OKTOBER 2021

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

MADE IN GERMANY

Powered by:

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

VOGEL IT MEDIEN

Eine Publikation von IT-BUSINESS SECURITY INSIDER


1ST IN CYBER DEFENSE
Vertrauen oder Verraten?
WIR SIND BEREIT.
gdata.de/vertrauen
Schutz der Privatsphäre, verantwortungsvoller Umgang mit Daten, keine Backdoors: IT-Sicherheitslösungen von G DATA entsprechen den strengen deutschen und europäischen Datenschutzstandards.
SecurITy made in Germany
CYBERSECURITY MADE IN EUROPE
GDATA
TRUST IN GERMAN SICHERHEIT

Wahl oder Qual?

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

Liebe Leserinnen und Leser,
die Digitalisierung in unserem Leben schreitet in allen Gebieten mit enormer Dynamik voran und verankert Informationstechnik in jedem Bereich des Alltags. Sie ist Treiber und Basis für das Wohlergehen unserer Gesellschaft in Deutschland.

Was im Kleinen gilt, hat auch im größeren politischen Rahmen Geltung, damit Europa und Deutschland im Besonderen eine Vorreiterrolle in IT-Sicherheit und Vertrauenswürdigkeit über die diesjährige Bundestagswahl hinaus einnehmen können.

Informationstechnik ist das Fundament der Digitalisierung. "Digitale Souveränität" ist eine entscheidende Vorbedingung für die Wettbewerbsfähigkeit Europas, gerade mit Blick auf den Betrieb kritischer Infrastrukturen. Darin liegt auch die Bedeutung von Vorhaben wie z.B. GAIA-X.

Generell beobachten wir einen Bewusstseinswandel – Digitalisierungsvorhaben werden heute und hoffentlich auch in Zukunft mit einem angemessenen Maß an IT-Sicherheit verbunden. IT-Sicherheit ist ein fortlaufender Prozess. Die Angriffsszenarien verändern sich sehr schnell. Wir empfehlen, die Sicherheitsanforderungen zu Beginn des Entwicklungsprozesses zu ermitteln und zu berücksichtigen. Wichtiges Ziel dabei ist es, spätere Aufwände zur Behebung von Sicherheitslücken zu verhindern oder zu minimieren. Aber natürlich verlangt IT-Sicherheit trotzdem regelmäßige Anpassungen, auch durch die Politik. Diese Änderungen sind zu interpretieren und umzusetzen; selbstverständlich ist diese nachhaltige Analyse der Umsetzungsstände regelmäßig durchzuführen.

Grundsätzlich ist der Staat für die Bereitstellung und Absicherung von für die Gesellschaft wichtigen Funktionen und Infrastrukturen verantwortlich. Dies frei und selbstbestimmt zu gestalten, gilt im allgemeinen politischen Sinne als Souveränität. Im Zuge der zunehmenden Komplexität der Infrastrukturen bedarf es einer intensiveren Zusammenarbeit von Politik, Verwaltung und Industrie, um diese Souveränität zu gewährleisten.

Die vorliegende Beilage vermittelt Einblicke in ausgewählte Themen, die uns als Bundesverband IT-Sicherheit derzeit beschäftigen. Die Beiträge zielen dabei auf grundsätzliche Fragen ab, mit denen Sie sich als IT-Verantwortliche befassen sollten: die digitale Transformation im Turbo, Homeschooling und Lösungen für den Mittelstand, Datenschutz und noch vieles mehr.

Als Bundesverband IT-Sicherheit wünschen wir uns entsprechende Schwerpunktsetzungen der Parteien auch nach der Wahl und werden weiterhin Wirtschaft, Verwaltung, Politik und Gesellschaft mit der Kompetenz eines interdisziplinären Netzwerkes mit Rat und Tat zur Seite stehen, um die bestmöglichen Technologien voranzubringen.

Die Herausforderungen nehmen für die kommende Bundesregierung zu. Dabei ist die mittelständisch geprägte deutsche IT-Sicherheitsbranche allerdings sehr gut aufgestellt und durch innovative Produkte, gepaart mit der starken deutschen bzw. europäischen Datenschutzgesetzgebung, international wettbewerbsfähig. "IT Security made in Germany" wird auch über das Jahr 2021 hinaus eine gute Wahl bleiben. □

Titelbild: © harvepino-stock.adobe.com (M) Carin Boehm

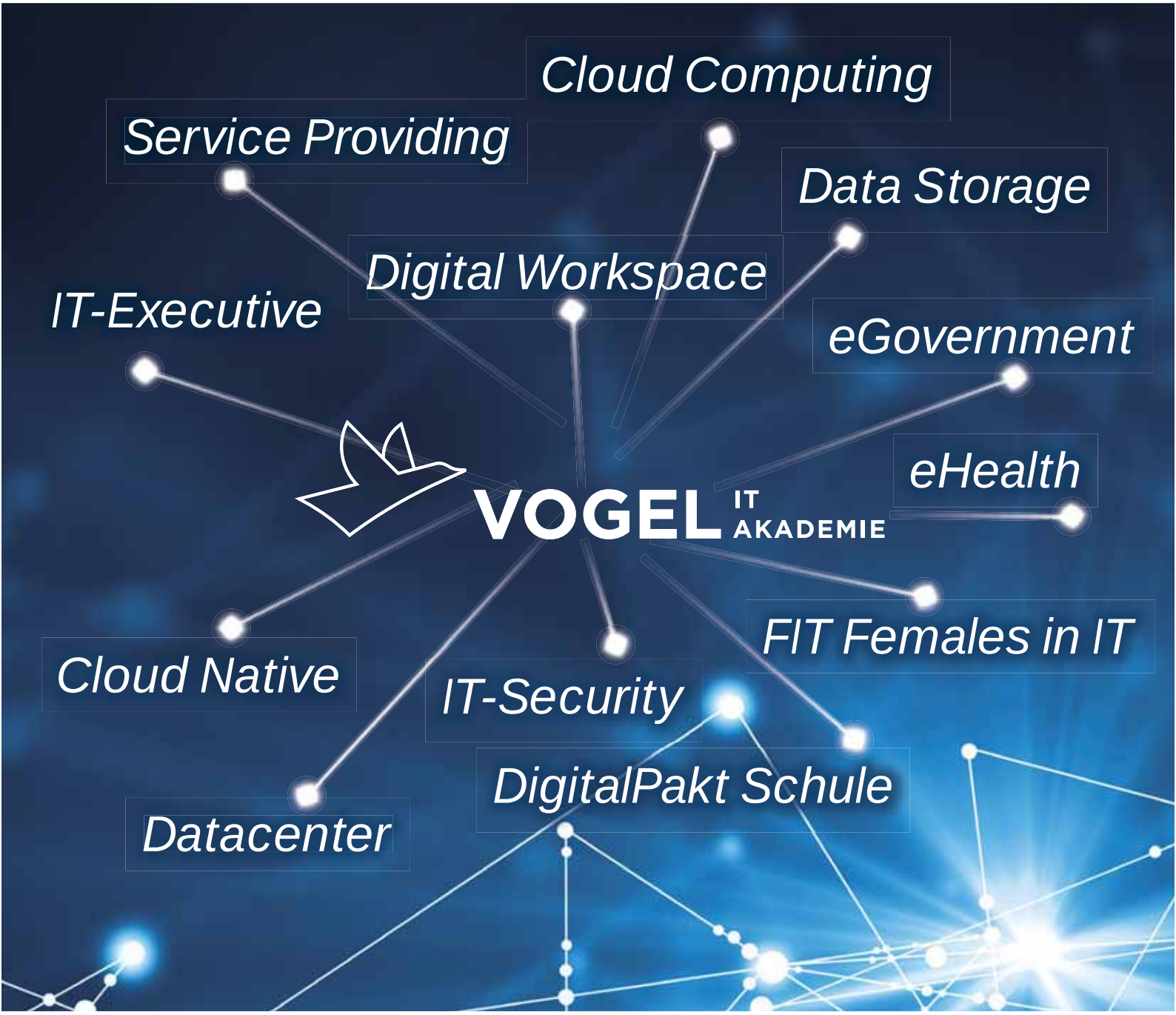
TeleTrusT-Initiative "IT Security made in Germany"

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

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

WE MATCH PEOPLE & TECHNOLOGY

VOGEL IT AKADEMIE



7.250
Teilnehmer p.a.

35
Events p.a.

461
Vorträge und Workshops p.a.

20+
Jahre Events vom Feinsten

Unsere Events – vor Ort, virtuell, hybrid.

Jetzt informieren: www.vogelitakademie.de

Vertrauen hat einen Namen

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

Von Dr. Holger Mühlbauer und Jürgen Paukner

Träger des Vertrauenszeichens "IT Security made in Germany" (Stand 20.09.2021)

- Accellence Technologies GmbH
- AceBIT GmbH
- achelos GmbH
- Achtwerk GmbH & Co. KG
- ads-tec GmbH
- akquinet enterprise solutions GmbH
- Allgeier IT Solutions GmbH
- ANMATHO AG
- Antago GmbH
- AOE GmbH
- apsec Applied Security GmbH
- ASOFTNET
- ATIS systems GmbH
- Atruvia AG
- AUTHADA GmbH
- Bank-Verlag GmbH
- Bechtle GmbH & Co. KG
- Beta Systems IAM Software AG
- Biteno GmbH
- Blue Frost Security GmbH
- Bosch CyberCompare
- Build38 GmbH
- Bundesdruckerei GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- certgate GmbH
- CERTIX IT-Security GmbH
- CGM Deutschland AG
- Cherry GmbH
- CHIFFRY GmbH
- Cloudsitter GmbH
- CoCoNet Computer-Communication Networks GmbH
- Cognitec Systems GmbH
- COGNITUM Software Team GmbH
- COMback Holding GmbH
- comcrypto GmbH
- comforte AG
- Communisystems-Care 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
- dhpg IT-Services GmbH Wirtschaftsprüfungsgesellschaft
- Digital Enabling GmbH
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- dinext. pi-sec GmbH
- ditis Systeme Niederlassung der JMV GmbH & Co.
- DocRAID(R) - professional data privacy protection
- DoctorBox GmbH
- DRACOON GmbH
- DriveLock SE
- D-Trust GmbH
- e-ito Technology Services GmbH
- eCom Service IT GmbH
- ecsec GmbH
- Enginsight GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- essentry GmbH
- exceet Secure Solutions GmbH
- floragunn GmbH
- FSP GmbH
- FZI Forschungszentrum Informatik
- GBS Europa GmbH
- G DATA CyberDefense AG
- genua GmbH
- glacier advisory & coaching
- GORISCON GmbH
- Hanko GmbH
- HiScout GmbH
- HK2 Rechtsanwälte
- Hornetsecurity GmbH
- Huf Secure Mobile GmbH
- IDEE GmbH
- if(is) - Institut für Internet-Sicherheit
- Infineon Technologies AG
- INFODAS GmbH
- Inlab Networks GmbH
- innovaphone AG
- INSYS Microelectronics GmbH
- intelliCard Labs GmbH
- Intelligent Minds UG
- IoT Inspector GmbH
- IS4IT Kritis GmbH
- isits AG International School of IT Security
- ISL Internet Sicherheitslösungen GmbH
- ITConcepts PSO 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/ □

- ITSG GmbH
- itWatch GmbH
- Johannes Kresse
- keepbit IT-SOLUTIONS GmbH
- KikuSema GmbH
- KnowledgeRiver GmbH
- LANCOM Systems 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
- M&H IT-Security GmbH
- MTG AG
- MTRIX GmbH
- NCP engineering GmbH
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- NETZWERK Software GmbH
- Nexis GmbH
- nicos AG
- nicos cyber defense GmbH
- Nimbus Technologieberatung GmbH
- OctoGate IT Security Systems GmbH
- ondeso GmbH
- OPTIMA Business Information Technology GmbH
- OTARIS Interactive Services GmbH
- pen.sec AG
- PFALZKOM GmbH
- PHOENIX CONTACT Cyber Security GmbH
- PHYSEC GmbH
- Pix Software GmbH
- PPI Cyber GmbH
- PRESENSE Technologies GmbH
- procilon GmbH
- Protforce GmbH
- PSW GROUP GmbH & Co. KG
- Pyramid Computer GmbH
- QGroup GmbH
- QuoIntelligence GmbH
- retarus GmbH
- Rhebo GmbH
- RheinByteSystems 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
- secucloud GmbH
- SECUDOS GmbH
- secunet Security Networks AG
- Secure Service Provision GmbH
- Securepoint GmbH
- secuvera GmbH
- SerNet GmbH
- signotec GmbH
- SL.IS Services GmbH
- Smartify IT Solutions GmbH
- Softline AG
- SoSafe GmbH
- SRC Security Research & Consulting GmbH
- Steen Harbach AG
- Steganos Software GmbH
- SVA System Vertrieb Alexander GmbH
- Symlink GmbH
- syracom consulting AG
- TDT AG
- TE-SYSTEMS GmbH
- teamwire GmbH
- Tenzir GmbH
- TESIS SYSware Software Entwicklung GmbH
- TG alpha GmbH
- TMB Service GmbH
- Trufflepig IT-Forensics GmbH
- TrustCerts GmbH
- TÜV Informationstechnik GmbH
- TÜV Rheinland i-sec GmbH
- TWINSOFT biometrics GmbH & Co. KG
- Uniki GmbH
- Uniscon GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- Veronym Holding GmbH
- virtual solution AG
- VisionmaxX GmbH
- Vulidity GmbH
- WMC Wüpper Management Consulting GmbH
- Würzburger Versorgungs- und Verkehrs GmbH
- XignSys GmbH
- XnetSolutions KG
- Zertificon Solutions GmbH

SECUREPOINT

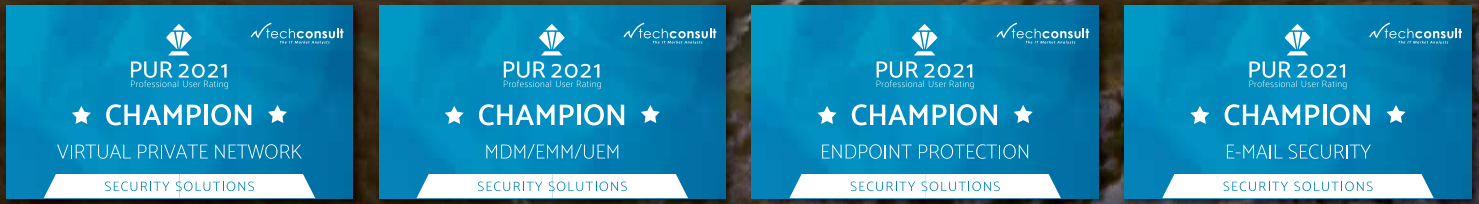
MEHR SICHERHEIT
MEHR ERREICHEN

Vertrauen durch Technik und Expertise.

Helm, Gurt, Haken, Check: Sicherheit entsteht, wenn man an alles gedacht hat. Securepoint Unified Security setzt dies für die IT-Sicherheit von Unternehmen um. Mit Firewalls, Virenscannern, Mobile Device Management und weiteren Sicherheitslösungen made in Germany.

Securepoint Unified Security

IT-Sicherheit aus ganzheitlicher Perspektive.



www.securepoint.de • Tel.: 04131 240 10 • info@securepoint.de

Startimpulse zur digitalen Souveränität gefordert

Deutschland und Europa müssen angemessen und souverän die digitale Zukunft gestalten können. Um das zu erreichen, hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) in der IT-Sicherheits-Agenda 2029 wichtige und dringende Forderungen aufgestellt.

Von Peter Schmitz, Security-Insider

Bild: vectorfusionart/stock.adobe.com

Deutschland und Europa müssen ihre Konkurrenzfähigkeit gegenüber anderen Regionen neu erlangen und erhalten, um weitestgehend unabhängig ihre digitale Zukunft gestalten zu können.

Digitalisierung und Vernetzung der Wirtschaft, Verwaltung und Kritischen Infrastrukturen bieten Unternehmen gute Chancen, ihr Know-how in neue Technologien und Dienstleistungen umzusetzen. Der Staat ist für die Rahmenbedingungen der Bereitstellung und Absicherung von für die Gesellschaft wichtigen Funktionen und Infrastrukturen verantwortlich. Im Zuge der zunehmenden Komplexität der Infrastrukturen bedarf es einer intensiven Zusammenarbeit von Politik, Verwaltung, Forschung und Industrie, um die technologische und digitale Souveränität herzustellen oder zu gewährleisten.

Der Staat ist gefordert

Technologische und digitale Souveränität kann nur durch ein zielgerichtetes und langfristiges Vorgehen erfolgreich umgesetzt werden. Derzeit existieren zu viele Einzelinitiativen, die kaum Wirkung zeigen. Es bedarf einer Umsetzungsstrategie, die Ziele definiert, Maßnahmen priorisiert und festlegt sowie eine Aufgabenverteilung zwischen Politik, Verwaltung, Hersteller- und Anwendungsunternehmen und Forschung vornimmt. Die Politik ist aufgerufen, den Startimpuls für die Umsetzungsstrategie zu setzen und sie langfristig zu unterstützen. Andere Staaten verfolgen bereits konsequent entsprechende Umsetzungspläne. Demzufolge müssen Deutschland und Europa ihre Konkurrenzfähigkeit gegenüber anderen Regionen neu erlangen und erhalten, um weitestgehend unabhängig die digitale Zukunft gestalten zu können.

Forderungen der IT-Sicherheitsagenda 2029 von TeleTrusT

Dazu hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) seine "IT-Sicherheitsagenda 2029" mit sechs zentralen Forderungen veröffentlicht (www.teletrust.de/teletrust-it-sicherheitsagenda/):

1. Klares Bekenntnis zu unbeschränkter IT-Sicherheit
2. Technologische Souveränität im Bereich IT-Sicherheit schaffen – für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft
3. Auf- und Ausbau von IT-Sicherheitsinfrastrukturen für Bürger, Unternehmen und Verwaltung fordern und fördern
4. Mehr IT-Sicherheitstechnologie "Made in Germany" in der Praxis
5. Verbot der Kompromittierung von IT-Sicherheit, keine Backdoors, Staatstrojaner oder geschwächte Verschlüsselung
6. Europäische IT-Sicherheitsgesetze für eine erhöhte Rechts- und Investitionssicherheit – klar, konsolidiert und agil.

TeleTrusT-Vorstandsvorsitzender Prof. Dr. Norbert Pohlmann: "Die IT-Sicherheitsprobleme und daraus resultierende Schäden nehmen stetig zu. Vor vier Jahren mit 50 Milliarden Euro beziffert, über 100 Milliarden Euro vor zwei Jahren, betragen sie mittlerweile mehr als 220 Milliarden Euro. Die neue Bundesregierung muss auf allen Ebenen und gemeinsam mit den relevanten Stakeholdern dafür sorgen, dass diese Schäden deutlich vermindert werden. Denn nur so erreichen wir das Ziel, eine souveräne, sichere und vertrauenswürdige digitale Zukunft zu schaffen."

RA Karsten U. Bartels LL.M., stellvertretender TeleTrusT-Vorstandsvorsitzender: "Wenn wir eine technologische und digitale Souveränität Deutschlands und Europas wollen, muss die Politik in den nächsten zwei Legislaturperioden die IT-Sicherheit massiv stärken. Unsere sechs Kernforderungen stellen zusammen, was dazu erforderlich ist: der Staat hat IT-Sicherheit aktiv zu fördern und nicht zu kompromittieren. Das betrifft auch das Recht auf Verschlüsselung ohne staatliche Hintertüren. IT-Sicherheitsinfrastrukturen sind so auszubauen und vom Staat selbst zu nutzen, dass sie im privaten und geschäftlichen Alltag ankommen." □

R&S®Trusted Gate: Rechtssicher in der Cloud arbeiten

Für Unternehmen und Behörden steigt die Herausforderung, US-amerikanische Cloud-Dienste gemäß den Vorgaben der EU-DSGVO einzusetzen. In einem neuen Rechtsgutachten analysiert Prof. Dr. Heckmann von der TU München das Schrems-II-Urteil, seine Auswirkungen für die Nutzung von Public-Cloud-Diensten und inwiefern die Cloud-Sicherheitslösung R&S®Trusted Gate des IT-Sicherheitsexperten Rohde & Schwarz Cybersecurity einen Ausweg aus dem derzeitigen Cloud-Dilemma darstellt.

ROHDE&SCHWARZ

Deutsche Unternehmen und Behörden nutzen für das Cloud-Computing überwiegend Anwendungen, Dienste und Services von US-amerikanischen Anbietern wie Microsoft, Google oder Amazon. Denn diese verfügen über eine hohe Funktionalität und Skalierbarkeit. Seit dem 16. Juli 2020 herrscht jedoch große Unsicherheit, inwiefern der Einsatz solcher Cloud-Dienste datenschutzrechtlich überhaupt noch möglich ist. Denn an diesem Tag hat der Europäische Gerichtshof das Datenschutzabkommen zwischen USA und EU „Privacy Shield“ für ungültig erklärt. Eine neue Regelung, die für Rechtssicherheit sorgt, lässt seither auf sich warten.

Enormes Risiko durch Cloud-Nutzung

Nach Auffassung des Europäischen Datenschutzausschusses (EDSA) besteht im Cloud-Computing derzeit kein zulässiger Weg für die Datenübermittlung in die USA. Europäische Unternehmen und Behörden gehen bei der Nutzung US-amerikanischer Cloud-Dienste daher ein enormes Risiko ein. Gegen deutsche Firmen, die die Dienste dennoch einsetzen, sind Bußgelder von bis zu 20 Millionen Euro möglich.

Für Unternehmen und Behörden besteht die Herausforderung deshalb darin, die gesetzlichen Vorgaben einzuhalten. Denn die Nutzung von Cloud-Diensten ist heute nicht mehr nur eine hilfreiche Ergänzung, sondern dringend erforderlich. Sie ermöglichen den flexiblen und weltweiten Datenzugriff innerhalb der Unternehmen – vor allem auch in Zeiten von Homeoffice und Remote Work ist die Bedeutung von Cloud-Diensten immens gestiegen.

R&S®Trusted Gate: Der Ausweg aus dem Cloud-Dilemma

In einem aktuellen Rechtsgutachten analysiert Prof. Dr. Heckmann von der TU München, wie die Cloud-Sicherheitslösung R&S®Trusted Gate einen Ausweg aus dem Cloud-Dilemma darstellt. Laut dieses Gutachtens bietet R&S®Trusted Gate Unternehmen und Behörden die Möglichkeit, die Herrschaft über ihre Daten zu behalten und die Anforderungen der EU-DSGVO in ihrer eigenen IT-Umgebung zu erfüllen. Dass diese Trennung auf technisch sichere Weise gelingt, garantiere der Hersteller Rohde & Schwarz Cybersecurity glaubhaft gegenüber seinen Kunden, so Heckmann. Rohde & Schwarz ist ein geheimschutzbetreutes Unternehmen und darf damit auch Informationen, mit der Einstufung „Verschlusssachen“ bearbeiten.

Die Besonderheit der Lösung liege laut Heckmann in der sicheren Gestaltung eines Mehrebenensystems: Danach werden die personenbezogenen Inhalte der Verschlüsselungsebene von den Cloud-Diensten auf der Geschäftsebene getrennt. Auf diese Weise können die Vorteile der externen Cloud-Dienste genutzt werden, ohne dass personenbezogene Daten in ein „unsicheres Drittland“ übermittelt werden. Die Unternehmen und Behörden behalten die Datenherrschaft und erfüllen die Anforderungen der EU-DSGVO.

Daten entkoppeln

Das Gutachten beurteilt zwar den Einsatz der Lösung vor dem Hintergrund der EU-DSGVO. Das Konzept der Entkopplung von Daten aus der Cloud ermöglicht jedoch auch das Einhalten von Datenschutzverordnungen anderer Länder. Eine solche Cloud-Lösung kann daher weltweit eingesetzt werden, um die eigenen Daten für ausgewählte Regionen zu entkoppeln und lokal zu speichern.

R&S®Trusted Gate lässt sich nahtlos in Storage-Systeme gängiger Public Clouds wie Microsoft Azure, Google, AWS und Collaboration-Tools wie Microsoft 365 oder SharePoint einbinden und gesetzliche Vorgaben sowie Compliance-Regeln können auch in globalen Cloud-Umgebungen problemlos umgesetzt werden. Dabei läuft die Lösung transparent in bestehenden Anwendungen, sodass Arbeitsabläufe unverändert bleiben. ■

Vermitteln Sie den Wert von IT-Sicherheit!

Egal in welcher Position oder Abteilung: Budgets und zeitliche Ressourcen sind heiß umkämpft. Nicht den leichtesten Stand haben in diesem Zusammenhang präventive Maßnahmen wie Security-Awareness oder Mitarbeiter-Trainings. Um das Thema dennoch als Business Case in der Führungsebene zu platzieren, können CISOs und IT-Sicherheitsverantwortliche auf Anleihen des Change-Managements zurückgreifen.

Von Dr. Niklas Hellemann, SoSafe

Cyberangriffe gehören mittlerweile zu den größten Betriebsrisiken. Zehntausende deutsche Unternehmen waren etwa von den Hackerangriffen auf Microsoft betroffen, ebenso wurden Abgeordnete des Bundestages von Cyberkriminellen attackiert. Mit Blick auf den aktuellen Stand der IT-Sicherheit in Organisationen ist es allerdings nicht überraschend, dass Cyberkriminelle immer wieder Einfallstore finden. Im besonderen Fokus steht der Faktor Mensch, denn hier starten 90 Prozent aller Cyberangriffe.

Bild: contrastwerkstatt/stock.adobe.com

Mit Prinzipien des Change-Managements argumentieren Sicherheitsverantwortliche überzeugender.

Sicherheitsverantwortliche wissen längst um diese prekäre Situation und sehen gerade in der aktuellen Lage Nachholbedarf. Das zeigen zum Beispiel die Analysen im SoSafe „Human Risk Review 2021“. Der Großteil der befragten IT-Sicherheitsexperten (57,1 Prozent) möchte seine Bestrebungen im Bereich der Mitarbeitersensibilisierung zukünftig steigern.

Dem Präventionsparadoxon trotzen …

Andererseits hat das Thema IT-Sicherheit generell keinen leichten Stand innerhalb der Gesamt-

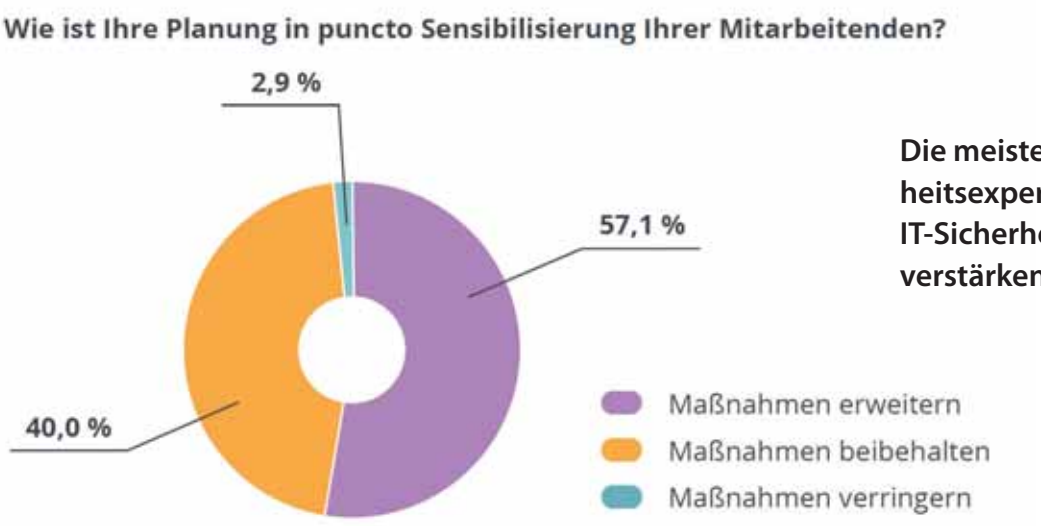


Bild: SoSafe Human Risk Review 2021

Die meisten IT-Sicherheitsexperten möchten IT-Sicherheitsmaßnahmen verstärken.

IT-Budgetierung. So verteilen Firmen weltweit nur circa sechs Prozent ihrer IT-Ausgaben auf Maßnahmen zur Steigerung der IT-Sicherheit, wie das Research-Unternehmen Gartner berichtet.

Ein Grund dafür: IT-Sicherheit schafft vermeintlich wenig Mehrwert. Und haben Maßnahmen einen Effekt, tritt das unerwünschte Ereignis nicht oder mit verringerter Häufigkeit ein. Eine Problematik, die wir in der Pandemie auch unter dem Namen „Präventionsparadox" sehr gut kennengelernt haben. Dennoch helfen Maßnahmen der IT-Sicherheit gerade in den aktuell herausfordernden Zeiten, Risiken zu minimieren. Sie verringern die Wahrscheinlichkeit für kostspielige Angriffe und sichern damit Wertschöpfung – und nicht zuletzt Arbeitsplätze.

… und Mehrwerte klar vermitteln

Um diese Mehrwerte auch klar allen Stakeholder-Gruppen zu vermitteln, kann es hilfreich sein, auf Prinzipien aus dem Change-Management zu schauen und so die Notwendigkeit für Investments zu verdeutlichen.

Die folgenden drei Schritte schaffen dabei eine gute Basis für eine klare Argumentation:

1. Risiken quantifizieren – oder: einen „Sense of urgency" etablieren

Aus dem Change-Management wissen wir: Um Menschen für eine Sache zu gewinnen oder zu einer Änderung zu bewegen, ist es wichtig, ihre Sprache zu sprechen und persönliche Relevanz zu erzeugen. Change-Experten sprechen vom „Sense of Urgency". Übertragen auf die Welt der Budgets und Business Cases bedeutet dies, die Größe des Problems quantitativ aufzuzeigen. Und die quantitativen Dimensionen sind enorm: So verursachten Cyberangriffe bereits 2019 allein in Deutschland einen Schaden von mehr als 100 Milliarden Euro.

Doch gerade sehr hohe Zahlen können ihren Effekt verlieren, wenn sie zu groß sind und damit sehr abstrakt bleiben. Dass Cybercrime äußerst kostspielig ist, ist letztlich auch durch die Berichterstattung in der Presse vielen Menschen bekannt. Daher ist es wichtig, hier Zahlen heranzuziehen, die eine möglichst hohe Relevanz für das eigene Unternehmen haben. Welche Cyberangriffe auf branchenverwandte Firmen oder Wettbewerber gab es zuletzt? Welche Folgen hatten diese? Wettbewerber, die bereits Cyberangriffen ausgesetzt waren, sind oftmals schnell zu finden. Vielleicht war sogar ⇨

INSYS icom – in kritischen Infrastrukturen zuhause

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.

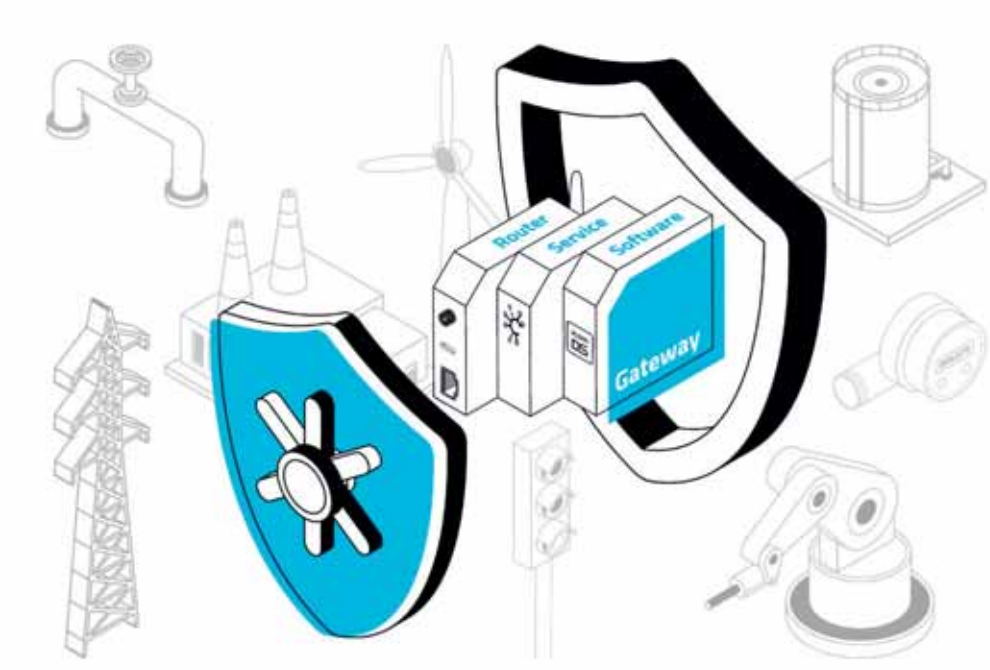
Zu Beginn dieses Jahres verschafften sich Hacker Zugang zu einer Wasseraufbereitungsanlage in einer Stadt in Florida. Dort versuchten sie, den Natriumhydroxid-Gehalt im System von den üblichen 100 Teilen pro Million (ppm) auf über 11.000 ppm zu erhöhen. Ein derartiger Anstieg hätte ernste gesundheitliche Folgen für alle haben können, die das Wasser getrunken hätten. Zum Glück wurde der Angriff sofort bemerkt und abgewehrt.

Die Cyberattacke zeigt deutlich: Gerade im Industrial Internet of Things (IIoT) lauern viele Gefahren, die Unternehmen und Infrastrukturbetreiber kennen und vor allem abwehren müssen. Einer Studie von Juniper Research zufolge wird die weltweite Anzahl der industriellen IoT-Verbindungen von 17,7 Milliarden im Jahr 2020 auf 36,8 Milliarden im Jahr 2025 ansteigen. Dadurch werden auch Angriffe auf diese Verbindungen immer häufiger.

Dabei sind die Absichten von Angreifern unterschiedlich. Die meisten Hacker wollen Geld erpressen, indem sie beispielsweise die Produktion von Unternehmen lahmlegen. Sie heben die Blockade dann erst gegen Bezahlung wieder auf. Aber auch der Diebstahl von geschäftskritischen Informationen und Know-how oder eine politische Motivation können hinter Angriffen stecken.

Geschützte Datenkommunikation mit INSYS icom

Lösungen von INSYS icom sind für Cyberattacken im IIoT bestens gerüstet. Wir sind Digitalisierungsexperten für industrielle Datenkommunikation und schlagen mit unseren Routern, Managed Services und Software die sichere Brücke zwischen IT und OT. Unsere Spezialisten verfügen über knapp 30 Jahre Erfahrung in den Bereichen Fernwartung, Fernsteuerung, Überwachung von



Zuständen und Vernetzung von Daten und unsere Lösungen sind „Made in Germany“. Die Hard- und Software entwickeln wir in unserem Hauptsitz in Regensburg. Unsere Lösungen entsprechen hohen industriellen Anforderungen in Bezug auf Langlebigkeit, Performance und IT-Sicherheit. Wir beziehen kritische Bauteile ausschließlich aus vertrauenswürdigen Quellen und setzen bei unseren Routern auf das eigenentwickelte, gehärtete Betriebssystem icom OS. Bei Angriffen auf Ihre Systeme können außerdem nach unterschiedlichen Kriterien Alarme abgesetzt werden und wir bieten verschiedene Managed Services an, um für zusätzliche Sicherheit zu sorgen. Dazu zählt zum einen die icom Connectivity Suite – VPN, eine sichere VPN-Verbindung für Wartung, Steuerung und Datenerfassung von Geräten weltweit. Diese wird ausschließlich in ISO27001-zertifizierten Datacentern gehostet. Zum anderen ermöglicht das icom Router Management den sicheren Zugriff auf die Router aus der Ferne. So wird das Gerätemanagement sowie Rollouts von Firmware, Konfigurationen und Sicherheitszertifikaten – inklusive Protokollierung – skalierbar und einfach. Des Weiteren lassen wir regelmäßig die IT-Sicherheit unserer Produkte durch Penetration-Tests und Widerstandsanalysen validieren.

Stimme aus der Praxis: BayWa r.e. AG

Aufgrund dieser Faktoren vertrauen hunderte Einrichtungen aus kritischen Infrastrukturen (KRITIS) auf unsere Geräte und Services. Die BayWa r.e. AG zum Beispiel plant, baut und betreibt Windparks und PV-Anlagen auf der ganzen Welt und setzt die Router von INSYS icom bereits seit mehreren Jahren ein. „Wir arbeiten ausschließlich mit Routern in Industriequalität, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für einen hohen Schutzstandard getestet wurden“, sagt Mohamed Harrou, Global Head of SCADA bei der BayWa r.e. Data Services GmbH. „Die Firewall der Router von INSYS icom konnte in unserer Anwendung alle acht Sekunden einen Cyberangriff abwehren und bietet daher einen hervorragenden Schutz vor Hackerangriffen.“

Mehr Informationen über IT-Sicherheit und INSYS icom finden Sie unter:
insys-icom.de/it-sicherheit ■

die eigene Organisation schon betroffen, denn: Laut einer Bitkom-Studie sind bereits 2018 und 2019 75 Prozent aller Organisationen Opfer von Cyberangriffen geworden. Mit einem Fokus auf Vergleichbarkeit stellen IT-Verantwortliche die Bedrohungslage und die damit einhergehende Dringlichkeit der Sicherheitsmaßnahmen besonders greifbar heraus.

2. Risiken greifbar machen – oder: „Uns kann es ja nicht treffen"

Kosten, die nur zu einer gewissen Wahrscheinlichkeit in der Zukunft aufkommen, erscheinen uns als weniger wichtig. Und wenn wir zur Vermeidung auch noch Aufwand betreiben müssen, schieben wir das Problem lieber „auf die lange Bank". Natürlich wissen wir, dass wir Sport treiben sollten, um die Wahrscheinlichkeit einer künftigen Krankheit zu reduzieren, aber der negative Effekt ist ja gefühlt auch noch sehr weit weg.

Für den Bereich der IT-Sicherheit heißt das: Probleme diagnostizieren und die konkrete Bedrohungslage beziffern. Im Fall von Mitarbeitersensibilisierungen führen zahlreiche Firmen beispielsweise Angriffssimulationen wie simulierte Phishing-Angriffe durch. Denn die resultierenden KPIs, wie Klick- oder Melderaten, sind sehr greifbare Werte für die Bedrohung des Unternehmens. Zudem erschließen sie sich auch nicht-technischen Stakeholdern. Wenn circa 40 Prozent der Mitarbeitenden auf eine echte Phishing-Mail klicken würden, ist auch Geschäftsführern klar, dass die Zeit zum Handeln gekommen ist.

3. Risiken minimieren – oder: „Return on Security Invest ableiten"

Hat man das spezifische Risiko für das eigene Unternehmen quantifiziert, ist der nächste logische Schritt die Reduktion. Für menschenbasierte Angriffe bedeutet dies: kontinuierliche Schulungen und Sensibilisierungsmaßnahmen. In der Vergangenheit wurde in diesem Bereich häufig in Richtung „Compliance" oder Pflichtmaßnahmen argumentiert. Auch heute ist die Erfüllung gesetzlicher Pflichten ein wichtiges Argument bei der Umsetzung von Security

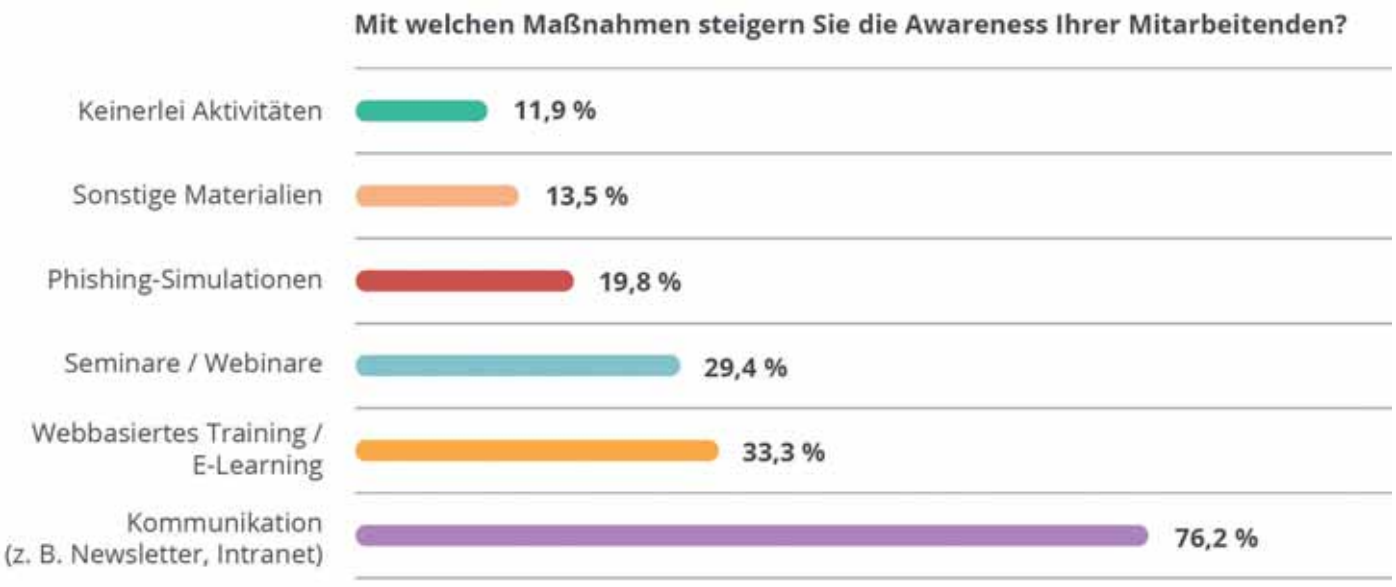


Bild: SoSafe Human Risk Review 2021

Der Großteil der IT-Sicherheitsexperten kommuniziert die Gefahren mit den Mitarbeitenden. Aktive und dauerhafte Awareness-Maßnahmen werden seltener ergriffen.

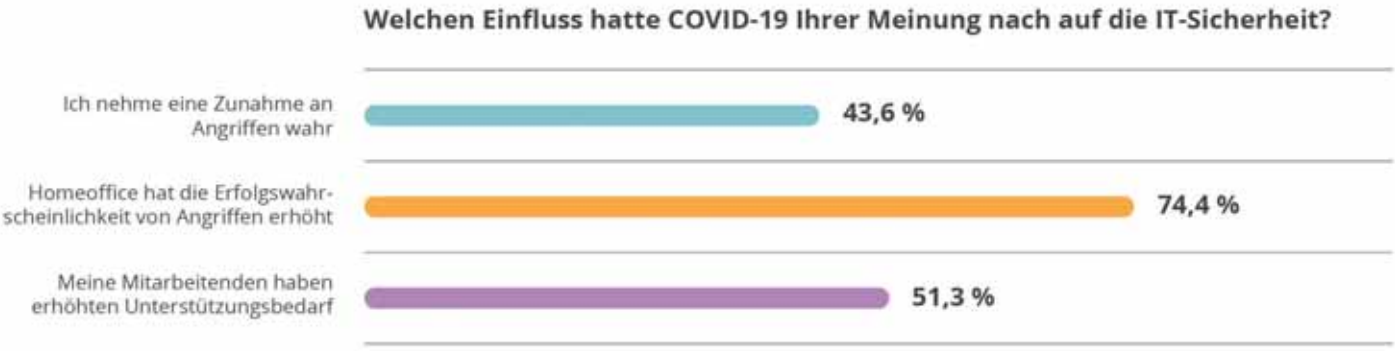


Bild: SoSafe Human Risk Review 2021

Corona und Homeoffice haben die Wahrscheinlichkeit von erfolgreichen Cyberangriffen erhöht.

Awareness. So schreibt die Datenschutzgrundverordnung (DSGVO) eine laufende Schulung von Mitarbeitenden vor. Die ISO-27001 geht sogar noch einen Schritt weiter und verlangt „Social Engineering-Simulationen".

Noch tragfähiger für die Budgetgewinnung als regulatorische Pflichten ist es aber, mit konkreten Mehrwerten im Sinne eines „Return on Invests" zu argumentieren. Aufbauend auf den genannten KPIs aus Angriffssimulationen lässt sich eine Reduktion der Phishing-Klickrate unmittelbar in eine Absenkung des monetären Risikos übersetzen. Zur Veranschaulichung nutzen wir ein Rechenbeispiel mit folgenden Annahmen.

ROI anhand eines einfachen Rechenbeispiels

- Der hypothetische Schaden durch einen erfolgreichen Cyberangriff könnte gut sechs Millionen Euro betragen (wie eine Studie des Bitkom-Verbandes für ein mittelgroßes Unternehmen schätzt).
- Rund neun von zehn erfolgreichen Angriffen starten über den Faktor Mensch – beispielsweise per Phishing-Mail.
- 75 Prozent aller Unternehmen wurden in den vergangenen zwei Jahren nachweislich mindestens einmal angegriffen. Vermutlich liegt die tatsächliche Zahl wesentlich höher; zudem berichtet das Sicherheitsunternehmen Crowdstrike, dass 68 Prozent aller von einer Attacke getroffenen Unternehmen, in den folgenden zwölf Monaten erneut angegriffen werden.

In diesem Fall könnte man durch die bloße Absenkung der Phishing-Klickrate von 40 Prozent um zehn Prozentpunkte eine Kostenersparnis von gut 200.000 Euro Kostenrisiko pro Jahr erreichen – wobei es sich dabei noch um eine konservative Rechnung handelt. So sehen wir mögliche Reduktionen von über zwei Drittel bei der Klickrate durch den Einsatz von Awareness-Maßnahmen.

Und selbst wenn dies ein Spiel mit statistischen Wahrscheinlichkeiten ist, steht der konkret zu beziffernde Mehrwert wesentlich kleineren Kosten gegenüber – was Budgetdiskussionen dann ein gutes Stück entspannter werden lässt. □

Der Autor

Bild: SoSafe

Dr. Niklas Hellemann ist Diplom-Psychologe, langjähriger Unternehmensberater und Geschäftsführer der Firma SoSafe Cyber Security Awareness.

Nachweisbare IT-Sicherheit testen, aber wie?

Nach einer BITKOM-Studie hat sich der Schaden für die deutsche Wirtschaft durch Cyberkriminalität im Jahr 2020 auf 223 Milliarden Euro mehr als verdoppelt. 88 Prozent der Unternehmen seien von Cyber-Angriffen betroffen gewesen. Im Bereich kritischer Infrastrukturen wird mit einer erhöhten Bedrohung gerechnet. Somit rückt der Wert von Cybersicherheit immer stärker in den Fokus. Ein wichtiger Sicherheitsanker ist die Überprüfung der Konfiguration und der verwendeten Komponenten im Protokoll-Umfeld von **TLS und IKE/IPsec**. Diese Protokolle bilden das Rückgrat der sicheren Kommunikation im Netzwerk und damit das Fundament für die darüber kommunizierenden Applikationen.

Nach welchen Kriterien sollte die Prüfung erfolgen?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) setzt in verschiedenen Bereichen über Technische Richtlinien Standards für die Einschätzung von Sicherheitsmerkmalen. An dieser Stelle beleuchten wir zwei Technische Richtlinien. Mit der **TR-03116-4** richtet sich das BSI direkt an

Heinfried Cznottka
Seit 2017 Director Security Solutions bei achelos, Referent und langjähriger Experte für Sicherheit in der digitalen Welt

achelos

Diensteanbieter für den sicheren Betrieb von Web-Diensten und fixiert in der dazugehörigen Checkliste relevante Parameter. In der **TR-03116-3** sind die Kriterien für den **sicheren Betrieb der Smart-Metering-Infrastruktur** definiert.
Zudem liefert der weltweite Kriterienkatalog für IT-Sicherheit – **Common Criteria** – messbare Vorgaben für sicherheitsrelevante Applikationen und Dienste.

Wie lassen sich diese Sicherheitseigenschaften überprüfen?

Mit genügend Fachwissen ist z. B. eine manuelle Prüfung möglich. Allerdings ist das zeitaufwendig und meist nicht reproduzierbar. Ideal wäre eine vollautomatische Prüfung gemäß den jeweiligen Vorgaben.

TLS-Inspector-Testfamilie

Die achelos GmbH bietet für die o. g. Anforderungen ein Portfolio von Testwerkzeugen und Testsuiten im Bereich von TLS und IKE/IPsec an. Die Besonderheit: **Alle Tests erfolgen vollautomatisch, die Testresultate sind reproduzierbar und liefern somit eine hohe Aussagekraft**. Lernen Sie hier die TLS-Inspector-Testfamilie kennen:

Kostenloser Website-Check gemäß BSI-Vorgaben

Mit dem **TLS Checklist Inspector** bietet achelos die kostenfreie automatische Sicherheitsprüfung von Websites über das Web-Portal **www.tls-check.de** an. Angesprochen sind Unternehmen jeglicher Größe, die den Nachweis einer sicheren TLS-Netzwerkverbindung gemäß den Anforderungen der Checkliste des BSI erbringen möchten. Bereits kurze Zeit nach Eingabe ihrer Domain sehen Diensteanbieter, ob ihre Website gemäß den Anforderungen der **BSI-Checkliste auf Basis der TR-03116-4** konfiguriert ist.
Das Prüfergebnis im Web-Portal weist mögliche Schwachstellen aus und stellt einen direkten Zusammenhang mit den Anforderungen aus der BSI-Checkliste her. Geprüft wird u. a. die korrekte Konfiguration von:

- Zertifikaten,
- Cipher-Suiten,
- Protokollen oder
- Algorithmen.

Der **TLS Smart Metering Inspector** richtet sich an Hersteller und Prüfstellen, die die Konformität von Smart Meter oder Smart Meter Gateways für die Energieversorgung gemäß den Vorgaben der TR-03116-3 anstreben.
Der **TLS Client Inspector** und der **TLS Server Inspector** sind für tiefergehende Prüfungen ausgelegt.
Neben der TLS-Konfiguration werden auch die RFC-Konformität und die TLS-Stacks auf korrekte Implementierung geprüft. Nachrichten lassen sich manipulieren, um die Robustheit der Software zu überprüfen und Angriffsmöglichkeiten, wie Bleichenbacher, Poodle und andere, zu detektieren.

Alle TLS-Testsuiten unterstützen Testfälle für die aktuelle TLS-1.3-Version. Neben der TLS-Inspector-Testfamilie lassen sich mit dem **IKE/IPsec Inspector** Internet-Key-Exchange-(IKE-)Implementierungen überprüfen. Die Testsuite behandelt Testaspekte der IPsec-Ebene auf Basis von IKEv2.
Die Tests basieren auf der IETF RFC 3602 „The AES-CBC Cipher Algorithm and Its Use with IPsec“ und BSI-Anforderungen aus dem CC-Schema. In den einzelnen achelos-TLS- und IKE/IPsec-Testsuiten sind zwischen 80 und 130 Testfälle definiert und implementiert.

Eine sichere digitale Präsenz von Unternehmen ist von entscheidender Bedeutung. Sie dient als vertrauenswürdiges Signal für Kunden und schützt sensible Unternehmensdaten. Die Testwerkzeuge von achelos helfen auf einfache Art und Weise dabei, die Netzwerksicherheit gemäß konkreten Vorgaben zu messen. Die Testergebnisse zeigen wichtige Stellschrauben für notwendige Maßnahmen auf, ermöglichen ein schnelles Handeln und vor allem mehr Netzwerksicherheit!

www.achelos.de | www.tls-check.de ■

IT-Security-Kosten, die gerne übersehen werden

Erfahrungen haben gelehrt, dass es meist kostengünstiger ist, eine Hacker-Attacke zu verhindern, als den Schaden nach einem Angriff beheben zu müssen. Doch werden wesentliche Budgetposten der IT-Security von Controllern häufig übersehen oder nicht realistisch bewertet.

Von Dipl. Betriebswirt Otto Geißler

Bild: Pcess609/stock.adobe.com

Da die Security-Budgets nicht in dem Maße steigen können, wie sich die Bedrohungen weiterentwickeln, müssen Unternehmen eine Priorisierung vornehmen.

Jedes Unternehmen, unabhängig von seiner Größe oder Ausrichtung am Markt, sollte ein maßgeschneidertes, genaues IT-Security-Budget erstellen. Dennoch versehen viele Unternehmen ihre IT-Security-Budgets mit kritischen Auslassungen, die sie anfällig für Hacker-Attacken und somit für erhebliche finanzielle Schäden machen können.

Da die Budgets natürlich nicht in dem Maße steigen können, wie Bedrohungen auftreten oder sich weiterentwickeln, ist es unmöglich, für alle Eventualitäten abgesichert zu sein. Das heißt, es muss eine Priorisierung erfolgen. Aber welche Budgetposten sind für die Cybersicherheit eines Unternehmens wichtig oder werden von Controllern gerne übersehen?

Gut geschulte Mitarbeiter können einen erheblichen Beitrag zur Abwehr von Cyber-Angriffen leisten.

Personalbeschaffung und -bindung

In den vergangenen Jahren hat sich die Kluft zwischen qualifizierten Fachkräften und der quasi exponentiell wachsenden Zahl von IT-Arbeitsplätzen stetig vergrößert. Der unerbittliche Wettbewerb um hoffnungsvolle Talente geht also unbeirrt weiter. Entgegen diesem langfristigen Trend unterschätzen viele Unternehmen nach wie vor die Kosten für die Einstellung und Bindung von qualifizierten IT-Security-Experten.

IT-Security-Schulungen

Viele Unternehmen haben verstanden, dass das Verhalten der Mitarbeiter ein großes Risiko darstellt. Somit schlummern die größten IT-Security-Risiken im eigenen Unternehmen. Trotzdem wird viel zu wenig in Mitarbeiterschulungen investiert. Ein gut aufgestelltes IT-Sicherheitsprogramm schließt auch alle betroffenen Mitarbeiter ein, die über ihre Pflichten im Bereich der IT-Security aufgeklärt sind. Nicht zuletzt, um sicherzustellen, dass böswillige Akteure schnell entdeckt und gefasst werden.

IT-Security-Versicherungen

Viele Unternehmen haben die Notwendigkeit von Versicherungen für die IT-Security noch nicht hinreichend erkannt – ein Versäumnis mit potenziell fatalen Folgen! Dies geschieht insbesondere vor dem Hintergrund wachsender Cyber-Bedrohungen. Gerade kleinere Unternehmen sind davon überproportional betroffen. Abgesehen davon, dass Unternehmen sich vor möglichen finanziellen Schäden schützen, kann schon allein die Beantragung einer IT-Security-Versicherung zu einer verstärkten IT-Security-Infrastruktur führen. Denn der Prozess einer Evaluierung, der nötig ist, um eine Police zu erhalten, kann schon dabei helfen, Sicherheitslücken zu identifizieren und Alternativen zur Verbesserung zu entwickeln.

Analysen durch externe Berater

Unternehmen unterschätzen des Weiteren oft die Bedeutung von Schwachstellen-Analysen ⇨

- durch externe Dienstleister, die das Management und Mitarbeiter über potenzielle Cyberbedrohungen aufklären. Es ist angeraten, hier ein größeres Budget vorzuhalten, damit sich Unternehmen gegebenenfalls von mehr als einem Dienstleister unterweisen lassen, um sicherzustellen, dass man eine sogenannte „360-Grad-Beratung“ erhält.
  Nicht wenige Unternehmen glauben, Budgets für externe Meinungen wären unnötig, weil sie mit ihren eigenen Maßnahmen und den angestammten Beratern bisher nie eine Hacker-Attacke erlebt haben. Gerade wenn es um etwas sensiblere Daten geht, gilt Input von verschiedenen Sicherheitsfirmen als angezeigt. Auf diese Weise können Unternehmen sicherstellen, dass sie ihre entsprechenden technischen, administrativen und physischen Sicherheitsvorkehrungen auch umfassend getroffen haben.

Reaktion auf Vorfälle

Insbesondere wenn es um die Planung von Budgets geht, werden gerne die indirekten Kosten für die Reaktionen auf Vorfälle (Incident Response, IR) übersehen. Dagegen würde eine sorgfältig geplante IR-Strategie die Organisation bei einem Hacker-Angriff vor finanziellen Verlusten bewahren. Es empfiehlt sich, eine Stelle dafür zu schaffen oder eine Gruppe von Experten einzustellen und zu schulen, die für die Reaktion auf solche Bedrohungen spezialisiert und verantwortlich ist. Im Krisenfall zahlt sich das weidlich aus.
Obwohl dieses Risiko tagtäglich präsent ist, versäumen es Unternehmen nach wie vor, IR-Ausgaben realistisch zu budgetieren. Angesichts der Horrormeldungen großer Unternehmen in der Presse, die offenbar trotz ausgetüftelter Sicherheitsprogramme gehackt wurden, ist es

Bild: leowolfert/stock.adobe.com

Oft werden die indirekten Kosten für die Reaktion auf Vorfälle (Incident Response) übersehen. Eine sorgfältig geplante IR-Strategie bewahrt die Organisation bei einem Hacker-Angriff vor finanziellen Verlusten.

Bild: ExQuisine/stock.adobe.com

Die jüngste Verlagerung der Arbeitsplätze in Homeoffices kann die Wiederbeschaffungskosten deutlich erhöhen.

nur schwer vorstellbar, warum kleinere Unternehmen sich nicht besser durch den Erhalt oder Aufbau von IR-Maßnahmen aufstellen.

Denn solche indirekte Kosten sind in der Gesamtbetrachtung nicht weniger wichtig als die direkten Kosten. Kein Budget für IR-Services zu haben, könnte dazu führen, dass sich Vorfälle wie beispielsweise Ransomware unnötig in die Länge ziehen, was zu ungleich größeren Geschäftsunterbrechungen, Kundenverlusten und Reputationsschäden führen könnte.

Kosten für die Wiederbeschaffung

Bei der Einordnung eines Budgets für die Wiederbeschaffung für potenziell gefährdete Anlagen nehmen viele Unternehmen eine ausgesprochen kurzsichtige Sichtweise ein, wenn es darum geht, welche der Systeme von einer Sicherheitsverletzung oder Malware betroffen sein könnten. Oftmals beschränken sie den Austausch nur auf die am stärksten gefährdeten Systeme. Doch erfahrungsgemäß entstehen meist Verluste, die weit über den Prognosen der Unternehmen liegen.

Beispielsweise kann die jüngste Verlagerung der Arbeitsplätze in Homeoffices die Wiederbeschaffungskosten deutlich erhöhen und lässt vorsichtige Schätzungen aus der Zeit vor der Pandemie weit in den Hintergrund treten. Denn wer den Austausch oder die Aufrüstung gefährdeter Heimsysteme sträflich vernachlässigt, riskiert viel.

Das bedeutet, wenn Homeoffices angegriffen werden, so können diese Systeme unbeabsichtigt eine Schwachstelle in das Unternehmensnetzwerk einschleusen, selbst wenn ein Unternehmen das Problem auf seiner Seite, also inhouse, behoben hat. □

Single Sign-On und Identity & Access-Management „Made in Germany“

Die drastische Erhöhung von Aktivitäten im Internet zieht eine Zunahme der sensiblen Daten, die elektronisch verarbeitet werden, nach sich. Gleichzeitig sind immer mehr SaaS-Produkte über das Internet in Unternehmensprozesse eingebunden. Alle über das Internet getätigten Transaktionen müssen höchsten Ansprüchen an Datenschutz und -sicherheit genügen.

Bare.ID

Umso heterogener und dezentraler eine Applikations-Landschaft wird, desto schwieriger ist es nachzuhalten und sicherzustellen, dass nur die richtigen Personen, zur richtigen Zeit, aus den richtigen Gründen Zugriff auf diese Anwendungen und die darin enthaltenen Daten erhalten. Für eine alle Anforderungen erfüllende Identity- und Access-Management-Lösung (IAM) ist häufig nicht nur mit Anschaffungskosten für Soft- und Hardware zu rechnen, es schlagen auch Personalkosten zu Buche, um Anwendungen dauerhaft zu betreiben, das meist sehr komplexe Know-how unternehmensintern aufzubauen sowie die betriebsinternen Prozesse entsprechend anzupassen.

Darüber hinaus decken solche IAM-Projekte meist auch nur die Systeme automatisiert ab, die ihre Authentifizierung über ein Active Directory realisiert haben und zum anderen ist in vielen Fällen der Betrieb einer vollwertigen OnPremise-IAM-Lösung eine Nummer zu umfassend und zu kostspielig. Verfügbare SaaS-Alternativen sind regelmäßig in NON-EU-Clouds gehostet und nur aufwändig mit der DSVGO in Einklang zu bringen.

Bare.ID – Lösung mit Datenschutz

Diesen Herausforderungen tritt mit Bare.ID von AOE eine neue Lösung für Identity- und Access-Management entgegen, die keine hohen Investitionen voraussetzt, da sie als ein in Deutschland betriebener SaaS Cloud-Login-Dienst ausgeführt wird. Angebunden sowohl an die eigene OnPremise-IT als auch an moderne Cloud-Applikationen schafft Bare.ID als zentraler Single Sign-On Authentifizierungs- und Autorisierungspunkt eine sichere Basis für hybride IT- und Geschäftsmodelle.

Aufbauend auf der leistungsstarken Open-Source-Lösung Keycloak bietet Bare.ID ein anwenderfreundliches Konfigurations-Interface mit App-Gallery, vorgefertigten White-Label-Templates, Best-Practice-Sicherheitskonfigurationen, Multi-Faktor-Authentifizierung und vielen weiteren nützlichen Features. Bare.ID verwaltet die Identitäten von Nutzer:innen und gibt einen Überblick über Zugriffe, Login-Fehlversuche, unsichere oder abgelaufene Passwörter sowie eine

Multi-Faktor-Authentifizierung

Auflistung von verwaisten Accounts. Sollten unternehmensintern bereits IAM-Lösungen oder Active Directories vorhanden sein, können diese selbstverständlich als Identitäts- und oder Berechtigungsquelle an Bare.ID angebunden werden.

Digitale Souveränität

Ein weiteres Plus ist die digitale Souveränität: Bare.ID wird ausschließlich in deutschen Rechenzentren gehostet. Ein Zugriff oder Eingriff aus Drittstaaten ist somit ausgeschlossen. Hinzu kommt, dass sämtliche Partner, die an der Leistungserbringung beteiligt sind, ebenfalls in Deutschland ansässig sind. Die zu verarbeitenden Daten verlassen also nicht den deutschen Rechtsraum und sind so stets konform mit Compliance-Richtlinien und Normen – auch in regulierten Bereichen.

Hochverfügbarer Cluster-Betrieb

Unternehmen müssen keine eigene Expertise aufbauen. Der hochverfügbare Cluster-Betrieb (SaaS) von Bare.ID kommt mit benutzerfreundlicher Konfigurationsoberfläche zur nachhaltigen Komplexitätsverringerung und wird fully-managed von AOE gehostet. Dabei ist das System von Start an nach sofort einsetzbaren Sicherheits-Best-Practices konfiguriert. So profitieren Kunden vom profunden Security-Know-how der AOE, ohne kostenintensiv eine eigene Expertise aufbauen zu müssen.

Erfahren Sie mehr: **https://www.bare.id** ■

Steffen Ritter

Commercial Director Cybersecurity / AOE

Mit einem Team aus Spezialisten begleitet Steffen Kunden bei IAM- und Single Sign-On-Projekten, macht Sicherheits-Analysen von Webanwendungen und trainiert Entwicklungsteams im Bereich IT-Security und Dev-Sec-Ops. Im Zuge sich wiederholender An- und Herausforderungen rund um Keycloak-Rollout-Projekte hat Steffen die Idee von Bare.ID geboren und an den Markt gebracht: Mit dem Ziel, die häufigsten Fragestellungen und Anforderungen abzudecken, ist eine Produktlösung entstanden, die nicht nur die tiefe Expertise rund um Keycloak, sondern auch die jahrelange Exzellenz im Betrieb von Cloud-Native-Infrastrukturen von AOE in sich vereint.

Die größten IT-Sicherheitslücken im Mittelstand 2020

Mobile Malware, Ransomware-Angriffe oder Cloud Jacking – Cyberangriffe sind heute so leicht und zahlreich wie noch nie, und Unternehmen stehen vor der Herausforderung, sie zu verhindern. Welche Angriffsmethoden kamen 2020 zum Einsatz und wie können diese abgewehrt werden?

Von Matthias Bollwein, Uniki

Im vergangenen Jahr wurde die IT-Sicherheit vor allem in vielen mittelständischen Unternehmen auf die Probe gestellt. Viele Mitarbeiter sind nach wie vor im Homeoffice und somit auch in ihren eigenen privaten Netzwerken unterwegs. Der Zugriff auf firmeninterne sensible Daten muss dennoch gewährleistet sein. Bei Problemen oder Bedenken kann die interne IT nur mit Ferndiagnosen helfen, und die Nutzer sind größtenteils auf sich gestellt. Sie müssen

neben der Umstellung im Arbeitsalltag auch neue digitale Sicherheitsrisiken meistern – keine leichte Aufgabe. Vor allem in Zeiten, in denen sich die Statistiken um Cybercrime nur in eine Richtung bewegen: steil bergauf.

E-Mail-Phishing auf dem Vormarsch

Phishing- und Malware-Mails sind oft nicht mehr so einfach zu erkennen wie noch vor einigen Jahren: Sie sind gut getarnt und individuell auf die „Zielpersonen" zugeschnitten. Wer sich aufgrund des vermeintlichen Aufwands eines solch individualisierten Angriffs nicht als vulnerables Ziel einstuft und in Sicherheit wägt, täuscht sich. Es kann ausnahmslos und ohne Rücksicht jedes Unternehmen treffen. In dieser Hinsicht ist ein Unternehmen auch von Geschäftspartnern, Kunden und deren Sicherheitsmaßnahmen abhängig. Gelangen E-Mails von externen Personen in die Hände der Cyberkriminellen, haben sie bereits inhaltlich die perfekte Grundlage für einen individualisierten Angriff. Denn die Angriffe können, wenn einmal Daten abgeflossen sind, größtenteils automatisiert durchgeführt werden.

Aber wie beugt man einem Angriff durch Phishing und Malware vor? Tendenziell gilt: Wachsam bleiben. Ein Klick in der falschen Mail kann schon zu viel sein. Deshalb sollten gerade „außerplanmäßige" Mails mit besonderer Vorsicht genossen werden. Jedoch reicht das leider bei weitem nicht mehr aus. Selbst Anti-Malware-Programme werden oftmals durch listig programmierte Schadsoftware manipuliert.

Grundsätzlich gilt: Selbst die beste Sicherheitssoftware hinkt immer einen Schritt hinterher, schließlich entwickelt sich Malware stetig weiter. Um eine Chance gegen die kaum überschaubare Landschaft an Schadsoftware wie Viren, Spyware und Trojanern zu haben, ist es zwar wichtig, die Sicherheitssoftware immer aktuell zu halten, aber jeder Mitarbeiter, egal ob aus der Führungsetage oder aus dem Front Office sollte regelmäßig an Sicherheitsschulungen teilnehmen. Die Kombination aus regelmäßigen Updates, einer aktiven Firewall und besonders aufmerksamen Nutzern macht es Malware schwer, ins Firmennetzwerk einzudringen.

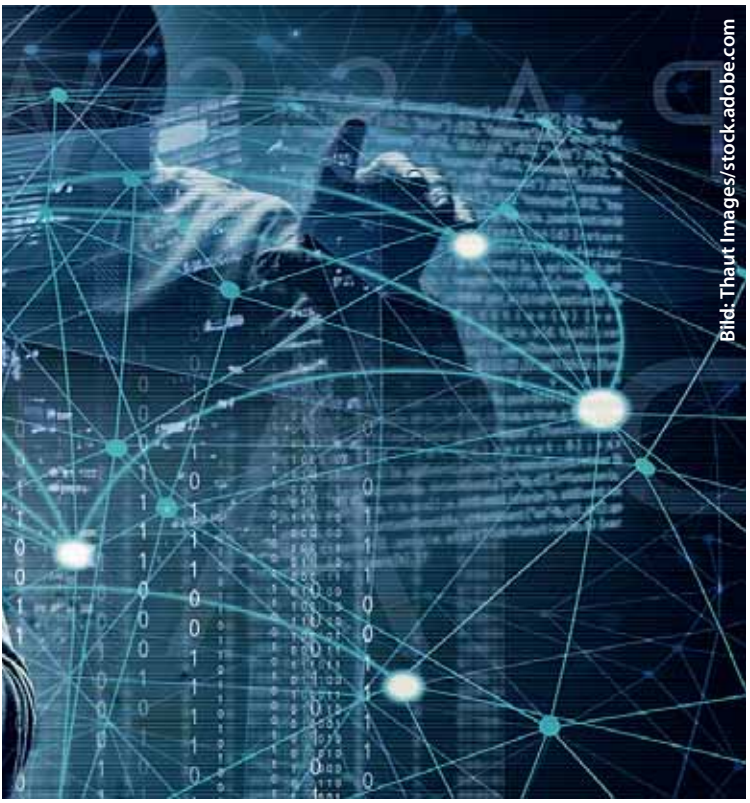


Bild: Thaut Images/stock.adobe.com

Psychologische Tricks hacken keine Maschinen sondern Menschen

Dies gilt auch für die Angriffsmethode „Social Engineering". Nur wird es hier deutlich persönlicher: Es muss keine E-Mail geöffnet und kein Programm heruntergeladen werden, um Daten offenzulegen. Es reicht ein Mitarbeiter und ein ⇨

2020 war aus vielen Gründen eine große Herausforderung für die IT-Sicherheit in Unternehmen und ein erfolgreiches Jahr für Cyberkriminelle.

Sicherheit und Qualität „Made in Germany“

Im Großbritannien des 19. Jahrhunderts eigentlich zum Schutz vor günstiger und vermeintlich schlechterer Importware geprägt, ist der Ausdruck längst zu einem Gütesiegel geworden, das weltweit von Unternehmen und Verbrauchern verstanden wird: „Made in Germany“ steht für eine Qualitätskultur – und dafür, dass die jeweilige Ware in Deutschland entwickelt und gefertigt wird.

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.
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 der Produktentwicklung steht immer ein Aspekt im Vordergrund: die Sicherheit und Qualität zu bieten, die unsere Kunden von uns gewohnt sind. TDT lebt höchste Standards und nachhaltige Leistungsversprechen – nicht nur im Produkt- und Technologiebereich, sondern gerade auch im Kundenservice. Das TDT Expert Support Team vereint seit jeher weitreichende technische Expertise, gelebtes Qualitätsbewusstsein und höchste Effizienz. Im Blick hat unser erfahrenes Service-Team dabei allein Ihre Bedürfnisse. Es gibt kein standardisiertes Schema. Im Gegenteil: Jeder Kunde erhält auf ihn persönlich zugeschnittene Supportleistungen, angepasst an seine individuellen Anforderungen.

Bild: Marina Geckeler/TDT AG

TDT® | Your experts in **DATA COMMUNICATION.**

Michael Pickhardt, Vorstandsvorsitzender der TDT AG: „Ein „Made in Germany“-Produkt hat nur dann Erfolg, wenn es dem Anspruch „Made in Germany“ gerecht wird: Langlebigkeit, Zuverlässigkeit, Sicherheit, persönlicher Service vom Hersteller und eine Funktionalität, die Anforderungen passgenau erfüllt und auch für den Kunden individuell angepasst werden kann. Wir alle müssen uns wieder bewusst machen, was diesen Begriff tatsächlich zu einem Qualitätssiegel gemacht hat – einer Auszeichnung, die auch in Zukunft Bestand hat und immer wichtiger werden wird. Dazu gehört auch, uns unserer kaufmännischen Gepflogenheiten zu erinnern, die tatsächlich der Tradition deutscher Kaufmannsehre entsprechen müssen – wenn wir Qualität nicht nur versprechen, sondern auch wirklich liefern. Wenn wir uns nicht nur vom Kunden Vertrauen wünschen, sondern auch ehrlich verdienen. „Made in Germany“ – Tag für Tag.“ ■

Bei der Produktentwicklung steht immer ein Aspekt im Vordergrund: die Sicherheit und Qualität zu bieten, die unsere Kunden von uns gewohnt sind.

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.

Bild: Drobot Dean/stock.adobe.com

Social Engineering bedient sich psychologischer Tricks z.B. über ein direktes Telefonat mit der Zielperson.

Telefon. Beim „Social Engineering“ wird mit psychologischen Tricks über ein direktes Telefonat mit der Zielperson versucht, dieser sensible Informationen zu entlocken. Bei dieser Methode wird nicht das System gehackt, sondern der Mensch selbst. Um solche Angriffe zu verhindern, sollte klar definiert sein, welche Informationen an Dritte weitergegeben werden dürfen und welche – egal in welchem vermeintlichen IT-Notfall sich die betroffene Person befindet – vertraulich behandelt werden müssen.

Investition in Weiterbildung zahlt sich aus

Viele mittelständische Unternehmen glauben immer noch, dass entsprechende Schulungen der Mitarbeiter Zeit und Geld kosten. Über ein Viertel der Unternehmen haben seit Beginn der Covid-19-Pandemie sogar Einsparungen in Sachen Mitarbeiterschulungen getätigt. Aber die Investition lohnt sich: Denn die Kosten in einem Ernstfall sind deutlich höher. Steht ein Betrieb über mehrere Tage, Wochen oder sogar

Monate still, da auf die eigenen Systeme und Daten nicht mehr zugegriffen werden kann, stecken Ausfallkosten in Millionenhöhe dahinter. Auch der Image-Verlust und der Wegfall wichtiger Kunden dürfen nicht außer Acht gelassen werden.

Augen auf bei der Cloud-Lösungs- und -Anbieter-Wahl

Sind Daten zusätzlich in einer verschlüsselten Cloud gesichert, kann zumindest einem Angriff durch Ransomware vorgebeugt werden. Auch hier sollte der Mittelstand aufstocken: 31 Prozent der mittelständischen Unternehmen sehen sich noch nicht gut genug für eine Migration in die Cloud aufgestellt, es fehle ihnen an Wissen und Ressourcen. Doch die passende Cloud-Lösung kann einen sicheren und entscheidenden Beitrag für die Datensicherheit des Unternehmens leisten, nicht nur im Falle von Hackerangriffen. Bei der Wahl der passenden Cloud-Lösung sollte das Augenmerk vor allem auf dem Sicherheitsaspekt liegen – denn auch Clouds fallen regelmäßig Angriffen, wie beispielsweise Cloud Jacking, zum Opfer. Hier werden Clouds ausgespäht oder sogar komplett übernommen, und Daten können im schlimmsten Fall trotz Backup verloren gehen. Wie auch sonst gilt: Aufmerksam bleiben und Zugangsdaten besonders schützen, etwa durch 2-Faktor-Authentifizierung. Korrekt eingerichtet und orchestriert, mit vollumfänglichen Maßnahmen durch den Anbieter, bedeutet eine Cloud-Lösung sehr hohe Sicherheit.

Viele Komponenten spielen zusammen, um die Datensicherheit zu gewährleisten

Datenlecks können an jeder noch so kleinen Schnittstelle auftreten. Doch alle haben eines gemein: Einen Nutzer, der die davon ausgehende Gefahr nicht erkennt. Hier stehen Führungskräfte in der Verantwortung, ihre Mitarbeiter zu regelmäßigen Schulungen zu verpflichten und das Bewusstsein für die Gefahr von diversen Hackerangriffen zu schaffen. Für erschreckende 31 Prozent der Unternehmen spielen Mitarbeiter bislang überhaupt keine Rolle in ihrer Sicherheitsstrategie. Sie unterschätzen also den Haupteintrittspfad. Um die IT-Security des Unternehmens optimal zu stärken, müssen Arbeitgeber und -nehmer zusammenspielen und an einem Strang ziehen. Helfen sich Mitarbeiter selbst, ist das zwar ein Pluspunkt in Sachen Eigeninitiative, aber möglicherweise eine Katastrophe für die IT-Sicherheit. □


Bild: denisismagilov/stock.adobe.com

Sind Daten zusätzlich in einer verschlüsselten Cloud gesichert, kann zumindest einem Angriff durch Ransomware vorgebeugt werden.

Der Autor

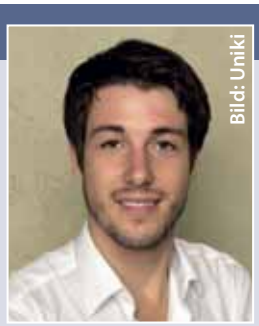


Bild: Uniki

Matthias Bollwein ist Mitgründer des IT-Startups Uniki, das mit der Private Cloud Lösung ELLY eine einfache und hochsichere IT-Lösung für mittelständische Unternehmen anbietet.

BSI-zugelassene VPN-Software für VS-NfD: Eine Lösung für die Zukunft!

Die IT-Welt dreht sich bekanntermaßen besonders schnell. In den letzten zehn Jahren gab es viele verschiedene Entwicklungen im Bereich von Hard- und Software zur sicheren Datenkommunikation der Geheimhaltungsstufe VS-NfD (Verschlusssachen – Nur für den Dienstgebrauch).

NCP
SECURE COMMUNICATIONS

Erhielten anfangs noch Produkte nach gewissen Kriterien eine Einsatzempfehlung des BSI (Bundesamt für Sicherheit in der Informationstechnik), wurde ab 2012 eine BSI-Zulassung durch die höhere Bedrohungslage zur Vorgabe. Es entstanden Hardware-Lösungen oder basierend auf Virtualisierung, da Windows als Betriebssystem als unsicher galt. An letzterem Sachverhalt hat sich bis heute nichts verändert.

VPN für VS-NfD: Hardware gehört der Vergangenheit an

Seit 2019 kam es aufgrund der schlechten Usability und Skalierbarkeit von Hardware zu einem Umdenken. Die prekäre Situation in der Corona-Pandemie durch Hardware-Lieferschwierigkeiten und den plötzlich erhöhten Homeoffice-Bedarf auch bei Bedarfsträgern, Behörden und der geheimschutzbetreuten Wirtschaft goss noch mehr Öl ins Feuer.

Aktuelle Einsatzmöglichkeiten

Im Juli 2020 kam mit dem NCP VS GovNet Connector die erste Softwarelösung mit Freigabeempfehlung des BSI für Endgeräte mit Standard-Windows 10 auf den Markt. Auf Hardware oder Hardware-Abhängigkeit setzt man beim Nürnberger Software-Spezialisten aus guten Gründen nicht mehr.
Die Version 2.0 des softwarebasierten NCP VS GovNet Connector ist führend und hat bereits eine BSI-Zulassung für die Geheimhaltungsstufen „VS-NfD“, „RESTREINT UE/EU RESTRICTED“ und „NATO RESTRICTED“. Durch ihre Leistungsfähigkeit, Skalierbarkeit und ihren Funktionsumfang unterscheidet sich die Lösung im Einsatzverbund mit zentralen NCP-Softwarekomponenten und dem NCP Secure VPN GovNet Server, der ebenfalls für die Kommunikation der Geheimhaltungsstufe VS-NfD vom BSI zugelassen ist, deutlich von anderen Produkten im Markt. Ein Betrieb für über 100.000 gleichzeitige Benutzer ist mit dieser Lösung möglich. Der Rollout, die eigentliche Inbetriebnahme,

das Softwareupdate und die Administration der NCP VS GovNet-Lösung erfolgen komfortabel über das NCP Secure Enterprise Management (SEM) als „Single Point of Administration“. Die Nutzungsmöglichkeiten von Endgeräten mit einem standardisierten Windows 10-Betriebssystem und verschiedene Lizenzmodelle eröffnen Bedarfsträgern neue Möglichkeiten und Flexibilität. Ein Integritätsdienst sorgt in gleichem Maße für erhöhte Sicherheit wie starke Authentisierungsmöglichkeiten und weitere Sicherheitsfunktionen z.B. im Rahmen von Network Access Control und Endpoint Policy Checks. Über sichere und zugleich komfortable Möglichkeiten der Administration wie z.B. das zentrale Rechte- und Konfigurationsmanagement oder „Quality of Service“-Unterstützung freuen sich IT-Verantwortliche.

Quo vadis? Was kann VPN-Software für VS-NfD in Zukunft?

Diese und weitere Vorteile orientieren sich durch jahrelange Erfahrung und Zusammenarbeit ganz eng am tatsächlichen Praxisbedarf. Die Lösung weiterer für die Bedarfsträger relevanter Probleme folgt bei der Zulassung der nächsten Produktversion des NCP VS GovNet Connector zeitnah noch in diesem Jahr.

Die Vision einer leistungsstarken, zentral administrierbaren NCP-Softwarelösung für VS-NfD wird in den kommenden Monaten und Jahren auch Punkte wie REST-API, SAML, Clientsoftware für weitere Betriebssystem-Plattformen und zusätzliche Komfortfunktionen bei der Installation und Konfiguration großer Nutzerzahlen beinhalten. Ziel ist es, Kunden hochskalierbar, hochsicher und gleichzeitig maximal flexibel auch für die Datenkommunikation nach „VS-NfD“ auszustatten.

„Wir freuen uns, dass die NCP VS GovNet-Lösung so gut im Markt ankommt. Mit dieser reinen Softwarelösung haben wir den VS-NfD-Markt revolutioniert und erfüllen mit ihr genau die Bedürfnisse von Ministerien, Behörden und geheimschutzbetreuten Unternehmen. Wir arbeiten mit Hochdruck daran, unsere GovNet-Lösung noch weiter auszubauen. Dabei wird natürlich auch die Anwenderfreundlichkeit nicht vernachlässigt. Die Roadmap ist vollgepackt mit neuen Funktionen, die unsere Kunden langfristig in die Lage versetzen werden, den Anforderungen des Marktes und der Bedrohungslage Rechnung zu tragen.

Patrick Oliver Graf
CEO & Managing Director
NCP engineering GmbH

Auch VS-Arbeitsplätze müssen remote für Homeoffice und mobiles Arbeiten bei großen Nutzerzahlen gut administrierbar sein. Managed-Service-Betreiber und Landesrechenzentren können einzelne Mandanten über eine zentrale Plattform sicher und voneinander getrennt betreuen, auch wenn Kunden einen Mischbetrieb aus VS-NfD und normalen Nutzern fahren.

Informieren Sie sich über die Einsatzmöglichkeiten und Funktionen unter: **www.ncp-e.com**

Security Management as a Service können nicht nur die Beratungshäuser

Viele KMU haben Probleme, einen Security-Verantwortlichen zu finden. Der Channel kann hier mit Security Management as a Service punkten. Dabei helfen Management-Tools, die die Identifizierung und Priorisierung der Risiken sowie die Auswahl und Kontrolle von Security-Lösungen unterstützen.

Von Dipl.-Phys. Oliver Schonschek

Laut einer Bitkom-Umfrage befürchten 83 Prozent der Unternehmen, die Zahl der Cyberangriffe werde bis Ende dieses Jahres zunehmen. Besonders bedroht sehen sich neben den Betreibern kritischer Infrastrukturen die mittelständischen Unternehmen mit 100 bis 499 Mitarbeiterinnen und Mitarbeitern.

Auch die EU-Agentur für Cybersicherheit ENISA hat die KMU im Blick. Wie eine ENISA-Studie ergab, erklären 85 Prozent der befragten KMU, dass Cybersicherheitsprobleme schwerwiegende nachteilige Auswirkungen auf ihr Unternehmen haben würden, 57 Prozent sagen, dass sie höchstwahrscheinlich ihre Geschäftstätigkeit einstellen würden. Von fast 250 befragten KMU gaben 36 Prozent an, in den letzten fünf Jahren einen Vorfall erlebt zu haben.

Fachkräftemangel erschwert Security-Verantwortung

ENISA nennt als ersten Schritt zur Verbesserung der Cybersicherheit bei KMU die Regelung der Security-Verantwortung: „Gute Cybersicherheit ist ein Schlüsselelement für den anhaltenden Erfolg jedes KMU. Die Verantwortung für diese kritische Funktion sollte einer Person innerhalb der Organisation übertragen werden, die angemessene Ressourcen sicherstellen sollte, wie Verfügbarkeit von geeignetem Personal, Cybersicherheitssoftware, Services und Hardware, Schulung des Personals und die Entwicklung wirksamer Richtlinien für die Cybersecurity."

Es steht außer Frage, dass diese verantwortliche Person im Unternehmen selbst sein sollte, doch diese Person braucht Unterstützung. Oftmals ist es die IT-Leitung, die Security nebenbei verantworten soll. Einen CISO haben viele Unternehmen noch nicht, das gilt natürlich besonders für den Mittelstand. Grund genug, über das Angebot „CISO as a Service" nachzudenken.

Security Management Services aus dem Channel

Nun gibt es natürlich schon Angebote, Unternehmen einen externen CISO, virtuellen CISO, einen CISO auf Zeit oder Interims-CISO zu stellen, wie es Beratungshäuser häufig tun. Viele Mittelständler haben jedoch die Sorge, dass solche Beraterinnen und Berater sehr kostspielig werden könnten, und verzichten dann lieber.

Der eigene IT-Dienstleister oder das Systemhaus, mit dem man bereits lange auf Augenhöhe zusammenarbeitet, hat da eine andere Ausgangsposition. Die Leistungen, die für ein externes Security Management notwendig sind, lassen sich durchaus von Vertretern des Security-Channels erbringen. Dazu gehören Services wie Definition und Aufbau der Security-Organisation, Data Discovery, Bedrohungs- und Risikoanalysen, Bewertung und Priorisierung der Risiken, Erstellung eines Security-Konzepts mit angemessenen Maßnahmen für Protection, Detection, Response und Prevention (darunter Security Awareness), die Prüfung der Wirksamkeit der Maßnahmen, das Management Reporting, Security-Beratung für das Management, die Vorbereitung und Reaktion mit Blick auf Vorfälle, um wesentliche Elemente zu nennen.

Ein Blick in das Security-Portfolio zeigt in den meisten Fällen, dass man sogar mehrere Lösungen für die einzelnen Aufgaben im Programm hat. Entscheidend ist dann aber noch die übergreifende Sicht auf die Security beim Kunden und die operative, zentrale Umsetzung von Maßnahmen. Hier können die Security-Management-Plattformen und Konsolen der Security-Hersteller helfen, die vielfach offen dafür sind, auch Lösungen anderer Anbieter zu verwalten.

CISO as a Service

Auch wenn eine Security-Management-Plattform, die man als Dienstleister für seine Kunden betreibt, keinen CISO komplett ersetzen kann, bildet sie doch eine gute Grundlage für ein Angebot wie CISO as a Service. Kann man als Channel-Partner zum Beispiel bestimmte Consulting-Leistungen nicht selbst erbringen, bietet es sich an, entsprechende Services der Hersteller zu vermitteln. Beispiele für Security-Management-Plattformen gibt es einige, darunter beispielsweise die Managementkonsole von G Data. Wie sich Security Management in der Praxis anbieten und betreiben lässt, zeigen Dienstleister wie beispielsweise IS4IT Kritis.

„Für mittelständische Unternehmen ist es oft nicht wirtschaftlich, diese Rolle durch einen eigenen Mitarbeiter zu adressieren, so dass sie nach unserer Erfahrung immer wieder einzelne Aufgaben punktuell durch den Zukauf von Dienstleistungen abdecken müssen. Diese Vorgehensweise ist aber nicht kosteneffizient, gleichzeitig fehlt einem externen Berater häufig der notwendige Gesamtüberblick. Mit ‚CISO as a Service' schaffen wir hier Abhilfe", erläutert Johann Troppmann, Geschäftsführer von IS4IT Schweiz, das Angebot.

Wer bereits Managed Security Services (MSS) anbietet, kann diese Security-Dienste noch um das Security Management oder CISO as a Service erweitern. Die genaue Aufgabenverteilung zwischen Dienstleister und Kunden im Security Management muss vertraglich genau fixiert sein, damit klar ist, wo die Leistungen aufhören und wo die alleinige Verantwortung des Kunden beginnt. □

Sicher vor Cyberattacken mit dem Cyber-Defense-Portfolio von G DATA

Ganzheitliche IT-Sicherheit ist essentiell für Unternehmen. Im vergangenen Jahr zählten die G DATA Security-Forscher:innen mehr als 16,1 Millionen neue Schadprogramme. Das zeigt: Ein umfassender und vertrauenswürdiger Schutz ist wichtiger denn je. Mit einem umfassenden Cyber-Defense-Portfolio aus Lösungen und Dienstleistungen „made in Germany“ macht G DATA Unternehmen verteidigungsfähig gegen Cyberangriffe. Dazu gehören unter anderem KI-Technologien, Endpoint Protection, Awareness Trainings und Incident Response. Fachhändler bieten ihren Kunden so ein breites Spektrum aus einer Hand an.

Lösegeldzahlungen im Zuge von Ransomware-Attacken haben weltweit zugenommen. 2020 lagen diese bei 356,4 Millionen Euro (Quelle: Chainalysis.com). Die G DATA Securitylösungen sind ausgestattet mit den modernsten Technologien und Erkennungsverfahren, um gegen die Erpresserschädlinge und andere Malware zu schützen. Darunter ist DeepRay – die Machine-Learning-Technologie mit künstlicher Intelligenz erkennt verhüllten Schadcode. Cyberkriminelle setzen oft darauf, bekannte Schadprogramme in immer neue Hüllen zu verpacken, um eine Erkennung durch eine Sicherheitslösung zu verhindern. BEAST erkennt Schadcode verhaltensbasiert und zeichnet dabei verdächtige Prozesse in einem Graphen nach. Das verhindert Fehlalarme und ermöglicht, Infektionen wieder zurückzurollen. Diese und weitere proaktive Technologien bilden ein für Angreifer unüberwindbares Bollwerk und schützen wertvolle Unternehmensdaten.

Die G DATA Securitylösungen schützen alle Devices, wie Server, Desktop PCs, Notebooks oder Smartphones. Außerdem bietet das Cyber-Defense-Unternehmen verschiedene Services an: Von Support-Vereinbarungen, bis hin zu vollumfänglicher gemanagter Endpoint-Sicherheit durch einen Dienstleister. Dank der zentralen Managementkonsole können Administratoren oder IT-Dienstleister die G DATA Sicherheitslösungen ohne großen Aufwand steuern.

IT-Systemhäuser haben zudem die Möglichkeit einer Multi-Tenancy-Funktion, damit sie mehrere Kunden auf einer Instanz des Management Servers verwalten können.

Mitarbeitende als Teil der Cyberabwehr

Technische Maßnahmen reichen allein nicht aus für einen umfassenden Schutz vor Cyberattacken. In Unternehmen spielt die Belegschaft eine große Rolle bei der Abwehr. Mitarbeitende werden durch die G DATA Security Awareness Trainings zu einem Teil der Cyberabwehr. Die Trainings umfassen mehr als 40 Kurse zu verschiedenen Themen der IT-Sicherheit, zum Beispiel Phishing. Dabei wird das Wissen in E-Learning-Einheiten praxisnah und bedarfsgerecht vermittelt. Die Lerninhalte verfestigen sich durch Wiederholungen. IT-Verantwortliche können zusätzlich eine Phishing-Simulation durchführen, um den Wissensstand der Mitarbeitenden zu messen.

Security für alle Fälle

Darüber hinaus bietet G DATA ein breites ergänzendes Dienstleistungsportfolio an und hilft, erfolgreiche Cyberangriffe zu bewältigen. Die Palette reicht von Incident Response über Red-Teaming und Penetrationstests bis zu hin weiteren Services. Partner und Kunden können sich dabei auf die Vertrauenswürdigkeit von G DATA verlassen.

Bereits 2011 bekannte sich das Cyber-Defense-Unternehmen dazu, keine Hintertüren für Ermittlungsbehörden oder andere staatliche Akteure in seine Sicherheitslösungen einzubauen. Nur so ist ein umfassender Schutz möglich. Dabei ist das gesamte Security-Portfolio von G DATA „made in Germany“ – davon profitieren Unternehmen und Fachhändler gleichermaßen.

Cybersicherheit in Zahlen

Das Thema IT-Sicherheit ist sehr komplex und für viele Menschen schwer verständlich. Um Licht in das Dunkel zu bringen, hat G DATA zusammen mit brand eins und Statista die Publikation „Cybersicherheit in Zahlen – Lernen. Wissen. Handeln“ herausgebracht. Das Magazin liefert Statistiken, Hintergründe und Fakten zum Thema. Darunter ist der G DATA Index, ein erstmals erhobener Indikator zur gefühlten Cybersicherheit in Deutschland. ■

Erhältlich ist das Heft unter

Warum sollte jemand einen Kühlschrank angreifen?

Smart Homes können für Hacker buchstäblich zu einer Goldmine werden, wenn sie Bank-Kennwörter, Online-Konten, Schlösserkombinationen oder persönliche Daten erbeuten. Denn schlecht gesicherte IoT-Geräte sind ein leichtes Ziel für Cyberkriminelle.

Von Dipl. Betriebswirt Otto Geißler

Bild: mangpor2004/stock.adobe.com

Smart Homes bieten viele Sicherheitsrisiken. Spielend leicht wird es manchmal Hackern gemacht, die Kontrolle über Smart-Lautsprecher, Thermostat, Türklingel oder andere IoT-Geräte zu übernehmen.

Vielen Smart Home-Eigentümern ist es nach wie vor nicht bewusst, dass vernetzte IoT-Geräte wie jede andere Website oder jeder andere Computer gehackt werden können. Zumal in den meisten Smart Homes schlecht gesicherte Heimrouter für Endverbraucher im Einsatz sind.

Über gehackte IP-Kameras lässt sich sehr leicht ein idealer Zeitpunkt für einen Einbruch bestimmen.

Leichte Ziele für Hacker

Zu den anfälligsten IoT-Geräten gehören solche im Freien mit Mini-Computern, die vor allem nur wenige oder keine Sicherheitsprotokolle unterstützen. Das sind beispielsweise Garagentoröffner, drahtlose Türklingeln oder sogenannte intelligente Sprinkler. Solche Geräte können ein leichtes Ziel für Hacker sein, die gerade einmal mit einem kleinen Computer oder einem anderen WLAN-Sender die Straße entlang fahren. Zum anderen lassen sich Geräte, die über eine App von einem Smartphone oder PC aus gesteuert werden, ebenfalls leicht hacken.

Solche Geräte können smarte Glühbirnen, Schalter, Überwachungskameras, Babyphones, Türschlösser oder Thermostate sein. Denn sie sind auf schwache Sicherheitstoken angewiesen und können aufgrund von Schwachstellen in den verwendeten Protokollen, Konfigurationseinstellungen oder anfälligen Einstiegspunkten, die der Anbieter für Wartungsarbeiten offen gelassen hat, sehr leicht manipuliert werden.

Mögliche Angriffs-Szenarien

Indem Cyberkriminelle in der Lage sind, über einfache IP-Kameras detaillierte Einblicke in ein Privatleben zu nehmen, lässt sich auch sehr leicht ein idealer Zeitpunkt für einen Einbruch bestimmen. Dann wird per Hacking zur passenden Zeit die Haustür geöffnet. Ob ein Smart Home angegriffen wurde, entdeckt der Eigentümer meist erst, wenn er den tatsächlichen Schaden des Einbruchs augenscheinlich feststellen kann.

Gleichzeitig können über gehackte Geräte eine Vielzahl an Spionageprogrammen oder Viren eingeschleust werden. Das vielleicht schrecklichste Szenario: Während der schönsten Fernsehzeit wird der Eigentümer per Smart-TV-Bildschirm aufgefordert, einer Lösegeldzahlung nachzukommen. Oder es verschafft sich ein Hacker Zugang zu persönlichen Daten wie beispielsweise Kreditkarten-Informationen, dann kann er damit ganz bequem Bestellungen, Geldüberweisungen oder Reisebuchungen im Internet ausführen.

Ein anderes Angriffs-Szenario könnte sein, dass kompromittierende Informationen wie intime Fotos oder ein vertraulicher Schriftverkehr gesammelt werden. Diese Daten nutzen Hacker, um den Smart Home-Eigentümer zu erpressen. Solche Attacken können sich ebenso auf die Manipulation und missbräuchliche Steuerung ⇨

Sicherer Datenaustausch aus dem Homeoffice

netfiles Datenraum bietet Sicherheit und Compliance bei der Arbeit von zuhause

NETFILES

Unsere Arbeitswelt wird immer mobiler und flexibler. Neben der Arbeit in Projektteams an wechselnden Arbeitsorten nimmt die Bedeutung von Heimarbeitsplätzen weiter zu. Auch nach einem Ende der COVID-19 (Corona) Pandemie wird dieser Trend anhalten.

Der Laptop Computer, der heute selbst bei festen Arbeitsplätzen im Büro meist zum Standard gehört, macht die Flexibilität hinsichtlich des Arbeitsortes einfach. Die Einbindung in das Firmennetzwerk und der sichere Datenaustausch vom Homeoffice gestalten sich jedoch in den meisten Fällen schwieriger. Hier ist in der Regel zusätzlicher IT-Administrationsaufwand und Installation von Software notwendig. Bei der aktuell sehr großen und weiter zunehmenden Anzahl von Heimarbeitsplätzen ist der Aufwand für eine sichere Vernetzung der Homeoffices für die IT-Abteilungen der Unternehmen kaum noch zu bewältigen. Doch das muss nicht sein. Ein virtueller Datenraum, wie netfiles, lässt sich sofort, ohne Installation von Software oder IT-Administration einsetzen und ermöglicht unabhängig vom Standort des Benutzers einen hochsicheren Datenaustausch mit anderen Mitarbeitern oder Geschäftspartnern und Kunden. Ohne aufwendige Einbindung ins Firmennetzwerk können so Compliance-Richtlinien und höchste Sicherheitsstandards beim Datentransfer aus dem Homeoffice berücksichtigt werden. Im netfiles Datenraum sind Daten sowohl bei der Speicherung als auch Übertragung durch 256-bit Verschlüsselung sicher und Compliance-konform geschützt.

Der Einsatz eines netfiles Datenraums im Homeoffice bietet darüber hinaus noch weitere Vorteile. So können beispielsweise auch größere Dateien (bis zu 4 GB) schnell und sicher übertragen werden. Probleme mit zu großen E-Mail-Anhängen gehören damit der Vergangenheit an. Und auch das typische Versionschaos, das leicht beim mehrmaligen Austausch von Dokumenten per E-Mail entsteht, wird durch den Einsatz eines virtuellen Datenraums vermieden. Mit netfiles ist sichergestellt, dass alle Beteiligten immer auf das aktuellste Dokument von überall zugreifen können. ■

www.netfiles.com

Testen Sie jetzt netfiles 14 Tage kostenlos oder vereinbaren Sie einen Termin für eine Online-Präsentation.

netfiles GmbH • Marktler Str. 2 • 84489 Burghausen • +49 8677 915 96-12 • vertrieb@netfiles.de

↪ von Smart Home-Geräten richten, um möglichst großen Schaden am Gebäude oder der Einrichtung zu verursachen.

Was tun?

Alle möglichen Angriffsziele haben immer eines gemeinsam: Im Prinzip können einfache Sicherheitsvorkehrungen solche Cyberattacken verhindern. Das Problem ist nur, es gibt meistens keine! Systeme, die sowohl vor internen als auch vor externen Attacken einen hinreichenden Schutz liefern, sind kein Hexenwerk und werden zahlriech angeboten.

Auf der anderen Seite sollte sich ein Eigentümer die Frage gestatten, ob der Komfort, den das eine oder andere Gerät ihm bietet, auch das potenzielle Risiko eines Angriffs wert ist.

Folgende Maßnahmen tragen dazu bei, ein Smart Home sicherer zu machen:

Sicheres WLAN

Standardmäßig sind die meisten Router entweder nicht gesichert oder verwenden ein generisches Kennwort. Das heißt, Hacker können problemlos in Geräten stöbern und auf Geräte zugreifen, die mit dem Router verbunden sind. Daher muss das WLAN mit einem sicheren Passwort versehen werden. Es ist unglaublich, aber das altmodische Passwortsystem ist nach wie vor die Hauptverteidigungslinie, die High-Tech-Geräte schützt.

Bild: urby/stock.adobe.com

Standardmäßig sind die meisten Router entweder nicht gesichert oder verwenden ein generisches Kennwort.

Ferner sollte ein Passwort niemals für verschiedene Smart Home-Geräte gleichzeitig verwendet werden. Wer seine Geräte von extern sicher steuern möchte, macht das natürlich nie über ein öffentliches WLAN!

Eine Zwei-Faktor-Authentifizierung bietet zusätzliche Sicherheiten. Das Verfahren ähnelt einem zweiten Kennwort, falls es einem Hacker gelang, die Schranke von Benutzernamen und Kennwort zu durchbrechen. Zusätzlich erhält der Eigentümer eine Benachrichtigung über verdächtige Aktivitäten, damit er sein Passwort ändern kann.

Es empfiehlt sich ebenso, ein zweites WLAN-Netzwerk speziell für Smart Home-Geräte zu erstellen. Bei vielen Routern können mehrere Netzwerke mit jeweils eigenem Kennwort eingerichtet werden. Damit wird das Hacking von IoT-Geräten auf bestimmte Teilbereiche beschränkt und vor allem von Bereichen getrennt, in denen Bankgeschäfte getätigt und vertrauliche Daten gespeichert werden. Zudem sollte der Hauseigentümer immer ein Gastnetzwerk für Smartphones und Computer der Besucher bereitstellen, in dem die IoT-Geräte nicht sichtbar sind und nicht auf sie zugegriffen werden kann.

Geräte und Systeme aktualisieren

Smartphones werden meist recht häufig ausgetauscht, aber was ist mit dem Router? Ein alternder Router bedeutet auch immer alternde Sicherheitsprotokolle und einen einfacheren Zugangspunkt für Cyberkriminelle. Registrierungen von Routern und sonstigen Geräten beim Hersteller sind wichtig, da diese häufig Firmware- bzw. Software-Updates veröffentlichen, die dabei helfen, neu entdeckte Fehler und Sicherheitsbedenken zu beheben. Bei der

Bild: Andrey Popov/stock.adobe.com

Einige Smart-TVs verfügen über eigene Betriebssysteme und somit auch über eigene Sicherheitsanwendungen wie beispielsweise Virenscanner.

Installation der zugehörigen Apps sollten die damit verbundenen Berechtigungen beachtet werden. Es gilt: Keine Zugriffe auf etwas erlauben, das nicht notwendig ist!

Security Apps installieren

Firewalls und Security Apps erhöhen die Netzwerksicherheit und den Schutz der Smart Home-Geräte vor Angriffen. Einige Smart-TVs verfügen über eigene Betriebssysteme und somit auch über eigene Sicherheitsanwendungen wie beispielsweise Virenscanner. Sicherheits-Apps gibt es im Internet oder bei den jeweiligen Herstellern. Kleiner Tipp: In den Geräte-Einstellungen lassen sich Kameras und Mikrofone deaktivieren, wenn sie sich nicht gerade im Gebrauch befinden. So sind sie nicht permanent aktiv und im „Lauschmodus".

Fazit

Angesichts der bestehenden Sicherheitsrisiken müssen Eigentümer jedoch nicht auf den Komfort eines Smart Homes verzichten. Im Grunde geht es darum, Risiken zu verstehen und die verfügbaren Sicherheitsfunktionen zu nutzen. Unabhängig davon, ob ein vollständiges Netzwerk smarter Küchengeräte oder nur ein einfacher Sprachassistent vernetzt wird, kann damit sichergestellt werden, dass Unbefugte keinen Zutritt dazu erhalten. □

Retarus Secure Email Platform: Höchstes Schutzniveau kombiniert mit Top-Performance

E-Mail stellt Unternehmen in Sachen Sicherheit, Compliance, Verfügbarkeit und Skalierbarkeit zunehmend vor Herausforderungen. Abhilfe schafft die Retarus Secure Email Platform, eine cloudbasierte Komplettlösung für E-Mail „made in Germany".

retarus

E-Mails sind nicht nur integraler Bestandteil jedes digitalen Arbeitsplatzes, sondern auch vieler unternehmenskritischer Geschäftsprozesse. Verteilte, heterogene und teils veraltete Systemlandschaften, fehlende Trennung von Arbeitsplatz- und Applikations-Traffic sowie Cyberkriminelle, die immer perfider vorgehen, machen E-Mail für Firmen immer komplexer und fehleranfälliger. Zudem muss die DSGVO eingehalten, für den Notfall geplant und die Digitalisierung vorangetrieben werden.

Ganzheitlicher Ansatz mit modularen Optionen

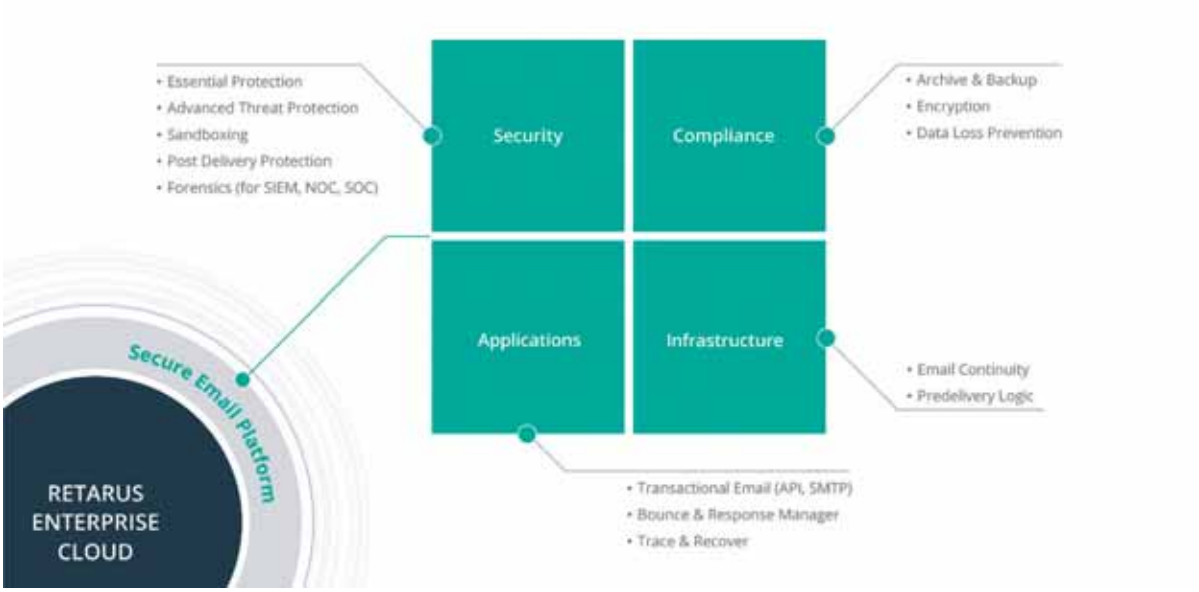
Um die gestiegenen Anforderungen zu erfüllen, sollten Unternehmen gezielt auf Enterprise-E-Mail-Services wie die modulare Retarus Secure Email Platform setzen. Diese berücksichtigen von Sicherheit und Continuity über Compliance bis hin zu Applikations-Traffic und Routing alle Aspekte der geschäftlichen E-Mail-Kommunikation und lassen sich an individuelle Anforderungen anpassen.

Maximale Sicherheit

Im Bereich E-Mail Security bietet Retarus umfassende und kontinuierlich weiterentwickelte Schutzmechanismen und patentierte Technologien zur Advanced Threat Protection und Post-Delivery Protection. Im Sinne von „Best-of-Breed" integriert die Plattform führende Drittanbieter (etwa zur Inhaltsklassifizierung und Threat Prevention). Ferner stellt Retarus optional in Echtzeit Events für SIEM-Tools bereit, um deren Datenstrom unkompliziert mit zusätzlichen Details zur E-Mail-Sicherheit anzureichern und vordefinierte Reaktionen automatisch anzustoßen.

Datenschutz und Compliance

Auch in puncto Datenschutz sowie der Einhaltung gesetzlicher Vorschriften sind Retarus-Kunden auf der sicheren Seite: Retarus Email Encryption bietet benutzerfreundliche, sichere Verschlüsselung über gängige Standards wie S/MIME und (Open-) PGP mit zentraler Schlüsselverwaltung. Für Empfänger ohne geeignete Infrastruktur steht zusätzlich ein sicherer Webmailer bereit. Mit dem Retarus Email Archive bewahren Unternehmen ihre Geschäftskommunikation revisionssicher auf. Wie bei allen Services erfolgt



auch hier die Datenverarbeitung in hochsicheren, auditierbaren Retarus-Rechenzentren in Deutschland. Neben höchsten Compliance-Anforderungen erfüllt Retarus selbstverständlich die Vorgaben der DSGVO und alle gängigen Branchenstandards.

Transactional Email aus Business-Anwendungen

Die schnelle und sichere Zustellung transaktionaler Mails spielt ebenfalls eine wichtige Rolle. Ob Newsletter, Bestellbestätigung, Passwortänderung oder Statusmeldung: Jede Nachricht, die zu spät oder gar nicht ankommt, belastet die Kundenbeziehung. Zur Retarus Secure Email Platform zählt deshalb auch Retarus Transactional Email. Mit Reputation Management einschließlich dynamischem IP-Routing und speziellen Zertifizierungen, Bounce und Response Management auf Basis eigener Regelwerke sowie der Kurzzeitarchivierung aller aus Business-Anwendungen generierten E-Mails erhalten Firmen ein Rundumpaket für den hochvolumigen E-Mail-Versand.

Management der E-Mail-Infrastruktur

Per Predelivery Logic lässt sich der gesamte eingehende E-Mail-Verkehr bereits auf Gateway-Ebene über selbst definierte Regeln kontrollieren, organisieren, umleiten oder anpassen. Das Ergebnis ist maximale Flexibilität, die serverseitige oder auf einzelne Postfächer beschränkte Regelwerke nicht bieten können. Die Cloud-Lösung erlaubt das Routing von E-Mails an bestimmte Standorte oder Tochterfirmen auf Benutzerebene genauso wie etwa das Editieren und Weiterverarbeiten aufgrund von Nachrichteninhalt oder -sprache.

E-Mail Continuity für den Ernstfall

Sollte die primäre E-Mail-Infrastruktur einmal ausfallen, etwa durch einen Security-Incident, einen Hardwarefehler oder eine Cloud-Downtime, springt Retarus Email Continuity ein und stellt das Routing auf vorab provisionierte Webmail-Postfächer um. Somit bleiben Unternehmen auch im Ernstfall per E-Mail erreichbar und Mitarbeiter können unterbrechungsfrei weiter kommunizieren, natürlich vollumfänglich geschützt durch Retarus Email Security. ■

Retarus auf der it-sa 2021

Besuchen Sie Retarus vom 12. bis zum 14. Oktober auf der it-sa in Nürnberg in Halle 7 an Stand 7-206.

IoT-Sicherheit – Land in Sicht oder Land unter?

Die Sicherheitsrisiken im und durch das Internet of Things (IoT) nehmen unaufhörlich zu, die IoT-Sicherheit tritt auf der Stelle, so scheint es. Doch ist es wirklich so? Kommt die IoT-Sicherheit nicht doch voran? Berichte und Empfehlungen von Sicherheitsbehörden geben spannende Einsichten, die bei der weiteren Strategie für die eigene IoT-Security helfen können.

Von Dipl.-Phys. Oliver Schonschek

Über 80 Prozent der Unternehmen haben das Internet der Dinge implementiert, und fast 20 Prozent der Unternehmen haben in den vergangenen drei Jahren einen IoT-basierten Angriff entdeckt, so die Marktforscher von Gartner. Weniger als ein Drittel der CISOs ist davon überzeugt, dass ihre Security-Abteilung das IoT-Risiko zuverlässig bewerten und mindern kann. Steht es also nicht gut um die IoT-Sicherheit?

Auf diese Frage gibt es mehr als eine Antwort. Einerseits nehmen die Cyberattacken zu, die Schwachstellen im IoT ausnutzen, um IoT-Daten auszuspähen und IoT-Systeme zu manipulieren. Die Angriffsziele reichen von Fitness-Trackern bis hin zu vernetzten Wasserwerken. Daneben werden unzureichend geschützte IoT-Geräte weiterhin zu Angriffszwecken missbraucht, zum Beispiel für die Ausführung von DDoS-Attacken.

Andererseits gibt es viele Initiativen und Bestrebungen, die IoT-Sicherheit deutlich voranzubringen. Dazu gehört in jedem Fall das Vorhaben, die IoT-Sicherheit transparenter werden zu lassen, zum Beispiel durch die Sicherheitszertifizierung bei IoT-Geräten.

Die Mitgliedsstaaten der Europäischen Union wollen die Cybersicherheit von vernetzten Geräten voranbringen, so eine Mitteilung des Bundesinnenministeriums im Dezember 2020. Künftig sollen möglichst alle vernetzbaren Geräte ein noch zu identifizierendes Mindestmaß an Sicherheitseigenschaften aufweisen müssen. Die EU-Mitgliedsstaaten unterstreichen, dass hierfür das europäische Rahmenwerk für Cybersicherheitszertifizierung herangezogen werden soll. Der Weg hin zu IoT-Sicherheitszertifikaten wird also langsam, aber sicher beschritten.

Komplexität in der IoT-Sicherheit berücksichtigen

Leicht wird aber eine solche Zertifizierung im IoT nicht, denn Sicherheit kann immer nur in der gesamten Lieferkette entstehen, sie betrifft alle Komponenten und beteiligten Hersteller. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) veröffentlichte entsprechend Richtlinien zur Sicherung des IoT, die die gesamte Lieferkette im Internet of Things, Hardware, Software und Dienste, abdecken sollen.

Bild: ZinetroN/stock.adobe.com

Das Ziel lautet Security by Design im IoT, doch der Weg ist lang.

Lieferketten sind derzeit einer breiten Palette von Bedrohungen ausgesetzt, von physischen Bedrohungen bis hin zu Cybersicherheitsbedrohungen, so ENISA. Organisationen werden mehr denn je von Dritten abhängig. Da Unternehmen die Sicherheitsmaßnahmen ihrer Lieferkettenpartner nicht immer kontrollieren können, sind IoT-Lieferketten zu einem schwachen Glied für die Cybersicherheit geworden. Unternehmen haben heute weniger Sichtbarkeit, wie die von ihnen erworbene Technologie entwickelt, integriert und bereitgestellt wird, als jemals zuvor, wie ENISA klarstellt.

Sicherheitsempfehlungen und Leitlinien für das IoT nutzen

Die Komplexität im IoT führt auch dazu, dass es nicht die eine IoT-Sicherheit gibt. So macht es Sinn, sich jeweils mit dem genauen IoT Use Case zu befassen.

So hat das BSI (Bundesamt für Sicherheit in der Informationstechnik) die Sicherheit in Smart Cities betrachtet, eine Prüfspezifikation zur Technischen Richtlinie für Breitband-Router veröffentlicht und die Cybersicherheit an Bord von Schiffen behandelt. Auch ENISA hat sich mit der Sicherheit bei vernetzten Fahrzeugen und in vernetzten Häfen befasst, um nur einige Beispiele zu nennen.

Security by Design im IoT als Ziel, Embedded Security als Unterstützung

Die Vielfalt der Bedrohungen und Angriffsmöglichkeiten im IoT macht zudem sehr deutlich, dass die Security auch und gerade im IoT mehr zum Bestandteil werden muss, weniger zur Ergänzung einer IoT-Lösung. Security by Design ist das Ziel, der Weg dahin weiterhin steinig.

Umso erfreulicher ist es, wenn nach Wegen gesucht wird, die Security in die IoT-Lösungen selbst zu bringen, im Sinne von Embedded-Security-Funktionen. Dann hat man zwar noch kein Security by Design, aber eine tiefe Integration von Security und IoT.

Offensichtlich gibt es weiterhin große Herausforderungen bei der Absicherung im IoT, doch nicht nur die IoT-Attacken nehmen zu, auch die IoT-Sicherheit kann Fortschritte verzeichnen. Gute Ansätze wie die IoT-Sicherheitszertifizierung können diese Fortschritte noch beschleunigen. Dann haben wir mehr Land in Sicht bei der IoT-Sicherheit. □

Wie Sie die Zahl erfolgreicher Cyberangriffe in Ihrer Organisation minimieren

Schwachstelle Mensch? Von wegen: Wenn Mitarbeitende wissen, wie sie richtig auf Cyberangriffe reagieren sollen, werden sie zu einer starken Human Firewall. Mithilfe der SoSafe Awareness-Plattform senken Organisation nachhaltig ihr Cyberrisiko – DSGVO-konform und ohne großen Aufwand.

SoSafe
Cyber Security Awareness

Die letzten Monate haben deutlich gezeigt: Die Kosten, die Cyberangriffe verursachen, steigen ins Unermessliche. Mehr als 220 Milliarden Euro haben Hacker in Deutschland alleine im vergangenen Jahr erbeutet, wie eine aktuelle Bitkom-Studie zeigt. Ein Tatort, der immer beliebter wird: das Homeoffice. Kein Wunder, schließlich ermöglicht mobiles Arbeiten weitere Wege in die Unternehmensnetzwerke. Die Phishing-Mail-Klickrate von Organisationen, die dezentral arbeiten, ist außerdem dreimal so hoch wie bei Organisationen, die ohne Remote Work tätig sind – zumindest solange die Mitarbeitenden nicht sensibilisiert sind. Denn mit dem richtigen Training kann die Klickrate bereits kurz nach Beginn um 50 bis 70 Prozent reduziert werden. Neben agilen Arbeitsweisen fokussieren sich Hacker weiterhin verstärkt auf aktuelle Themen wie Impfungen und emotionale Reize wie Neugierde. Auch in den nächsten Monaten ist deshalb mit einer verschärften Cyber-Bedrohungslage zu rechnen.

Wächst die Bedrohungslage durch Künstliche Intelligenz?

Cyberkriminelle sind kreativ, jährlich entstehen zahlreiche neue Tricks in der Hackerszene. Mithilfe von Künstlicher Intelligenz etwa ist es nur eine Frage der Zeit, bis Social-Engineering-Angriffsmethoden noch

massentauglicher werden – und somit noch flächendeckender verwendet werden können. Von Organisationen ist deshalb schnelle Reaktion gefragt. Und zwar nicht nur in Bezug auf technische Sicherheitsvorkehrungen. Denn 90 Prozent der Cyberangriffe zielen bewusst auf emotionale Faktoren wie Neugierde und taktieren damit den Faktor Mensch.

Die enge Verknüpfung von Mensch und IT-Sicherheit zeigt: Mit agilen Arbeits- und damit einhergehenden neuen Angriffsmethoden kommt Mitarbeitenden eine verstärkte Verantwortung zu. Je flexibler die Angriffstaktiken der Cyberkriminellen sind, desto dynamischer müssen Organisationen ihre Sicherheitsstrategie aufbauen. Hilfreich sind hierbei kontinuierliche Schulungen. Denn nur so können Gewohnheiten langfristig geändert werden.

Sobald Mitarbeitende typische Tricks und neue Maschen der Cyberkriminellen verinnerlicht haben, erkennen sie Phishing-Mails und Co. deutlich besser – und schalten bei der nächsten riskanten Situation einfach in den „Autopilot-Modus“.

Flexibel und individuell: So geht modernes Awareness-Training

Was zunächst aufwendig klingt, kann problemlos umgesetzt werden. Die SoSafe Awareness-Plattform bietet:

- **Nachhaltige Sensibilisierung**:
  Kurze Micro-Module, die auf Lernpsychologie basieren, und smarte Angriffssimulationen fördern nachhaltiges Lernen. Mitarbeitende werden effektiv zum Umgang mit Cyberrisiken geschult und können zukünftig im Autopilot-Modus reagieren.

- **Einfache Implementierung**:
  Für Administratoren besteht bei der Implementierung kaum Aufwand. Diverse Optionen erleichtern die Einführung. Umfassende Auswertungen machen das Organisationsrisiko messbar.

- **Gesicherter Datenschutz**:
  SoSafe wird in Deutschland entwickelt und läuft ausschließlich auf deutschen Servern. Die Auswertungen zum Beispiel der Phishing-Simulationen sind anonym, sodass personenbezogene Daten jederzeit geschützt sind. Alle Daten werden vollständig DSGVO-konform gespeichert und verarbeitet.

- **Individuell anpassbar**:
  E-Learning und Phishing-Simulationen können über die „Customization Engine“ optisch und inhaltlich an interne Richtlinien angepasst werden.

Worauf also warten? Setzen Sie IT-Sicherheit einfach um und minimieren das Cyberrisiko in Ihrer Organisation.

Weitere Informationen zur Awareness-Plattform gibt es unter **www.sosafe.de**. Eine individuelle Demo können Sie kostenfrei unter **https://lp-sosafe.de/individual-demo** vereinbaren. ■

Wie die Cybersicherheit in Deutschland gestärkt werden kann

Die Politik in Deutschland hat Cybersicherheit seit Jahren auf der Agenda. Die neue Cybersicherheitsstrategie der Bundesregierung ist ein Beispiel dafür. Doch wie steht es um die Umsetzung der Strategien? Und stimmen die Ziele und Schwerpunkte? Wirtschaftsverbände und Sicherheitsexperten melden Kritik an und nennen Bereiche, die stärker in den Fokus rücken oder geändert werden müssen.

Von Dipl.-Phys. Oliver Schonschek

Bild: Norbert/stock.adobe.com

Mit der „Cybersicherheitsstrategie für Deutschland 2021" hat die Bundesregierung einen neuen Fünf-Jahres-Plan zur Cybersicherheit vorgestellt.

Ein neuer Fünf-Jahres-Plan für Cybersicherheit

„Cybersicherheit ist kein notwendiges Übel, sondern Voraussetzung dafür, dass die Digitalisierung gelingt", betonte der Bundesminister des Innern, für Bau und Heimat, Horst Seehofer, bei der Vorstellung der „Cybersicherheitsstrategie für Deutschland 2021". Bei einer hohen Gefährdungslage im Cyberraum müssten sich Staat, Wirtschaft und Gesellschaft gemeinsam um die sichere und freie Nutzung neuer Technologien kümmern. „Dazu gehören gut ausgestattete Sicherheitsbehörden, ein effektiver Schutz von kritischen Infrastrukturen und

Wirtschaftsunternehmen und mehr Sicherheit für die Bürgerinnen und Bürger im digitalen Raum", so der Minister.

An diesen Zielen besteht bei den relevanten Wirtschaftsverbänden und bei Sicherheitsexperten kaum ein Zweifel. Doch der Weg dahin, die konkrete Umsetzung bedarf noch der Optimierung, so der Tenor der anschließenden Diskussion.

„Die Cybersicherheitsstrategie ist grundsätzlich ein zentraler Baustein für die Cyber-Sicherheit in Deutschland", so TeleTrusT-Vorstandsvorsitzender Prof. Dr. Norbert Pohlmann. „Es ist daher ein wichtiges Signal, dass die Bundesregierung mit der Fortschreibung der Strategie strategische Ziele und Schwerpunkte im Bereich Cyber-Sicherheit auch für die kommende Legislaturperiode definiert." Prof. Pohlmann nennt auch Kritik: „Bedauerlich ist allerdings, dass das Bundesinnenministerium die Novellierung der Cybersicherheitsstrategie nicht für eine grundlegende Aktualisierung genutzt hat."

Es ist jedoch nicht nur die fehlende grundlegende Aktualisierung, die kritisiert wird. Diese könnte man durchaus damit erklären, dass ein Fünf-Jahres-Plan in der Cybersicherheit nicht alle konkreten Maßnahmen benennen kann, da die Cybersicherheitslage und die technische Entwicklung einfach zu dynamisch sind. Sicherheitsexperten und Verbände kritisieren aber auch ein falsches Verständnis, wie man die Cybersicherheit stärken kann. Ein Beispiel ist der richtige Umgang mit Schwachstellen.

Den Umgang mit Schwachstellen überdenken

Die Ziele, einerseits größtmögliche IT-Sicherheit zu gewährleisten und andererseits die Notwendigkeit, Strafverfolgungs- und Sicherheitsbehörden die Erfüllung ihres gesetzlichen Auftrags zu ermöglichen, stehen in einem Spannungsverhältnis zueinander, so die Strategie der Bundesregierung.


Bild: eco

„Die Bundesregierung konterkariert durch fragliche Ziele und Ansätze im Bereich der Strafverfolgung und der Geheimdienstpolitik das Ziel der Verbesserung der Cyber-Sicherheit", sagt Prof. Dr. Norbert Pohlmann, Vorstand Ressort IT-Sicherheit, eco - Verband der Internetwirtschaft e.V., und Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT.

Geplant ist deshalb insbesondere eine „Risikoabwägung zwischen dem Gefährdungspotenzial von (Zero-Day-)Schwachstellen bei temporärer Ausnutzung durch die Sicherheits- und Strafverfolgungsbehörden und dem prognostizierten Nutzen für die nachrichtendienstliche Aufklärung, Gefahrenabwehr und Strafverfolgung".

Was damit gemeint ist, zeigt die Reaktion der Branchenverbände und Experten: Ein mögliches Zurückhalten bei der Bekanntmachung von Schwachstellen durch staatliche Behörden für andere Zwecke erachtet zum Beispiel der Verband der Internetwirtschaft eco als verantwortungslos und kontraproduktiv für die IT-Sicherheit. Behörden untergraben damit nicht nur die IT-Sicherheit, sondern beschädigen auch das Vertrauen von Bürgerinnen und Bürgern in staatliche Institutionen, so eco. ⇨


Bild: Henning Schacht

„Damit Digitalisierung gelingt, brauchen wir Cybersicherheit", betont Horst Seehofer, Bundesminister des Innern, für Bau und Heimat.

Mehr Fokus auf Ausbildung und Fortbildung

Eine weitere gefährliche Entwicklung kann es sein, dem Fachkräftemangel nicht nachhaltig zu begegnen. Bekanntlich ist der Fachkräftemangel in der Cybersicherheit eine der größten Herausforderungen, um den steigenden Cyberbedrohungen besser begegnen zu können. Ausbildung und Weiterbildung im Bereich Cybersicherheit sollten sich deshalb in den zentralen Eckpfeilern einer Sicherheitsstrategie finden.

Eine exzellente IT-Sicherheitsforschung sowie gut ausgebildete IT-Sicherheitsfachkräfte sind wichtige und nachhaltige Grundpfeiler für die Wahrung der Cybersicherheit, sagt auch die Cybersicherheitsstrategie 2021.

Konkret adressiert die Cybersicherheitsstrategie der Bundesregierung dies jedoch eher untergeordnet, zum Beispiel in dem allgemeinen Punkt „Digitale Kompetenzen bei allen Anwenderinnen und Anwendern fördern". Hierbei geht es um die verstärkte Sensibilisierung und die Steigerung von Cyberkompetenz in der Bevölkerung. Wünschenswert wäre jedoch eine starke Betonung, Fachkräfte für Cybersicherheit in der Aus- und Fortbildung noch besser zu unterstützen.

Das gilt auch mit Blick auf das Vorhaben, mehr Souveränität in der Cybersicherheit zu erlangen, eine Aufgabe, die sich nicht nur durch Technologie lösen lässt.

Keine digitale Souveränität ohne starke IT-Sicherheit in Deutschland und in der EU

Die Cybersicherheitsstrategie 2021 erklärt: „Die Strategie stärkt die Digitale Souveränität und damit die sichere Digitalisierung unseres Landes. Hierzu wird die deutsche Digitalwirtschaft durch gezielte Förderung von Schlüsseltechnologien und die Vernetzung mit relevanten Forscherinnen und Forschern vorangebracht."

Dazu RA Karsten U. Bartels LL.M., stellvertretender TeleTrusT-Vorstandsvorsitzender: „Wenn wir eine technologische und digitale Souveränität Deutschlands und Europas wollen, muss die Politik in den nächsten zwei Legislaturperioden die IT-Sicherheit massiv stärken." Technologische und digitale Souveränität kann nur durch ein zielgerichtetes und langfristiges Vorgehen erfolgreich umgesetzt werden, so TeleTrusT.

Es zeigt sich: Um die Cybersicherheit in Deutschland zu stärken, gilt es, den neuen Fünf-Jahres-Plan zur Cybersicherheit an verschiedenen Stellen weiterzuentwickeln. Neben der Konkretisierung der Maßnahmen muss noch an der Einsicht gearbeitet werden, dass sich Cybersicherheit nicht erhöhen lässt, indem man die Schließung von Schwachstellen verzögert. Ebenso sollte der Fachkräftemangel noch stärker in den Blick genommen werden, wenn es um Förderprogramme in der Cybersicherheit geht. Nicht zuletzt ist es wichtig zu verstehen, dass sich eine digitale Souveränität nur mit einer starken Cybersicherheit und Cybersicherheitsbranche erzielen lässt. Wer also die Cybersicherheit im Land fördern will, sollte die entsprechende Industrie dabei stärker berücksichtigen. □

Wichtige Datenschutz-Themen für 2021

Das Thema Datenschutz lässt die deutschen Unternehmen schon seit Jahren nicht mehr los und spätestens seit dem Schrems-II-Urteil des EuGH gehört zu den Problemfeldern auch der Datenaustausch mit Drittstaaten. Was die aktuelle Datenschutzlage für Unternehmen bedeutet, erläutert Dr. Marc Maisch, Fachanwalt für IT-Recht, im Gespräch mit Security-Insider.

Von Peter Schmitz, Security-Insider

Bild: peterschreiber.media/stock.adobe.com

Die neuen Standardvertragsklauseln (SCC) haben aus Unternehmersicht nicht nur Vorteile. Sie verpflichten Unternehmen in Zukunft unter anderem zur Datentransfer-Folgenabschätzung.

Die Kommission der Europäischen Union hat neue Standardvertragsklauseln (SCC) veröffentlicht. Wieso sind neue SCC notwendig geworden und was müssen Unternehmen jetzt tun?

Marc Maisch: Bei den SCC handelt es sich um Musterverträge, die eine geeignete Garantie nach Art. 46 DSGVO darstellen sollen, wenn personenbezogene Daten in Drittstaaten, z.B. die USA, übermittelt werden. Eine „geeignete ⇨

Garantie“ ist die rechtliche Erlaubnis, Daten in ein (aus EU-Sicht) unsicheres Land zu übermitteln. Die „alten“ Standardvertragsklauseln stammten aus der Zeit, bevor die Datenschutzgrundverordnung in Kraft getreten ist. Auch das so bedeutende Schrems II-Urteil des EuGH vom 16.7.2020 war natürlich auch nicht berücksichtigt. Aus diesem Grund wurden die neuen SCC-Klauseln erstellt.

Als Unternehmer sollte man neue Verträge nur nach den neuen SCC abschließen bzw. danach fragen. Diejenigen Verträge, die nach den alten SCC abgeschlossen wurden, gelten bis einschließlich 27.12.2022. Bis dahin sollten diejenigen Partner, die im EU-Ausland ihren Sitz haben und mit welchen ein SCC abgeschlossen wurde, kontaktiert werden, um die Verträge zu erneuern. Bis zum 28.12.2022 sollten alle bislang implementierten „alten“ SCC durch die neuen „Cross-Border SCC“ ersetzt werden.

Bringen die neuen Standardvertragsklauseln jetzt endlich Rechtssicherheit für deutsche Unternehmen?

Marc Maisch: Wenn es nach dem EU-Kommissar für Justiz, Didier Reynders, geht, wurden mit den neuen Standardvertragsklauseln benutzerfreundliche Instrumente entwickelt, auf die sich Unternehmen „voll und ganz verlassen können“. Die neuen Klauseln helfen zwar insbesondere kleinen und mittelständischen Unternehmen, die Anforderungen an eine sichere Datenübermittlung zu erfüllen. Man darf jedoch nicht außer Acht lassen, dass es nicht ausreichend ist, die SCC lediglich zu unterschreiben. Denn erstens müssen Unternehmen darüber hinaus Einzelfallprüfungen vornehmen, um eine Risikobewertung zu treffen. Und zweitens nehmen die neuen SCCs den Unternehmen nicht die Pflicht ab, im Fall von Drittstaatenübermittlungen in Drittstaaten geeignete Schutzmaßnahmen, z.B. Pseudonymisierung oder Verschlüsselung, zu evaluieren und zu treffen, wie der Europäische Datenschutzausschuss mit seinen Empfehlungen bekräftigt hat.

Haben die neuen Standardvertragsklauseln auch neue Pflichten für deutsche Unternehmen „im Gepäck“?

Marc Maisch: Die neuen SCC haben aus Unternehmersicht nicht nur Vorteile. Sie verpflichten Unternehmen in Zukunft unter anderem zur Datentransfer-Folgenabschätzung, also dazu, sich davon zu überzeugen, dass der entsprechende Vertragspartner aus dem Drittstaat in der Lage ist, seinen Pflichten aus den aktuellen SCC nachzukommen. Diese Datentransfer-Folgenabschätzung muss dokumentiert und den Aufsichtsbehörden auf Verlangen vorgelegt werden.

Es wird eine Einzelfallprüfung des Datenschutzniveaus (sog. Transfer Risk Assessment) nötig, bei der der Vertragstext und das tatsächliche Datenschutzniveau überprüft werden. Diese

Bild: Gorodenkoff/stock.adobe.com

Wer eine Website oder App betreibt, muss künftig die datenschutzrechtlichen Vorgaben des TTDSG beachten.

kann z.B. mithilfe eines Fragenkatalogs an den Verarbeiter im Drittstaat stattfinden. Dabei obliegt es dem Verantwortlichen zu überprüfen, ob der Vertragspartner alle notwendigen Maßnahmen ergriffen hat, um ein ausreichendes Schutzniveau zu garantieren.
Neu ist außerdem die Pflicht zur Abwehr von Regierungsanfragen, die den Anforderungen der Standardschutzklauseln widersprechen, und zum Informieren der zuständigen Aufsichtsbehörde über die Anfragen. Derartige Selbstverpflichtungen, die man bereits aus Amazon Web Services-Verträgen kennt, wird man nun im Zusammenhang mit den neuen SCC häufiger lesen.

Ende Mai hat ja der Bundesrat dem Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) zugestimmt. Das TTDSG soll mehr Rechtssicherheit und Rechtsklarheit zum Schutz der Privatsphäre in der digitalen Welt schaffen, wenn es am 1. Dezember in Kraft tritt. Was kommt da jetzt schon wieder auf die deutsche Wirtschaft zu?

Marc Maisch: Der Gesetzgeber hat mit dem TTDSG, das grundsätzlich viele Parallelen zu der alten, aber immer noch gültigen e-Privacy-Richtlinie hat, diese endlich in nationales Recht umgesetzt und einen neuen Regelungsrahmen für den Einsatz von Cookies und Tracking geschaffen, der einen wirksamen Schutz der Privatsphäre gewährleisten soll. Es soll die Rechtsunsicherheit bei Verbrauchern, Dienstanbietern und Aufsichtsbehörden auflösen, die aus dem Durcheinander von Regelungen in der Datenschutzgrundverordnung, dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz (TKG) entstanden ist.
Wer eine Website oder App betreibt, muss künftig die datenschutzrechtlichen Vorgaben des TTDSG beachten. Dazu sind auch Unternehmen verpflichtet, die keine Niederlassung in Deutschland haben, wenn von ihnen Dienstleistungen in Deutschland erbracht werden.
In § 19 Abs. 4 TTDSG stellt der Gesetzgeber klar, dass technische und organisatorische Maßnahmen gegen Störungen getroffen werden müssen, die den Stand der Technik berücksichtigen müssen, wobei anerkannte Verschlüsselungsverfahren genannt werden. Es müssen insofern zusätzlich geeignete Maßnahmen im Hinblick auf die Informationssicherheit implementiert werden. In diesem Zusammenhang betont der Gesetzgeber wiederholt das Prinzip der Datenminimierung; soweit es technisch zumutbar ist, soll die Nutzung von Telemedien und ihre Bezahlung anonym oder unter einem Pseudonym ermöglicht werden. Händler werden daher prüfen müssen, ob es nötig ist, Bestellungen auch über ein Gastkonto zu ermöglichen. Zudem findet sich eine Neuerung in den Regelungen zu § 25 TTDSG: Danach müssen Webseiten-Betreiber eine aktive und informierte Einwilligung von jedem Besucher einholen, wenn sie auf ihrer Webseite Cookies oder vergleichbare Technologien zum Speichern oder Abrufen auf den Endgeräten verwenden. Cookie-Banner sind also (leider) gekommen, um zu bleiben, und das Datenschutzrecht wird weiter viele Neuerungen und Überraschungen für deutsche Unternehmen zu bieten haben. □

Über Dr. Marc Maisch


Bild: M. Maisch

Dr. Marc Maisch ist Rechtsanwalt, Fachanwalt für IT-Recht, Datenschutzbeauftragter (TÜV) und Gastdozent für Cyber Security & Compliance an der HWZ Hochschule für Wirtschaft Zürich.

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, Dr. Andreas Bergler/ab (-141) – CvD/ltd. Redakteur

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:
Sabine Assum (-194), Fax (-228)
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, Cloud-Insider, DataCenter-Insider, Dev-Insider, Healthcare-Insider, IP-Insider, Security-Insider** und **Storage-Insider**.

Inserenten

Achelos GmbH	Paderborn	https://www.achelos.de/de/	20
AOE GmbH	Wiesbaden	https://www.aoe.com/de/	26
G DATA Software AG	Bochum	https://www.gdata.de/	38, U2
INSYS MICROELECTRONICS GmbH	Regensburg	https://www.insys-tec.de/	16
NCP engineering GmbH	Nürnberg	https://www.ncp-e.com/de/	34, U4
netfiles GmbH	Burghausen	https://www.netfiles.de/	42
procilon GmbH	Taucha bei Leipzig	https://www.procilon.de/	U3
retarus GmbH	München	https://www.retarus.com/de/	46
Rohde & Schwarz Cybersecurity GmbH	München	https://www.rohde-schwarz.com/cybersecurity/	12
Securepoint GmbH	Lüneburg	https://www.securepoint.de/	8
SoSafe GmbH	Köln	https://sosafe.de/	50
TDT AG	Essenbach	https://tdt.de/de/	30
Vogel IT-Akademie	Augsburg	https://www.vogelitakademie.de/	5

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
Auffallend flexibel
Mehr als einfaches VPN: Bleiben Sie mit Ihrem Unternehmen
in JEDER Situation produktiv und sicher!
Ermöglichen Sie Homeoffice und mobiles Arbeiten –
mit skalierbaren VPN-Lösungen und flexiblen Lizenzmodellen
für schwankenden Bedarf.
Wie flexibel sind Sie?
www.ncp-e.com
NCP
SECURE COMMUNICATIONS
my access
SecurITy
made
in
Germany