird und die Maßnahmen schnell umgesetzt werden. □

Mit ganzheitlicher IT-Sicherheit Cybergefahren trotzen

Die IT-Sicherheitslage ist kritisch: 2021 zählten die Security-Expert*innen von G DATA CyberDefense mehr als 23 Millionen neue Schadprogramme – Tendenz steigend. Hinzu kommen unzählige Phishing-Mails und andere Cyberattacken. Wirksamen Schutz vor Cyberkriminalität erreichen Unternehmen nur durch ein ganzheitliches Security-Konzept. Ein passendes Lösungsportfolio zeigt G DATA Fachhändlern und Besuchern auf der it-sa.

Mitarbeitende als Teil der Cyberabwehr

Einen Virenschutz hat nahezu jedes Unternehmen im Einsatz und dieser ist eine gute Basis für IT-Security – aber damit allein ist es nicht getan. Ein erfolgreicher Schutz muss vielschichtig sein. Ein weiterer zentraler Baustein der Cyberabwehr von Firmen ist die eigene Belegschaft. Cyberkriminelle setzen auf gezieltes Social Engineering, um über Angestellte in die IT-Infrastruktur zu gelangen. Dazu setzen sie auf personalisierte Phishing-Mails – auch bekannt als Spear-Phishing. Durch die G DATA Security Awareness Trainings werden Mitarbeitende für Cybergefahren sensibilisiert und sie erhalten das nötige Wissen rund um IT-Sicherheit, um richtig zu reagieren.

In mehr als 40 Kursen werden verschiedene Themen rund um IT-Sicherheit bedarfsgerecht und spielerisch vermittelt. Die Lerninhalte der G DATA Security Awareness Trainings verfestigen sich durch Wiederholungen. Ein spielerischer Ansatz erhöht dabei die Motivation bei den Lernenden. Besondere Aufmerksamkeit erhält dabei das Thema Phishing: Zusätzlich können IT-Verantwortliche Mitarbeitenden eine Phishing-Trainingsreihe anbieten, um sie speziell in diesem Thema nachhaltig zu schulen.

G DATA CyberDefense

TRUST IN GERMAN SICHERHEIT

Das Netzwerk im Blick durch G DATA SecMon

Die IT-Systeme in Unternehmen sollten laufend überwacht werden, um Unregelmäßigkeiten und auch mögliche Cyberangriffe frühzeitig zu erkennen und zu stoppen. Oft ist das für IT-Abteilungen aufgrund der Aufgabenfülle und dem Fachkräftemangel nicht leistbar. Mit G DATA SecMon legen IT-Verantwortliche die Überwachung der IT-Infrastruktur in die kompetenten Hände des Cyber-Defense-Unternehmens aus Bochum. Die Security-Experten von G DATA übernehmen die Analyse und Bewertung der Daten aus dem Monitoringsystem und schlagen umgehend Alarm, wenn sie einen Security-Vorfall entdecken.

Incident Response

Für Unternehmen stellt sich heute nicht mehr die Frage, ob sie von Cyberkriminellen angegriffen werden, sondern wann dies passieren wird. Ist eine Attacke erfolgreich, ist der Schaden oft groß – wenn es zu System- und Arbeitsausfällen kommt. Schnelle Hilfe ist dann entscheidend. Die Incident-Response-Teams von G DATA machen Unternehmen wieder arbeitsfähig und helfen beim Beseitigen der Schäden. Aufgrund der Kompetenzen im Bereich Incident Response ist G DATA CyberDefense mit seiner hundertprozentigen Tochter G DATA Advanced Analytics vom Bundesamt in der Informationstechnik (BSI) in die Liste der qualifizierten APT-Response-Dienstleister aufgenommen worden. Damit ist klar: Partner und Kunden können sich auf die Vertrauenswürdigkeit von G DATA verlassen.

Workshops „Learning aus Incidents“ auf der it-sa

Auf der it-sa in Nürnberg präsentiert G DATA CyberDefense in Halle 7a, Stand 311 sein ganzheitliches Security-Portfolio aus Dienstleistungen und Lösungen. Darüber hinaus veranstaltet G DATA zwei Workshops während der Messe: Am 25.10.2022 von 14:30 bis 17:30 Uhr und am 26.10.2022 von 9:30 bis 12:30 Uhr geht es um das Thema „Learnings aus Incident Response: Darauf kommt es bei Cybersicherheit heute an“. Dabei geben die Cyber-Defense-Experten einen Einblick aus erster Hand, was zu tun ist, wenn eine Cyberattacke erfolgreich war. Kern der Workshops ist die Frage, welche Maßnahmen Unternehmen ergreifen müssen, um Schäden durch Angriffe deutlich zu verringern oder ganz zu verhindern. Die Referenten greifen dabei auf ihren großen Erfahrungsschatz zurück und berichten direkt aus der Praxis, auf was es bei IT-Sicherheit ankommt. ■

Sichern Sie sich jetzt Ihren Platz im Workshop:

Wenn eine Cloud die andere Cloud angreift

Mit dem Multicloud-Ansatz steigt nicht nur die Komplexität, auch die Cloud-Sicherheit muss neue Risiken berücksichtigen. Dazu gehört, dass Angriffe auf eine Cloud auf die anderen übergehen können. Viele Sicherheitskonzepte haben noch Lücken, wenn es um Multicloud-Attacken geht.

Von Dipl.-Phys. Oliver Schonschek

Bild: alexyz3d/stock.adobe.com

Clouds sollten nicht nur als Angriffsziel gesehen werden, sondern auch als Angriffswerkzeug.

Eine Umfrage von HashiCorp zum Stand der Cloud-Strategie zeigt, dass bereits 76 Prozent der Unternehmen eine Multicloud-Strategie eingeführt haben. „Die Ära der Multicloud ist da, angetrieben von der digitalen Transformation, dem Kostendruck und von Organisationen, die eine Anbieterabhängigkeit vermeiden wollen“, sagte Armon Dadgar, Mitbegründer und CTO von HashiCorp. „Allerdings waren bisher nicht alle Unternehmen in der Lage, Multicloud zu operationalisieren, was auf Fachkräftemangel, inkonsistente Arbeitsabläufe in Cloud-Umgebungen und Teams, die in Silos arbeiten, zurückzuführen ist.“

Die Umfrageergebnisse zeigen zudem, dass Cloud-Sicherheit sowohl ein Treiber als auch ein Hemmnis für die Einführung von Multiclouds war. Die Befragten waren sich einig, dass die größten Sicherheitsherausforderungen in der Multicloud der Schutz von Daten und Privatsphäre (40 %), Datendiebstahl (33 %) und die Einhaltung gesetzlicher Vorschriften (31 %) waren. Personal- und Fachkräftemangel (26 %) standen ganz oben auf der Liste, als die Befragten nach den wichtigsten Herausforderungen für die Cloud-Sicherheit gefragt wurden. Darauf folgten unzureichende Tools und keine Sichtbarkeit in Echtzeit (jeweils 12 %).

Multicloud-Sicherheit ist komplex und uneinheitlich

Trotz der zunehmenden Verbreitung und Nutzung von Cloud-Diensten haben Unternehmen weiterhin Bedenken hinsichtlich der zunehmenden Komplexität von Cloud-Diensten, so der Thales Cloud Security Report 2022. Die Mehrheit (51 %) der IT-Fachleute ist der Meinung, dass es komplexer ist, den Datenschutz in einer Cloud zu verwalten als On-Premises.

Mit zunehmender Komplexität steigt auch der Bedarf an robuster Cybersicherheit. Auf die Frage, wie viel Prozent ihrer sensiblen Daten in der Cloud gespeichert sind, antwortete eine Mehrheit (66 %) mit 21 bis 60 Prozent der Daten. Allerdings gab nur ein Viertel an, dass sie alle Daten vollständig klassifizieren können. Auch Cyberangriffe stellen ein ständiges Risiko für Cloud-Anwendungen und -Daten dar. Die Befragten berichteten über zunehmende Angriffe, wobei ein Viertel eine Zunahme von Malware und Ransomware und ein Fünftel eine Zunahme von Phishing/Whaling feststellten. 45 Prozent haben eine Datenschutzverletzung erlebt oder ein Audit nicht bestanden, das Daten und Anwendungen in der Cloud betraf, gegenüber 35 Prozent im Jahr 2021.

Dabei ist Multicloud-Sicherheit oftmals nicht übergreifend umgesetzt, sondern in vielen Fällen Cloud für Cloud, was mit weiterer Komplexität und mit Risiken verbunden ist. So besagt der 2022 Multicloud Security Report von Valtix, dass 72 Prozent der IT-Führungskräfte angeben, ihre Cloud-Sicherheitsstrategie sei für jeden Cloud-Anbieter unterschiedlich. Valtix fordert deshalb: Im Jahr 2022 muss diese Single-Cloud-Sicherheitsmentalität einer Multicloud-Sicherheitsmentalität weichen. Andernfalls wird die Sicherheit unweigerlich zu einer Belastung für das Geschäft.

Tatsächlich können nicht nur Belastungen für das Geschäft die Folge sein, sondern sogar Risiken wie Cloud-Cloud-Attacken.

Angriffe und Schwachstellen in allen Clouds erkennen

Werden alle genutzten Clouds einzelnen verwaltet und abgesichert, fehlt der Blick auf ein Risiko, das noch viel zu häufig übersehen wird: Angreifende nutzen Schwachstellen in einer Cloud aus, um sich dort einzunisten. Dann verwenden sie die Migration von Daten innerhalb der Multicloud, um auf einem scheinbar vertrauenswürdigen Weg in die nächste Cloud zu gelangen. Letztlich erfolgt also ein Angriff von der einen Cloud auf die andere Cloud, die ein Unternehmen verwendet. ⇨

- Die Cloud Matrix innerhalb der Mitre Att&ck Matrix for Enterprise zeigt die Vielfalt der Angriffsmöglichkeiten auf Clouds. Hinzu kommt noch, dass viele dieser Attacken auch aus dem Inneren der Multicloud gestartet werden können, als Cloud-Cloud-Attacke.

Die Unternehmen würden eine einzige einheitliche Sicherheitsplattform mit einem einzigen Dashboard bevorzugen, auf der sie alle erforderlichen Richtlinien zum Schutz von Daten in der Cloud konfigurieren können. Derzeit müssen sie aber mit drei oder mehr separaten Sicherheitslösungs-Dashboards arbeiten, um die Sicherheit ihrer Multicloud zu konfigurieren.

Ein neuer Blick auf die Multicloud-Sicherheit

Mehr Transparenz in jede genutzte Cloud, aber auch in die Migration der Daten und Workloads zwischen den Clouds einer Multicloud-Umgebung, das ist das Ziel einer übergreifenden Multicloud-Security. Unternehmen, die zunehmend auf Multicloud-Umgebungen setzen, müssen bereits jetzt eine Reihe von Herausforderungen angehen, die eine Cloud-Cloud-Migration mit sich bringt, darunter inkompatible Schnittstellen (APIs) und Infrastrukturen, verschiedene Cloud-Tools und -Funktionen, die fehlende Übereinstimmung bei den Cloud-Richtlinien, unterschiedliche Kostenmodelle der Cloud-Anbieter, Abhängigkeiten der Applikationen von bestimmten Cloud-Services, lange Datenübertragungszeiten zwischen den Clouds und die unterschiedliche Performance der Clouds.

Zusätzlich aber müssen Unternehmen an die möglichen Angriffe denken, die ebenfalls von Cloud zu Cloud gehen können, wie es die Daten und Workloads tun. Um das zu verhindern, müssen alle Schwachstellen und Anzeichen für Cloud-Attacken gesehen werden – nicht nur Cloud für Cloud, sondern auch von Cloud zu Cloud und damit übergreifend. Andernfalls wird die Entwicklung zur Multicloud auch zu multiplen Sicherheitsproblemen und Attacken führen, das zeigt sich bereits heute. □

Alle Schwachstellen für Cloud-Attacken müssen bekämpft werden – nicht nur Cloud für Cloud, sondern auch von Cloud zu Cloud.

OT-Security: Die Suche nach dem Königsweg

Der Schutz vor Cyberattacken auf Kritische Infrastrukturen und Industrie muss intensiviert werden. Wie kann der IT-Security-Channel in der OT-Security Fuß fassen? Genau wie IT und OT konvergieren, müssen auch die Security-Lösungen für beide Bereiche zusammenfinden.

Von Dipl.-Phys. Oliver Schonschek

Bild: Gorodenkoff/stock.adobe.com

Security-Lösungen für IT und OT müssen zusammenfinden.

„Die Zeitenwende, die wir erleben, erfordert deutliche Investitionen in unsere Cyber- und Informationssicherheit. Das hat besondere Priorität für uns", sagte Bundesinnenministerin Nancy Faeser bei der Vorstellung des neuen „Digitalpolitischen Programms". Vertreter der Security-Branche wie der Bundesverband IT-Sicherheit e.V. (TeleTrusT) sehen einen konkreten Handlungsbedarf gerade bei Kritischen Infrastrukturen (KRITIS) und der Industrie. Cyberangriffe auf Unternehmen, staatliche Einrichtungen und kritische Infrastrukturen ⇨

Ein Problem hat sich über die Jahre nicht verändert: Es fehlen die erforderlichen Fachkräfte.

der Ukraine haben gezeigt, dass kritische Infrastrukturen und industrielle Netzwerke zunehmend in den Fokus politisch motivierter Cyberattacken geraten, so TeleTrusT. Entsprechend fordert der Verband unter anderem die wirksame Absicherung der Industrieproduktion und digitaler Industrie-Netzwerke, einschließlich Logistik und Supply Chain, sowie eine Verbesserung des Qualifizierungsniveaus des Personals in Bezug auf IT-/OT-Sicherheit.
Aufgaben und mögliche Projekte für Security-Hersteller und den Security-Channel gibt es damit genug, gerade auch im Bereich der Operational Technology (OT).

Sicherheit bei Industrie 4.0 ist seit Jahren eine Herausforderung

Der Bedarf an OT-Security steigt gegenwärtig besonders an, doch ein Thema ist die Sicherheit im Umfeld von Industrie 4.0 schon seit langem. Leider nicht nur ein Thema, sondern eine echte Herausforderung. Die Hemmnisse für den Einsatz von Industrie-4.0-Anwendungen haben sich in den vergangenen Jahren praktisch nicht verändert, so eine Umfrage des Digitalverbands Bitkom zu Industrie 4.0. Die größten Herausforderungen waren und sind fehlende finanzielle Mittel (77 %), Anforderungen an den Datenschutz (61 %) und an die IT-Sicherheit (57 %) sowie der Fachkräftemangel (55 %).
Offensichtlich ist es nicht einfach, dem Bedarf an Operational Technology Security gerecht zu werden. Einige Gründe liefert bereits die Bitkom-Umfrage: Es fehlen oftmals das notwendige Budget und die erforderlichen Fachkräfte.

Neue Risiken bedürfen auch neuer Security-Ansätze

Der entscheidende Schritt für Ramsey Hajj, Global Industrial IIoT/ICS Leader bei Deloitte, ist, dass nicht nur IT und OT technisch zusammenwachsen, sondern dass auch die Teams für IT-Sicherheit und OT-Sicherheit miteinander sprechen und arbeiten. „Sie müssen sie zusammenbringen und alle Missverständnisse korrigieren, die eine Gruppe möglicherweise über die andere hat. Sie müssen verstehen, dass es für sie strategisch wichtig ist, zusammenzuarbeiten, anstatt Gegner zu sein“, so Hajj. „Zum Beispiel könnte eine Änderung in einem Herstellungsprozess eine Cyber-Schwachstelle öffnen, über die die IT-Leute Bescheid wissen und die sie beheben müssen, bevor der Prozess implementiert ist“, begründet Hajj die notwendige Kooperation.
Überträgt man diesen Gedanken auf die Anbieter und Dienstleister aus der IT-Sicherheit, sollten auch diese mit OT-Anbietern und -Dienstleistern kooperieren. Die Lösungen und Services für IT-Sicherheit und OT benötigen entsprechend Schnittstellen und gemeinsame Management-Tools und Dashboards.
Tatsächlich gibt es bereits viele Beispiele für genau solche Kooperationen und Schnittstellen.

OT-Security hält im Security-Channel Einzug

Partnerschaften dieser und anderer OT-Security-Anbieter mit Security-Dienstleistern, MSSP und Distributoren sind keine Seltenheit mehr. „Der dynamische Vernetzungsprozess macht die Produktion flexibler und schneller. Dadurch entstehen neue Geschäftsmodelle, aber gleichzeitig auch neue Angriffspunkte für Cyberkriminelle“, sagt Dr.-Ing. Stefan Rummenhöller, Geschäftsführer des Wuppertaler IT-Sicherheitsspezialisten r-tec.

Die richtigen Startpunkte zur Absicherung der OT

OT-Sicherheit ist ein weites Feld. Es wird kaum gelingen, sofort in allen Bereichen die gewünschte Kooperation und die notwendigen Schnittstellen aufzubauen. Eine Priorisierung erscheint deshalb sinnvoll. Die Security-Experten von KPMG nennen drei Bereiche, die zuerst angegangen werden sollten: Endpunktschutz von OT-Ressourcen, Perimeter-Firewalls um OT-Assets herum und Netzwerksegmentierung innerhalb von OT und zwischen OT/IT.

Daneben sollten Unternehmen die Sichtbarkeit von OT-Netzwerken frühzeitig implementieren und eine Überwachung des OT-Netzwerks auf bekannte Bedrohungen oder verdächtiges Verhalten ermöglichen. Idealerweise sollten diese Technologien in das bestehende Überwachungs- und Reaktions-Framework der Organisation integriert werden, also in ein bestehendes SOC (Security Operations Center) und Incident Response Team, so KPMG.

Trotz steigender OT-Risiken muss noch Awareness geschaffen werden

Die Marktforscher von Gartner berichten, dass 38 Prozent der Industrieunternehmen die Ausgaben für OT-Sicherheit im Jahr 2021 um fünf bis zehn Prozent erhöhen wollten, weitere acht Prozent um mehr als zehn Prozent. Laut Gartner reicht dies jedoch möglicherweise nicht aus, um der jahrelang zu geringen Investition in diesem Bereich entgegenzuwirken.

Trotz der hohen Risiken im OT-Bereich sind Projekte für OT-Security keine Selbstläufer. Neben der Suche nach geeigneten Partnern müssen auch die Kunden überzeugt werden. Gartner prognostiziert, dass die finanziellen Auswirkungen von OT-Angriffen, die sogar zu Todesfällen führen können, bis 2023 einen Schaden von über 50 Milliarden US-Dollar erreichen werden. Selbst ohne Berücksichtigung des Wertes von Menschenleben entstehen den Organisationen Kosten in Form von Entschädigungen, Rechtsstreitigkeiten, Versicherungen, Bußgeldern und Reputationsverlust, so Gartner. Durchaus wichtige Argumente für Gespräche mit den Industriekunden. □

Neue Cyber-Security-Strategien für Smart Manufacturing

Das Beratungshaus Deloitte empfiehlt für die Verbindung von IT- und OT-Sicherheit:

- Schaffung eines Production Security Operations Center: Use Case Design auf Basis bestehender IT Standard Use Cases (z. B. BruteForce und DoS, Suspicious User Behavior, Inappropriate Credential Usage)
- Design eines Incident-Handling-Prozesses für die Zusammenarbeit zwischen IT und OT
- Neugestaltung der Sicherheitsorganisation, um OT-Security in die globale Struktur der Organisation zu integrieren.
- Security by Design sowie Risiko- und Schwachstellenanalyse für Smart Products
- Secure Life Cycle Development (SLCD) für Smart Products
- Schaffung eines Security Frameworks und eines erhöhten Datenschutz-Bewusstseins bei Mitarbeitern, Kunden und Anwendern

VPN und Cloud – Vereinen Sie Flexibilität mit Sicherheit!

Im Zuge des weiter voranschreitenden Cloud-Booms scheinen Schlagwörter wie „Zero Trust“, „Single Sign On“ oder „SD-WAN“ den klassischen VPN-Tunnel immer weiter abzulösen. Doch wieso eigentlich? Weil sich virtuelle private Netzwerke und Cloudanbindung von vornherein ausschließen? Mitnichten! Entscheidet man sich für die richtige, moderne Lösung, lassen sich zeitgemäße VPN-Strukturen und digitale Cloud-Technik zu einem mächtigen IT-Security-Instrument kombinieren.

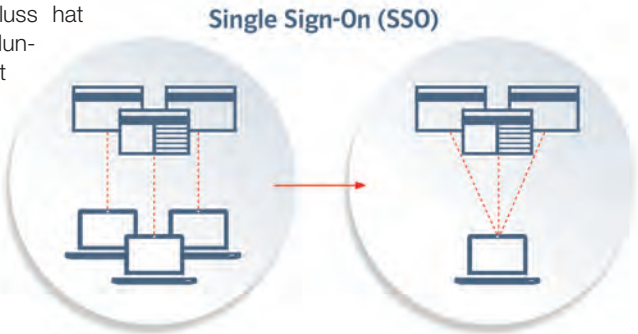
NCP SECURE COMMUNICATIONS

Security auf einer neuen Stufe

Damit dies gelingt, müssen vor allem zwei Punkte erfüllt sein: Hochsichere IPsec-Datenkommunikation und vollständige Kompatibilität mit allen gängigen Cloud-Technologien. Das entsprechende Sicherheitslevel kommt bei einer cloud-integrierten VPN-Lösung durch das Gateway in Verbindung mit einem Management-System zustande. Dies kann z.B. der NCP Virtual Secure Enterprise VPN Server (vSES) in Kombination mit dem NCP Secure Enterprise Management (SEM) sein. Dieser Zusammenschluss hat den Vorteil, dass alle Verbindungen IPsec-basiert und somit hochsicher übertragen werden. Außerdem liegt das Gateway nicht direkt in der Cloud, sondern bildet hinter der Firewall eine abgesicherte Umgebung direkt auf dem Server, welcher im Hinblick auf Ihre digitale Souveränität in einem deutschen Rechenzentrum beheimatet sein sollte.

VPN kann auch Cloud!

Um die Kompatibilität zu allen etablierten Cloud-Services zu garantieren, setzen Unternehmen am besten auf Lösungen wie das Enterprise-VPN von NCP, die z.B. mühelos als Teil einer SASE- oder SD-WAN-Infrastruktur eingesetzt werden können. Die



VPN-Komponenten sind hier bereits von Natur aus „cloudfähig“ und fügen sich auch in komplexe SD-WAN-Verbünde ein. Die Integration in ein SAML-System ist ebenfalls kein Problem. Hier gilt die Authentisierung des Nutzers am SSO-Portal dank des Tunnels dann sowohl für interne Dienste als auch externe Cloudanwendungen. So genießen Administratoren und Nutzer weiterhin alle Vorteile ihrer SAML-Schnittstelle, können Daten allerdings über einen hochsicheren IPsec-Tunnel mit voller Geschwindigkeit übertragen.

Volle Kontrolle dank Zero Trust

Technologien wie SAML/SSO sind oft auch Bestandteil einer übergeordneten Zero-Trust-Strategie, bei der Nutzer durch granulare Firewall-Regeln nur Zugriff auf für sie relevante Anwendungen haben (Least-privilege-Prinzip). Mithilfe einer zentralen Management-Komponente wie dem NCP Secure Enterprise Management (SEM) definieren Administratoren alle Zugriffsrechte ihrer Anwender mit wenig Aufwand. Zusätzlich profitieren Sie von einem großen Funktionsumfang der VPN-Software: Der NCP VPN-Bypass oder Split Tunneling helfen dabei, den VPN-Server zu entlasten, indem datenhungrige Anwendungen ohne Sicherheitsrelevanz am Tunnel vorbeigeleitet werden. Für die Sicherheit des gesamten Netzes sind auch Endpoint Policy Checks unerlässlich, die Endgeräte vor jedem Login-Versuch auf vordefinierte Security-Parameter hin überprüft. Stellt das System z.B. veraltete Software auf einem Laptop fest, wird die Verbindung erst nach Abschluss der notwendigen Updates aufgebaut. Da der Administrator sowohl Policies als auch Updates mit wenigen Klicks an einzelne Nutzergruppen oder die gesamte Organisation verteilt, bleiben so auch große Anwenderzahlen immer auf dem neuesten Sicherheitsstand! ■

Besuchen Sie uns auf der it-sa (Halle 7A – Stand 412)
oder informieren Sie sich unter: **www.ncp-e.com**

CISOs gewinnen an Bedeutung und Einfluss

Zunehmende Sicherheitsverletzungen, komplexer werdende Datenschutzbestimmungen und die Trennung von Sicherheit und IT – Das Aufgabenfeld eines CISO entwickelt sich aufgrund der sich ändernden Erwartungen in Bezug auf Datenschutz und Datensicherheit immer schneller. Gleichzeitig erhöht sich so die Bedeutung der Sicherheitsfunktion der CISOs.

Von Dipl. Betriebswirt Otto Geißler

Bild: Rido/stock.adobe.com

Heute wird von CISOs meist nicht nur verlangt, dass sie dem Vorstand berichten, sondern auch, dass sie in diesem vertreten sind.

Wenn es in den vergangenen Jahren eine Führungsposition im Sicherheitsbereich gab, war sie in der Regel einem Vice President of Infrastructure oder einer ähnlichen Funktion unterstellt und beschränkte sich auf operative Tätigkeiten wie beispielsweise die Zugangskontrolle. Heute wird von CISOs (Chief Information Security Officers) meist nicht nur verlangt, dass sie dem Vorstand berichten, sondern auch, dass sie in diesem vertreten sind. Aufgrund der aktuellen Schlagzeilen und Sicherheitslage wollen viele Vorstände eher mit der Sicherheitsleitung sprechen, bevor sie den CIO kontaktieren.

Veränderte Anforderungen

Das Aufgabenfeld der CISOs entwickelt sich aufgrund der sich ändernden Erwartungen in Bezug auf Datenschutz und Datensicherheit rasch weiter. Datenschutzverletzungen, die Einhaltung von Vorschriften und das Risikomanagement für Dritte sind zu einem wichtigen Thema geworden. Denn Unternehmen, die von Datenschutzverletzungen betroffen sind, müssen mit enormen Kosten und Markenschäden rechnen.

Gesetze wie die Datenschutz-Grundverordnung der Europäischen Union verstärken den Druck, indem sie von Unternehmen verlangen, neue und weitaus detailliertere Kontrollen für Kunden- und Verbraucherdaten einzuführen. Ferner werden Unternehmen mit Datenschutzverletzungen konfrontiert, die auf Schwachstellen in der Lieferkette und bei Dritten zurückzuführen sind, die wiederum neue Haftungsfälle auslösen können.

CISOs befinden sich inmitten dieses Wandels und werden zunehmend mit der Verantwortung für den Aufbau von Datenschutz-Risikoprogrammen und der Verwaltung von Drittanbieter-Risiken und Anbieterkontrollen betraut. Für viele sind dies neue Aufgabengebiete, in denen sie bis dato meist wenig Erfahrung vorweisen können.

Neues Risiko- und Regulierungsumfeld

Viele Unternehmen sehen sich beispielsweise gezwungen, neue Funktionen für das Daten-Mapping und die Nachverfolgung von Datenflüssen einzuführen, um die gestellten Anforderungen zu erfüllen. Ebenso stehen Themen wie die Datenminimierung im Rahmen der gesetzlichen Vorgaben in direktem Widerspruch zu den Data-Mining- und Data-Analytics-Initiativen, die viele Unternehmen in den letzten Jahren umgesetzt haben.

CTOs und CIOs wollten so viele Daten wie möglich sammeln und sie in Data Warehouses einspeisen, um das Unternehmen smarter zu machen. Das Risikomanagement von Drittanbietern bzw. die Kontrolle von Anbietern sind weitere Bereiche, die die Bedeutung und damit die Sichtbarkeit der CISOs deutlich prominenter machen.

Ein zunehmender Teil der Aufgaben eines Chief Information Security Officers besteht heute darin, die Produkte und Dienstleistungen von Anbietern für seine Organisation zu prüfen. Denn viele der jüngsten Sicherheitsverletzungen sind auf Angriffe zurückzuführen, bei denen Schwachstellen in Partnernetzwerken ausgenutzt wurden. Das bedeutet, die Sicherheitsorganisation ist häufiger damit betraut, potenzielle Probleme der Partnerunternehmen zu identifizieren und zu beseitigen.

Das bedeutet, der Chief Information Security Officer entscheidet mit dem C-Level (hochrangige Führungspositionen) mit welchen Partnern das Unternehmen Geschäfte machen sollte. Viele Sicherheitsorganisationen, mit denen CISOs zu tun haben, verbringen mittlerweile bis zu 40 Prozent ihrer Zeit mit der Verwaltung von Risiken durch Dritte. Das bringt sie in eine Reihe mit dem Einkauf und anderen Abteilungen beziehungsweise Aufgabenstellungen, mit denen sie in der Vergangenheit kaum etwas zu tun hatten.

⇨


Bild: Rido/stock.adobe.com

Der CISO muss heute in der Lage sein, mit dem C-Level bzw. Vorstand zusammenzuarbeiten, Geschäftsanforderungen zu verstehen sowie neue Initiativen zu ermöglichen.

Einflussreichere Rolle für CISOs

Nachdem CISOs bisher auf eine weitgehend operative und technische Rolle beschränkt waren, werden die Sicherheitsverantwortlichen in einer wachsenden Zahl von Unternehmen erstmals mit einer breiteren und einflussreicheren Rolle bedacht. CISOs erhalten damit mehr Gelegenheiten, Einfluss zu nehmen, Partnerschaften einzugehen und Veränderungen im gesamten Unternehmen zu unterstützen.

Wo es früher ausreichte, über operative und technische Fähigkeiten zu verfügen, müssen CISOs heute in der Lage sein, Geschäftssinn zu beweisen und aufzuzeigen, wie Sicherheit Werte und neue Marktchancen schafft. CISOs müssen daher befähigt sein, mit Geschäftsführern des C-Levels und dem Vorstand zusammenzuarbeiten, Geschäftsanforderungen zu verstehen, neue Initiativen zu ermöglichen und als Vermittler zwischen verschiedenen Geschäftsfunktionen zu fungieren.

Neues Berichtswesen für CISOs

Traditionell berichten CISOs an den CIO, CTO oder in einigen Fällen an die Leiter der Infrastruktur, da die Rolle in erster Linie als operativ und technisch angesehen wurde. Während CIOs in der Regel daran gemessen und dafür belohnt werden, dass sie die Systeme aufrechterhalten und neue Technologien installieren, konzentrieren sich CISOs auf den Schutz der Unternehmensressourcen und die Reduzierung der Risiken. Mittlerweile wird in der Diskussion jedoch immer deutlicher, dass die Rolle des CISO aufgrund der gegensätzlichen Interessenslage von der IT getrennt werden sollte, um noch umfassender Einfluss auf die Risiken zu nehmen und Veränderungen voranzutreiben. Aus diesem Grunde berichten einige CISOs direkt an CEOs, CFOs, COOs oder sogar General Counsels.

Natürlich untersteht die überwältigende Mehrheit der CISOs jedoch weiterhin den CIOs, da sie in Bereichen wie der Verwaltung der Netzwerksicherheit mit operativen Aufgaben betraut sind. Wenn diese operativen Aufgaben in andere Führungspositionen verlagert werden, wird der Fokus der CISOs mehr auf Governance und Strategie liegen.

Daher werden Forderungen laut, dass ein CISO eher die Rolle eines sogenannten Chief Information Risk Officer (CIRO) übernehmen sollte, der eng mit den Bereichen Finanzen, Strategie und anderen Gruppen zusammenarbeitet. Es ist zu erwarten, dass auch Funktionen des Richtlinienmanagements in die Rolle des CIRO übergehen könnten. □

Security-Kennzahlen für Vorstände

Geschäftsorientierte Vorstandsmitglieder wollen mit technisch-orientierten IT-Security-Daten auf strategischer Ebene versorgt werden. Welche Zahlen und Messgrößen sind geeignet, um Geschäftsführer auf C-Level zu überzeugen?

Von Dipl. Betriebswirt Otto Geißler

Bild: everythingpossible/stock.adobe.com

Trotz der hohen Komplexität sehen viele Top-Entscheider am liebsten simple Charts.

Security-Teams murren sehr gerne über die für sie meist viel zu verkürzten Darstellungsformen, die Vorstände gerne von ihnen wünschen. Am liebsten sehen viele Top-Entscheider simple Charts wie beispielsweise Ampel-Indikatoren in Rot-Gelb-Grün, um ein komplexes Gesamtbild mit Signalcharakter in ein einziges, sehr übersichtliches Bild zu packen.

Aber mal ehrlich: Einzelhandelsgeschäfte verkaufen ihre Smartphones auch nicht mit Kennzahlen wie „Umsatz pro Quadratmeter“ oder „Deckungsbeiträgen pro Stück“. Ampel-Indikatoren sind daher sicherlich eine Möglichkeit für sehr kompakte Präsentationen an den Vorstand, solange die einzelnen „Farben“ bzw. Eskalationsstufen klar verständlich definiert sind und ⇨


Bild: AnnaStills/stock.adobe.com

Bei der Präsentation eines IT-Security-Programms sollten die technischen Daten direkt in einen strategischen Rahmen übersetzt werden.

↪ über einen überschaubaren Umfang an Details genau erklärt werden können.
Dies impliziert ebenso eine gezielte Auswahl an Daten, Kennzahlen und Maßnahmen, die dem Vorstand letztlich vorgelegt werden, die aber auch gleichzeitig immer auf eine umfassende Unternehmensperspektive bezogen sein sollen. Dabei kann es zur Orientierung hilfreich sein, die Präsentation darauf aufzubauen, was Vorstandsmitglieder in der Regel über IT-Security in jedem Unternehmen wissen wollen.

Wichtigste Fragen zur IT-Security

In der Folge die vielleicht am häufigsten gestellten Fragen von Unternehmensvorständen zur Cybersicherheit:

- **„Sind wir sicher?“** Diese Frage ist der Fluch vieler CISOs bzw. Security-Teams, denn die Antwort lautet jetzt und in Zukunft immer „Nein“, wenn es um einen buchstäblich 100-prozentigen Schutz geht. Wenn man die Frage in „Wie hoch ist unser Gefährdungsgrad?“ umformuliert, geht es in die richtige Richtung und das Unternehmen beginnt, Fortschritte zu machen.
- **„Sind wir compliant?“** Diese Frage lässt sich oft leicht anhand von Audit-Ergebnissen beantworten, bietet aber keinen wirklichen Trost, da es sich immer um eine „punktuelle“ Perspektive handelt, die sich in jedem Augenblick ändern kann. Besser wäre es, ein IT-Security-Programm anhand eines gezielten Kontrollrahmens zu bewerten.
- **„Hatten wir irgendwelche relevanten Vorfälle?“** Die Mitglieder des Verwaltungsrats sind über alle bedeutenden Vorfälle gut informiert, daher wird diese Frage in der Regel mit Details sowie Schätzungen der Kosten und der potenziellen Haftung beantwortet.
- **„Wie effektiv ist unser Sicherheitsprogramm?“** Standardelement einer guten Unternehmensführung. Das heißt, Qualität geht vor. Und dann die Quantität.

Wichtige Messgrößen für die IT-Security

Bei der Ausarbeitung eines IT-Security-Programms sollte das erklärte Ziel darin bestehen, die detailliertesten technischen Daten direkt in einen strategischen Rahmen zu übersetzen, der auf Vorstandsebene verständlich ist.

- IT-Ressourcen (Anzahl der User, Geräte, Server, Anwendungen etc.)
- Nutzungsaktivität (Sitzungen, Flüsse, Nachrichten etc.)
- Prozesskontrollen (Erstellung/Änderung/Löschung von Benutzerkonten, Erkennung/Patch von Sicherheitslücken, Erkennung/Reaktion auf Vorfälle etc.)
- Echtzeit-(Inline-)Kontrollen (Anti-Malware, Firewall, E-Mail-Sicherheit etc.)
- Vorfälle

Wesentliche Kennzahlen für die IT-Security

In der Folge sind Kennzahlen aufgelistet, die einen strategischen Einblick in das IT-Security-Programm des Unternehmens bieten:

- **Cyber-Risiko:** Der prozentuale Anteil der unangemessenen Nutzungsaktivitäten an allen Nutzungsaktivitäten.

- **Wirksamkeit der IT-Security:** Prozentuale Verringerung des IT-Security-Risikos durch die Echtzeit-IT-Security-Kontrollen.
- **IT-Security-Belastung:** Durchschnittliche Anzahl von Nutzungsaktivitäten pro IT-Anlage.
- **IT-Security-Resilienz:** Durchschnittliche Anzahl der für jede Nutzungsaktivität angewendeten Echtzeit-Kontrollen.
- **Risiko-Aversionsverhältnis:** Die Bereitschaft, Produktivitätseinbußen (z. B. Passwortfehler, Falschmeldungen) im Vergleich zu den erlaubten oder verweigerten bösartigen Aktivitäten (echte Positivmeldungen plus Falschmeldungen) zu akzeptieren.

Zentrale Kostenaspekte für die IT-Security

Darüber hinaus müssen die anfallenden Kosten auf das jeweilige zu schützende Asset bezogen werden. Schließlich sind Finanzinformationen eine wichtige „Verkehrssprache" der Vorstände:

- **Verhältnis zwischen Verlust und Asset:** Ausgaben für IT-Security, einschließlich der Verluste durch Zwischenfälle, im Vergleich zum finanziellen Wert der IT-Anlagen.
- **Kontrollkosten pro IT-Asset (Anwendung):** Zugewiesene Kosten für IT-Security-Kontrollen pro IT-Asset.
- **Reduziertes Risiko pro Kosteneinheit:** Finanzieller Wert des reduzierten Risikos im Vergleich zu den gesamten IT-Security-Ausgaben.

Der Weg zum IT-Security-Programm

Mithilfe der Messgrößen zeigen CISOs bzw. die Security-Experten, dass sie über Bedrohungen strukturiert und ergebnisorientiert nachdenken und handeln. Ferner können sie belegen, wie relevant diese Bedrohungen für das Programm und seine Performance sind. Gleichzeitig wird veranschaulicht, wo es gegebenenfalls noch Verbesserungsmöglichkeiten gibt.

Das interne IT-Security-Programm sollte mit einer sogenannten „Außenperspektive" in Verbindung gebracht werden. Hier kann das Security-Team Vertrauen aufbauen, indem es ein Framework verwendet, das von einer externen Autorität unterstützt wird. Eine Möglichkeit wäre beispielsweise das NIST Cybersecurity Framework (CSF). Das NIST CSF ist um fünf Funktionsbereiche herum organisiert: Identify, Protect, Detect, Respond und Recover.

Damit wäre es möglich, zum Beispiel eine funktionsübergreifende Supply-Chain-Security zu implementieren. Das Prinzip wird nachfolgend an drei der Funktionen beispielhaft veranschaulicht:

- Identify verfügt über Unterfunktionen wie Asset Management, Identity and Access Management (IAM) und mehr.
- Protect verfügt über Unterfunktionen wie Vulnerability Management und SDLC etc.
- Detect verfügt über Unterfunktionen wie SIEM etc.

Das heißt, jede der fünf Fähigkeiten wird in wichtige „messbare" Teilfähigkeiten aufgeteilt. Diesen Unterfunktionen sollen dann Messgrößen bzw. Key Performance Indicators (KPIs) basierend auf den CSF-Ebenen zugewiesen werden. Wobei der KPI eine Messgröße für die jeweilige Reifestufe darstellt, die innerhalb dieser Unterfunktion erreicht wurde.

Fazit

Vergleicht man die oben skizzierten Messgrößen und Kennzahlen mit den zahlreichen Finanzkennzahlen auf den Investment-Websites, so lässt sich sehr schnell erkennen, dass dieser Ansatz auf einer weitaus zielführenderen strategischen Basis angesiedelt ist als das Durcheinander von Patch-Levels und gefundener Malware. Wenn CISOs bzw. die Security-Experten wollen, dass Führungskräfte die IT-Security im Unternehmen ernst nehmen, ist dies ein Weg dorthin. □

Warum „Made in Germany“ sicher und nachhaltig ist

Längst ist das Thema Nachhaltigkeit global zu einem Kernbaustein in der Strategie von Firmen geworden. Dabei besteht die Gefahr, dass der Begriff inflationär gebraucht oder sogar als Feigenblatt für Kunden missbraucht wird. Will man dies vermeiden, müssen in Unternehmen nicht nur das eigene nachhaltige Tun, sondern auch die Implementierung und die Sicherung der Prozesse berücksichtigt werden. Letztlich geht es um das unternehmerische Handeln und Denken, für das „Made in Germany“ ein Gütesiegel sein kann.

Seit 1978 gehört es zum unternehmerischen Selbstverständnis von TDT, als Experte für sichere und innovative Telekommunikation für unsere Kunden da zu sein: mit Produktneuerungen, einem ausgeprägten Servicebewusstsein und gelebter Nähe. Bei TDT kommen über 90% der Zulieferer aus der direkten Umgebung. Diese kurzen Wege und Lieferketten sind auch im Sinne von Nachhaltigkeit und Umweltschutz eine mehr als nur wirtschaftliche Lösung. Denn in Anbetracht der welt- und marktweiten Anspannungen hinsichtlich Lieferungen und Verfügbarkeiten von Material, muss „Made in Germany“ als Marke die Chance nutzen, nicht als museal-nostalgisches Relikt einer Wirtschaftswunder-Zeit eingeordnet zu werden. Stattdessen sollte „Made in Germany“ als international renommiertes Gütesiegel vital für Sicherheit, Verlässlichkeit und Zukunft stehen.

Michael Pickhardt, Vorstandsvorsitzender der TDT AG: „E für Environment, S für Social, G für Governance – die so genannten ESG-Kriterien sind aktuell im Zusammenhang mit dem neuen Lieferketten-Gesetz in aller Munde. Wir bei TDT haben diese Aspekte seit langem im Blick und gehen darüber hinaus: Unsere Geräte werden seit jeher weit über die jetzt geforderten fünf Jahre hinaus mit Updates versorgt und sogar um neue Fea-

Bild: Marina Geckeler/TDT AG

TDT® | Your experts in TELE COMMUNICATION

tures erweitert. Es fehlt bei den weiter anstehenden Herausforderungen unserer Zeit immer noch enorm an digitaler Kompetenz und Infrastruktur – und damit an digitaler Souveränität. Statt ausschließlich auf Expansion und Gewinne zu schielen, müssen wir jetzt und zukünftig auf Sicherheit setzen. Sicherheit muss bei uns allen schnellstmöglich den Stellenwert einnehmen, den bis jetzt noch der Profit um jeden Preis innehat."

Der immer günstigere Einkaufspreis kann hier nicht die Lösung sein, da er meist zu Lasten einer nachhaltigen Softwarepflege wie auch der Produktqualität geht. Wir sollten uns unternehmerisch von falsch verstandener Optimierung und den fatalen Abhängigkeiten des „Just in time"-Denkens lösen. Erst wenn Sicherheit – und als Bestandteil davon digitale Souveränität – ins Zentrum von gesellschaftlichem Denken und Handeln rücken, werden wir gestärkt aus der aktuellen Situation hervortreten. So erreichen wir die Voraussetzung dafür, das zu tun, was echte Nachhaltigkeit in unserem Markt bedeutet: qualitativ hochwertige Geräte, langlebige Hardware und eine langfristige Versorgung mit sicheren Software-Updates.

Ein Beispiel für gelebtes „Made in Germany" ist, dass wir als Unternehmen mitsamt unserer kompletten Prozesse 2017 vom BSI zertifiziert wurden. ■

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

Michael Pickhardt arbeitet seit dem Jahr 1984 in der Telekommunikationsbranche, ist Handelsrichter und Vorstandsvorsitzender der TDT AG, die seit über vier Jahrzehnten ein Pionier und Vorreiter für Lösungen in der digitalen Kommunikation ist.

Niemand will noch ein Passwort – oder?

Es gibt Themen rund um die IT, die immer wieder totgesagt werden und trotzdem mit schöner Regelmäßigkeit wieder auftauchen: Dazu gehören unter anderem die Grabgesänge der Messenger-Apologeten auf die E-Mail und der bereits häufig verkündete „Tod der Passwörter". Von Frank-Michael Schlede und Thomas Bär

Bild: Vitalii Vodolazskyi/stock.adobe.com

Unternehmen und ihre IT-Abteilungen werden auf absehbare Zeit nicht auf den Einsatz von Passwörtern verzichten können.

Die fast schon sprichwörtlichen gelben Sticker am Monitor, auf denen das Passwort oder auch mehrere Passwörter eines Nutzers notiert sind, können IT-Verantwortliche und Administratoren zu ihrem Leidwesen auch heute noch an vielen Monitoren oder unter vielen Tastaturen finden. Mit der vermehrten Abwanderung der Nutzer und ihrer Client-Systeme in den mobilen Bereich und Home-Offices hat sich dieses Problem noch einmal verschärft.
Der Administrator sieht diese „Beweise" nicht mehr und kann seine Nutzer nicht ermahnen. Also scheint es nur sinnvoll, Passwörter ganz abzuschaffen. Schließlich gibt es doch genügend andere Methoden, Nutzer sicher zu authentifizieren. Selbst wer sich diesem grenzenlosen Optimismus anschließt, sollte die Augen vor der Realität in den Unternehmen nicht verschließen: Passwörter existieren, sie werden eingesetzt und sie werden gestohlen, ausgelesen und missbraucht.

Passwörter sind da – ebenso wie ihre Schwachstellen

Während viele Befürworter des Zero-Trust-Ansatzes deshalb immer wieder vehement dafür eintreten, dass es ohne den Einsatz der traditionellen Passwörter gehen muss, sehen sich die IT-Abteilungen mit einer großen Menge „real existierender" Passwörter konfrontiert. Gerade bei den kleinen und mittelgroßen Betrieben (SMB – Small and Medium Business) ist das ein Problem.
Viele Security-Spezialisten weisen schon seit einigen Jahren darauf hin, dass sowohl die IT-Verantwortlichen und -Administratoren als auch die Geschäftsleitung in diesen Unternehmen häufig kaum einen Überblick darüber besitzen, wie ihre Mitarbeiter mit dem sensiblen Passwort-Thema umgehen.
Die Sicherheitsspezialisten des amerikanischen Unternehmens Keeper haben in Zusammenarbeit mit den Analysten vom Ponemon Institute einen globalen Bericht über die Cybersicherheit in kleinen und mittleren Unternehmen zusammengestellt. Dieser zeigte die Problematik auf: Nicht nur dass fast 70 Prozent der Unternehmen zu berichten wussten, dass Passwörter gestohlen wurden, sondern auch die für das Zurücksetzen der Passwörter benötigte Zeit und die Änderung der Passwörter, wenn ein Mitarbeiter das Unternehmen verlässt, wurden eindeutig von den Unternehmen als Schwachstellen identifiziert.
Für die Verantwortlichen gilt es also, dem Umgang ihrer Mitarbeiter mit den Passwörtern erhöhte Aufmerksamkeit zu schenken. Das heißt, dass neben Richtlinien für Schulungen und Unternehmen auch geeignete technische Lösungen bereitstehen müssen, die eine einheitliche, sichere Bewältigung dieser Problematik ermöglichen.

Es geht (noch) nicht ohne – aber es geht besser

Passwörter spielen eine wichtige Rolle in jeder IAM-Strategie (Identity and Access Management). Wie viele andere Begriffe und Akronyme in der IT wird auch IAM von den Security-Firmen und -Experten jeweils unterschiedlich definiert. Drei Hauptkomponenten, die aber vielfach vorkommen, sind Single-Sign-On- (SSO) und Privileged-Access-Management-Lösungen (PAM) und ganz sicher auch das Enterprise-Passwort-Management (EPM). Dabei wird Single Sign-On vielfach als die Lösung schlechthin betrachtet, ermöglichen solche Programm es den Nutzern doch, sich mit nur einem einzigen Set von Login-Daten an vielen Webseiten, SaaS-Lösungen (Software as a Service) wie Salesforce, Google oder SAP anzumelden. Doch SSO allein ist sicher nicht die ultimative Lösung: Verwendet die eingesetzte SSO-Software beispielsweise keine konsequente End-to-End-Verschlüsselung tut sich an dieser Stelle bereits wiederum eine Sicherheitslücke auf. ⇨

Während also SSO „nur“ den generellen Zugriff der Nutzer ermöglicht, kann eine PAM-Lösung einen sehr feiner strukturierten Zugriff (hier wird oft der Begriff „granular“ verwendet) realisieren, was zumeist mit einem Rollen-basierten Zugriff (RBAC – Role-Based Access Control) einhergeht. Einfach gesagt, bedeutet eine solche Technik, dass durch eine PAM-Lösung ganz genau definiert wird, welche Personengruppe oder auch einzelne Person beispielsweise welche Operationen auf einer Datenbank ausführen darf.

Die Komplexität einer solchen Lösung sorgt unter anderem dafür, dass RBAC und PAM zumeist nur in großen Unternehmen mit einer entsprechend ausgebildeten IT-Abteilung zum Einsatz kommen.

Welche Möglichkeiten bietet da noch ein Passwort-Manager, besonders dann, wenn er speziell für den Einsatz im Business-Umfeld entwickelt wurde? Grundsätzlich erlaubt es beispielsweise ein derartiges Programm den Nutzern, ihre Login-Daten sicher in einem zentralen, privaten und sicheren Repository abzulegen. Genau wie beim Einsatz einer SSO-Lösung müssen die Nutzer sich dann nur noch ein „Masterpasswort“ merken, um auf alle in diesem Archiv abgespeicherten Zugangsdaten zugreifen zu können.

Im Gegensatz zu SSO können Passwort-Manager mit allen Webseiten, allen Anwendungen und Systemen funktionieren, die im Unternehmen von den Nutzern eingesetzt werden. Zudem bieten sie zusätzliche Funktion wie das Generieren von sicheren Passwörtern, automatisches Ausfüllen beispielsweise auf Webseiten und zusätzliche private gesicherte Ablagen (Tresore) für die Nutzer.

Manche Anbieter sind zudem dazu übergegangen, ihre Lösung auf einer Zero-Trust- und Zero-Knowledge-Plattform in der Cloud aufzubauen und anzubieten. Somit entfällt für die Unternehmen das Problem, dass sie eine eigene Netzwerk- und Speicherinfrastruktur für das

Bild: profit_image/stock.adobe.com

Single Sign-On wird vielfach als die Lösung schlechthin betrachtet, da die Nutzer sich mit nur einem einzigen Set von Login-Daten an vielen Webseiten anmelden können.

Bild: momius/stock.adobe.com

Eine PAM-Lösung kann einen sehr fein strukturierten Zugriff realisieren, was zumeist mit einem Rollen-basierten Zugriff (RBAC – Role-Based Access Control) einhergeht.

Passwort-Management On-Premise aufbauen und warten müssen.

Fazit: Passwörter brauchen maximale Sicherheit

Schon diese kurzen Ausführungen zeigen deutlich, dass die Unternehmen und ihre IT-Abteilungen in absehbarer Zukunft nicht auf den Einsatz von Passwörtern verzichten können. Worauf Unternehmen ebenfalls nicht verzichten können, ist die maximal mögliche Sicherheit: Das gilt in verstärktem Maße nicht nur für die großen Enterprise-Unternehmen, sondern auch für die Firmen aus dem SMB-Umfeld. Passwörter brauchen maximale Sicherheit und sollten deshalb möglichst komplex sein. Dabei sollten jedoch der Einsatz und die Pflege der Passwörter eine minimale Komplexität bieten – der Umgang mit diesen Daten muss für die Nutzer möglichst einfach und trotzdem sicher sein.

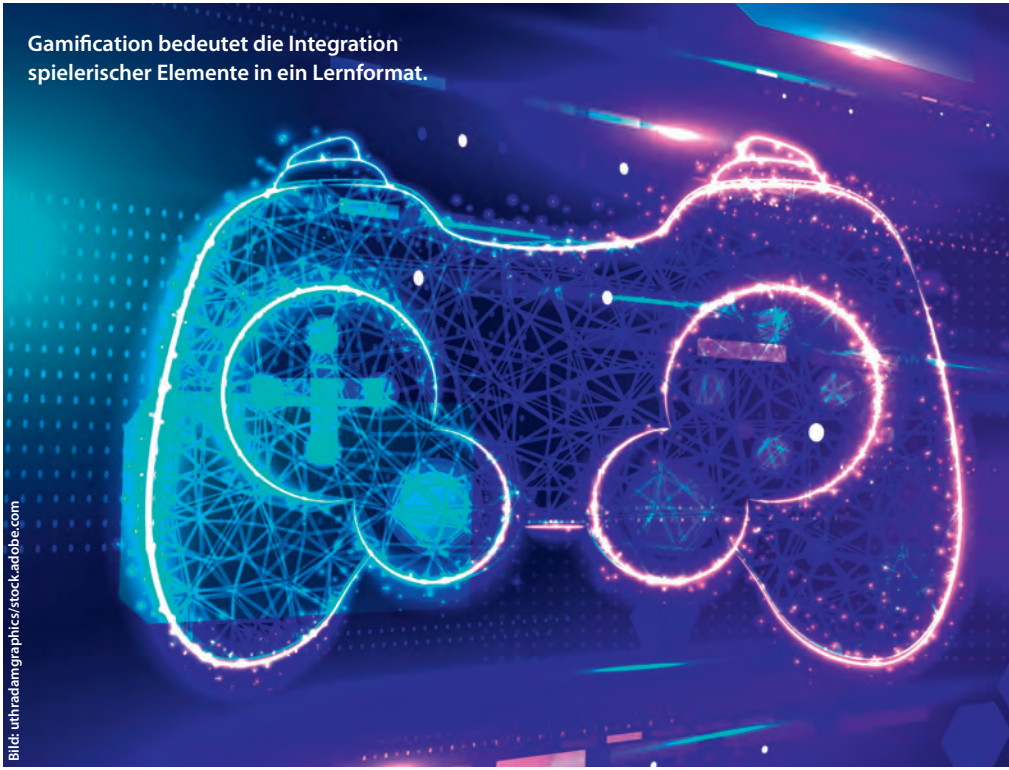
Was aber gerade diese Unternehmen nicht benötigen, ist ein noch höheres Level an Komplexität, wenn es um ihre IAM-Strategie geht. Passwort-Manager sind gerade für kleinere Unternehmen sehr gut dazu geeignet, die Probleme rund um diesen Bereich in den Griff zu bekommen. Dabei ist es besonders gut, wenn diese Software den kleinen Unternehmen die Möglichkeit bietet, auch als Lösung für SSO und PAM zu funktionieren. Kommt hingegen im Unternehmen bereits eine Lösung für SSO, zur 2-Faktor-Authentifizierung oder für PAM zum Einsatz, so kann ein moderner Business-Passwort-Manager problemlos mit diesen kombiniert werden.

Passwörter werden weder durch den Einsatz einer 2-Faktor-Authentifizierung noch durch die Verwendung eines Business-Passwort-Managers „zum alten Eisen“ oder gar obsolet: Sie werden besser, einfacher und vor allen Dingen sicherer verwendet und verwaltet. □

Nachhaltig lernen mit Gamification und Storytelling

Um Cyberattacken abzuwehren, braucht es heute mehr als nur Schutztechnologien. Aufmerksame Mitarbeitende können mit dem richtigen Verhalten Angriffsversuche via Phishing oder Social Engineering frühzeitig unterbinden. Mit Security-Awareness-Trainings lässt sich das Bewusstsein für Cyberrisiken in der Belegschaft verbessern. Moderne Schulungen setzen auf Gamification und Storytelling.

Von Christian Laber, G DATA



Gamification bedeutet die Integration spielerischer Elemente in ein Lernformat.

Bild: uthradamgraphics/stock.adobe.com

Können Sie sich noch an das Thema und an zentrale Inhalte ihrer letzten Fortbildung erinnern? Vielen Menschen geht es ähnlich wie den Eichhörnchen, die einige ihrer vergrabenen Wintervorräte schlicht vergessen. Gelerntes Wissen ist flüchtig. Ein Grund gerade bei Präsenzschulungen: vorherrschender Frontalunterricht, ohne Interaktivität und Praxisbezug.

Sicherlich denkt der eine oder die andere jetzt mit Grauen an die Schulzeit zurück. Was für Schüler:innen vielleicht undramatisch ist, weil die Inhalte im späteren Berufsleben keine entscheidende Rolle spielen, kann im Berufsleben weitreichende Konsequenzen haben. Wenn beispielsweise wichtige Lektionen der IT-Sicherheit nicht nachhaltig beim Lernenden haften bleiben, hat nicht nur er selbst, sondern auch sein Arbeitgeber ein größeres Problem.

Denn technologische Schutzmaßnahmen allein reichen nicht aus, um Unternehmen vor Cyberattacken zu schützen. Insbesondere mit Phishing-Mails umgehen Angreifer Schutzmechanismen und zielen direkt auf Anwender:innen. Die Erfolgschancen stark individualisierter Angriffe – sogenannte Spear-Phishing-Angriffe – sind deutlich höher als bei einem Massenangriff. Phisher nutzen gezielt perfide Tricks und verleiten Menschen zu Handlungen, welche sie naturgemäß sonst nie gemacht hätten.

Mittels Security-Awareness-Trainings wird die Aufmerksamkeit gegenüber digitalen Risiken erhöht. Auf diese Weise können Unternehmen sich und ihre Mitarbeitenden gegen diese Angriffsversuche wappnen. Das Ziel: die Sicherheit des Unternehmens, aber auch die persönliche Sicherheit im digitalen Zeitalter.

Nachhaltig fortbilden

Im Gegensatz zu fachlichen Fortbildungen für einzelne Abteilungen gilt für Security-Awareness-Trainings: Jede:r ist ein potenzielles Opfer und muss daher die Tricks der Cyberkriminellen kennen. Allerdings reicht es nicht aus, der Belegschaft einfach ein Youtube-Video mit den gängigsten und gefährlichsten Cyberrisiken zur Verfügung zu stellen. Der Lernerfolg ist hier vergleichbar mit dem vorhin schon kurz angesprochenen Frontalunterricht und geht daher gegen null. Die Gefahr, dass Mitarbeitende auf einen gefälschten Link klicken, bleibt dementsprechend hoch.

Doch wie wird Lernen nachhaltig? Die Antwort lautet: Durch intrinsische Motivation, also durch Tätigkeitsanreize, durch Spaß, durch Emotionalität und durch das Vermitteln des direkten Praxisbezugs, auch über den Arbeitskontext hinaus. Hinzu kommt der Wunsch nach kurzen Lerneinheiten, denn Lernzeit ist, ⇨

Bilder: G DATA

Beispiele für ein Security-Awareness-Training

vor allem in den Augen vieler Arbeitgeber, auch Arbeitszeit.

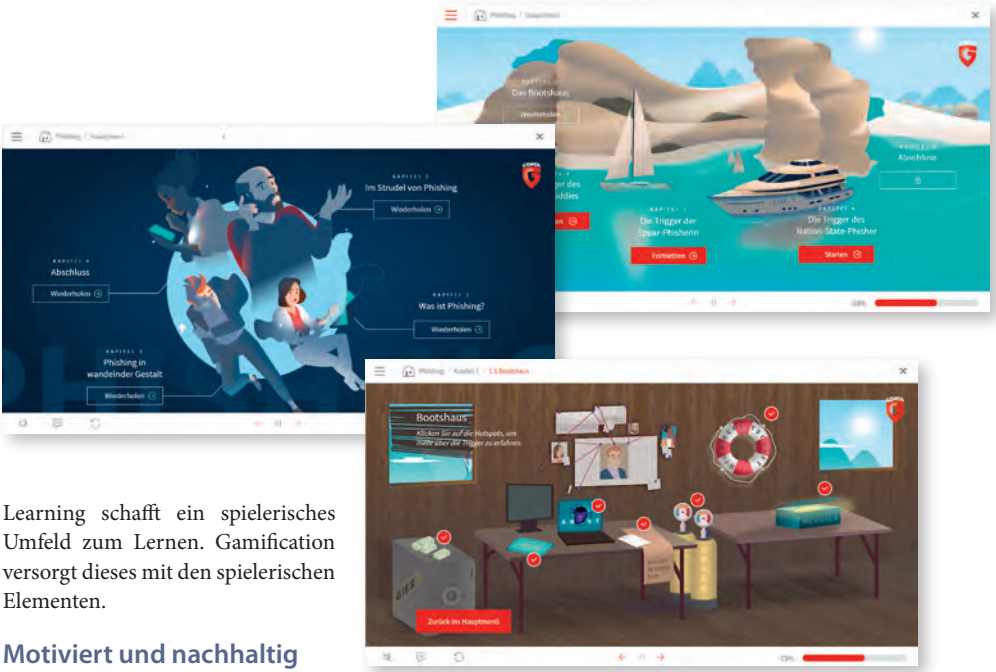
Eine entsprechend nachhaltige Lösung bieten eLearnings, die Teilnehmende zeit- und ortsunabhängig absolvieren können. Deren Standardportfolio besteht zum Großteil allerdings immer noch aus Videos und Multiple-Choice-Tests, ohne zu beachten, dass sich die Anforderungen der Lernenden und deren Lernverhalten stark verändert hat, im Vergleich zu vor einigen Jahren. Die Quintessenz: Um den „modernen" Lernenden auch wirklich emotional gedanklich abzuholen, müssen Formate ansprechend und innovativ gestaltet sein. Das führt zu der Frage, was moderne eLearnings auszeichnet. Was sorgt dafür, dass Lernende nachhaltig lernen und die Inhalte in ihrem Arbeitsalltag anwenden? Zwei Aspekte werden im Folgenden näher betrachtet: Storytelling und Gamification.

Gamification und Storytelling

Viele eLearnings folgen dem sogenannten Storytelling-Ansatz. Das Thema der Lerneinheit wird dabei mit einer passenden Geschichte verknüpft. Im Zuge des Storytellings kommen meistens speziell dafür geschaffene Charaktere zum Einsatz, sodass die Lernenden nicht nur durch eine erzählte Geschichte lernen, sondern das Gelernte auch an bereits vertraute Personen knüpfen können.

Entscheidend ist: Unser Gehirn unterscheidet nicht, ob wir etwas selbst erleben oder ein fiktiver Charakter. Deshalb speichern wir die Information auch so gut. Bei allen Vorteilen von Storytelling gilt insbesondere die Regel: „In der Kürze liegt die Würze." Lerneinheiten, die länger als zehn Minuten dauern, sorgen dafür, dass die Aufmerksamkeit ebenso wie der Spannungsbogen der Geschichte sinkt. Und damit auch der Lerneffekt. Daher sollten umfangreiche Themengebiete in mehrere Episoden aufgeteilt werden.

Starten wir beim zweiten Aspekt zunächst mit einer Begriffsklärung: Wenn die meisten Personen von „Gamification" sprechen, dann meinen sie „Game-based Learning". Game-based Learning überträgt teils trockenes und umfassendes Lernmaterial in ein spielerisches Format, welches zudem sehr interaktiv ist. Gamification meint also die Integration von spielerischen Elementen in ein bereits bestehendes Lernformat. Ein Beispiel dafür ist ein Belohnungssystem mit Punkten, die Teilnehmende sammeln, wenn sie Lernkapitel abschließen. Game-based



Learning schafft ein spielerisches Umfeld zum Lernen. Gamification versorgt dieses mit den spielerischen Elementen.

Motiviert und nachhaltig lernen mit Serious Games

Das Fazit: Moderne eLearnings setzen verstärkt auf gute Geschichten und spielerische Elemente mit dem Ziel, den Lerntransfer zu maximieren. So kommen beispielsweise in einer eigenen Lernwelt wie etwa einem Serious Game Gamification-Elemente (Schieberegler, Punktestand, Click-and-Reveal oder zeitgesteuerte Herausforderungen) zum Einsatz. Ein Rahmen mit einer Geschichte sorgt für positive Emotionen und Motivation. Ein klar vorgegebenes Ziel schafft eine hohe intrinsische Motivation während des gesamten Trainings. Die Lernenden halten den Fokus auf das zu lernende Thema und sind über die Dauer des Trainings hoch motiviert.

Übrigens: Untersuchungen geben den Methoden recht. „Normale“ eLearnings auf freiwilliger Basis haben eine ungefähre Abschlussquote von 25 Prozent. Serious Games von bis zu 90 Prozent. Die Lernenden bleiben durch Interaktionen, Emotionen und Sinn am Training dran, weil sie intrinsisch motiviert werden. Dadurch bleibt umgangssprachlich formuliert „mehr hängen“.

Mit Blick auf die IT-Sicherheit heißt das: Technologische Schutzmaßnahmen alleine sind unzureichend. Wenn Mitarbeitende verstehen, wie Cyberkriminelle agieren, bilden sie eine Human Firewall im Unternehmen und verhindern mit ihrem Verhalten, dass Angreifer ins Netzwerk gelangen. □

Der Autor

Christian Laber ist Head of E-Learning Development bei G DATA CyberDefense.

Impressum

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

Geschäftsführer:
Werner Nieberle (-100), Günter Schürger

IT-BUSINESS

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

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

Account Management:
Besa Agaj/International Accounts (-112),
Stephanie Steen (-211),
Hannah Lamotte (-193)
eMail media@vogel-it.de

SECURITY-INSIDER.DE

Redaktion: Peter Schmitz/ps (-165) – Chefredakteur, Jürgen Paukner/jp (-166) – CvD

Co-Publisher: Markus Späth (-138), Tobias Teske (-139)

Key Account Management: Brigitte Bonasera (-142)

Anzeigendisposition: Mihaela Mikolic (-204)

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

EBV: Carin Böhm, Brigitte Krimmer

Anzeigen-Layout: Johannes Rath

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

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

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

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

Inserenten

proTECTr

www.protectr.com

Cloud Verschlüsselung & Signaturen zusammen in einer App

Schützen Sie Vertraulichkeit und Echtheit Ihrer Daten

- ✓ Kostenfreie E2EE-Dateiverschlüsselung
- ✓ Einfache, fortgeschrittene und qualifizierte Signatur
- ✓ Integration in bestehende Systeme möglich
- ✓ Umfangreiche Roadmap

Die Evolution der Verschlüsselung

Skytale	***Chiffrierscheibe***	***One-time Pad***	***proTECTr***
500 vor Christi	*15. Jahrhundert*	*19. Jahrhundert*	*21. Jahrhundert*

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

procilon GROUP

NCP

SECURE COMMUNICATIONS

Zero Trust

Zunehmende Cyberbedrohungen, Mitarbeiter im Homeoffice und technologische Strategien von Cloud bis Zero Trust bereiten IT-Abteilungen Kopfschmerzen.

Nutzen Sie für Ihr Unternehmen die Vorteile von VPN, Cloud und High Security durch die NCP Secure Enterprise Lösung.

Vertrauen Sie der richtigen Technologie?

NCP SECURE COMMUNICATIONS my access

www.ncp-e.com

SecurITy made in Germany