OKTOBER 2020

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

MADE IN GERMANY

DSGVO
IDENTITY & ACCESS MANAGEMENT
VERSCHLÜSSELUNG
ADVANCED PERSISTENT THREATS
ENDPOINT PROTECTION
BACKDOORS
PATCH MANAGEMENT
RANSOMWARE
MANAGED SECURITY SERVICES

Powered by:

SecurITy made in Germany

VOGEL IT MEDIEN

Eine Publikation von IT-BUSINESS SECURITY INSIDER


G DATA
TRUST IN
GERMAN
SICHERHEIT
Kaffee geholt.
Daten weg.
Desktop sperren rettet
Unternehmen.
Schaffen Sie IT-Sicherheitsbewusstsein
gdata.de/awareness-training

IT-Sicherheitslösungen im Home Office

Liebe Leserinnen und Leser,
die derzeitige "coronabedingte" flächendeckende Umstellung auf mobiles Arbeiten, Home Office, Datenübermittlung und Remote-Authentifizierung stellt erhöhte Anforderungen an die IT-Sicherheit, um keine neuen Gelegenheiten für Angreifer zu schaffen, die sich die Gunst der Stunde zunutze machen.
Der Bundesverband IT-Sicherheit e.V. hat dies zum Anlass genommen und befristet kostenfreie IT-Sicherheitslösungen seiner Mitglieder gelistet, um betroffenen Anwendern Unterstützung zu bieten.
Die Situation führt erzwungenermaßen zu einer enormen Digitalisierungsbeschleunigung. In kürzester Zeit werden zu Hause Arbeitsplätze nachgebildet, um Betriebsstrukturen digital aufrechtzuerhalten. Während technisch gut aufgestellte Unternehmen ihre Mitarbeiter mit professionellem Equipment ausrüsten, ist anderswo Improvisation und Pragmatismus gefragt. Dabei kann die IT-Sicherheit auf der Strecke bleiben.
Nicht jedes Unternehmen verfügt über die IT-Infrastruktur, um das Home Office der Mitarbeiter adäquat zu sichern. Gerade jetzt schwärmen digitale Raubritter aus, um die Gunst der Stunde zu nutzen und mit Spam, Phishing und Malware, Identitätsdiebstahl und Datenklau schnelle Beute zu machen. In etlichen Fällen werden hilfsweise private Hard- und Software sowie Netzanbindungen genutzt, die es den Tätern noch vereinfachen.
In diesem Zusammenhang sei auch auf den TeleTrusT-Leitfaden "E-Mail-Verschlüsselung" hingewiesen. Die Verschlüsselung von E-Mails stellt einen wesentlichen Schritt zu verbesserter Kommunikationssicherheit dar.

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

Die E-Mail ist nach wie vor das Hauptkommunikationsmittel im Geschäftsleben. Täglich werden vertrauliche Informationen, auch unternehmenskritische Vorgänge und sensible Daten, im ungesicherten Modus versendet. Dabei sind die übermittelten Informationen nicht nur für Fremde lesbar, sondern können auch auf dem Transportweg manipuliert oder gelöscht werden.
Die Themenschwerpunkte dieser Sonderpublikation laufen unter der Überschrift "IT Security made in Germany". Der Hervorhebung eines Produktes als "Made in Germany" kommt eine prädikatsgleiche Wirkung zu, die die Angabe als ein Gütesiegel erscheinen lässt und eine besondere Qualitätsvorstellung der Abnehmer hervorruft.
Gerade in solchen Zeiten wie jetzt sollte das Herkunftsland Deutschland mit bestimmten technischen Standards und hochwertiger Verarbeitung assoziiert werden.
Diese Publikation gibt Orientierung und fasst die wichtigsten Maßgaben für die digitale Transformation und das sichere Arbeiten zusammen.
Gemeinsam mit den TeleTrusT-Mitgliedern wünsche ich Ihnen eine spannende Lektüre! □

TeleTrusT-Initiative "IT Security made in Germany"

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

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

SINA Communicator H

Das Multikrypto-Telefon für die Post-ISDN Ära

Telefonieren, Chatten, Kollaborieren, Thin-Clients nutzen, Dateien austauschen und vieles mehr – zulassungsfähig bis GEHEIM.
Der SINA Communicator H bietet All-IP-Technologie auf höchstem Sicherheitsniveau, inklusive moderner NATO-Protokolle. Bedarfsgerecht und zukunftssicher.

secunet.com **protecting digital infrastructures**

secunet

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 17.09.2020)

- A N T I L|E|A|K|S.D E
- 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
- apsec Applied Security GmbH
- ASOFTNET
- ATIS systems GmbH
- ausecus GmbH
- Avira GmbH & Co. KG
- Bank-Verlag GmbH
- BCC Unternehmensberatung GmbH
- Bechtle GmbH & Co. KG
- Beta Systems IAM Software AG
- Biteno GmbH
- Blue Frost Security GmbH
- bowbridge Software GmbH
- Build38 GmbH
- Bundesdruckerei GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- certgate GmbH
- CERTIX IT-Security GmbH
- CGM Deutschland AG
- Cherry GmbH
- CHIFFRY GmbH
- C-IAM GmbH
- Cloudsitter GmbH
- CoCoNet Computer-Communication Networks GmbH
- Cognitec Systems GmbH
- COMback Holding GmbH
- comcrypto GmbH
- comforte AG
- comtime GmbH
- Condition-ALPHA Digital Broadcast Technology Consulting
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- CONTURN Analytical Intelligence Group GmbH
- Crashtest Security GmbH
- CryptoMagic GmbH
- Cryptshare AG
- cv cryptovision GmbH
- dacoso data communication solutions GmbH
- dal33t GmbH
- DATAKOM GmbH
- datenschutzklinik
- DATUS AG
- DERMALOG Identification Systems GmbH
- Detack GmbH
- Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG
- DFN-CERT Services GmbH
- dhpg IT-Services GmbH Wirtschaftsprüfungsgesellschaft
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- ditis Systeme Niederlassung der JMV GmbH & Co.
- DocRAID(R) – professional data privacy protection
- DoctorBox GmbH
- DRACOON GmbH
- DriveLock SE
- D-Trust GmbH
- eCom Service IT GmbH
- ecsec GmbH
- e-ito Technology Services GmbH
- Enginsight GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- exceet Secure Solutions GmbH
- Fiducia & GAD IT AG
- floragunn GmbH
- FSP GmbH
- FZI Forschungszentrum Informatik
- G Data Software AG
- genua GmbH
- Giegerich & Partner 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
- intelliCard Labs GmbH
- Intelligent Minds UG
- IS4IT Kritis 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 enthalten (keine "Backdoors").
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 und ist deshalb tagesaktuellen Änderungen unterworfen. Die aktuelle Liste der Unternehmen, denen die Nutzung des Vertrauenszeichens derzeit eingeräumt wird, können Sie einsehen unter: www.teletrust.de/itsmig/zeichentraeger/ □

- isits AG International School of IT Security
- ISL Internet Sicherheitslösungen GmbH
- itWatch GmbH
- Johannes Kresse
- keepbit IT-SOLUTIONS GmbH
- KikuSema GmbH
- KIWI.KI GmbH
- KnowledgeRiver GmbH
- LANCOM Systems GmbH
- limes datentechnik® gmbh
- Link11 GmbH
- Linogate GmbH
- LocateRisk UG
- maincubes one GmbH
- MaskTech GmbH
- MATESO GmbH
- Matrix42 AG
- MB Connect Line GmbH Fernwartungssysteme
- Mentana Claimsoft GmbH
- metafinanz Informationssysteme GmbH
- M&H IT-Security GmbH
- MTG AG
- NCP engineering GmbH
- NEOX NETWORKS GmbH
- Net at Work GmbH
- netfiles 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
- P-ACS UG
- PFALZKOM GmbH
- PHOENIX CONTACT Cyber Security GmbH
- Pix Software GmbH
- PPI Cyber GmbH
- PRESENSE Technologies GmbH
- procilon IT-Solutions GmbH
- PROSTEP AG
- Protforce GmbH
- PSW GROUP GmbH & Co. KG
- QGroup GmbH
- QuoScient GmbH
- retarus GmbH
- Rhebo GmbH
- RheinByteSystems GmbH
- Rohde & Schwarz Cybersecurity GmbH
- r-tec IT Security GmbH
- SAMA PARTNERS Business Solutions GmbH
- sayTEC AG
- Schönhofer Sales and Engineering GmbH
- SCHUTZWERK GmbH
- SC-Networks GmbH
- Secomba GmbH
- secrypt GmbH
- secucloud GmbH
- SECUDOS GmbH
- secunet Security Networks AG
- Securepoint GmbH
- Secure Service Provision GmbH
- secuvera GmbH
- SerNet GmbH
- signotec GmbH
- Softline AG
- SoSafe GmbH
- Steen Harbach AG
- Stefan Lanz Consulting
- Steganos Software GmbH
- SVA System Vertrieb Alexander GmbH
- Symlink GmbH
- syracom consulting AG
- TDT AG
- teamwire GmbH
- Tenzir GmbH
- TESIS SYSware Software Entwicklung GmbH
- TE-SYSTEMS GmbH
- T-Systems International GmbH
- turingpoint GmbH
- TÜV Informationstechnik GmbH
- Uniki GmbH
- Uniscon GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- Veronym Holding GmbH
- virtual solution AG
- Vulidity GmbH
- WMC Wüpper Management Consulting GmbH
- Würzburger Versorgungs- und Verkehrs GmbH
- XignSys GmbH
- XnetSolutions KG
- Zertificon Solutions GmbH

Nachweisbare IT-Sicherheit mit flexiblen Software-Tools und Beratung

IT-Sicherheit und Datenschutz sind die zentralen Themen im elektronischen Datenverkehr und betreffen alle Branchen. Eine Vielzahl von Cyberattacken und Bedrohungspotenzialen sind zur Realität geworden, und die Methoden der Angreifer werden immer professioneller. Der Wert von Cybersicherheit rückt immer stärker in den Fokus.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) setzt in verschiedenen Bereichen über Technische Richtlinien Standards für die Einschätzung von Sicherheitsmerkmalen. Mit der TR-3116-4 richtet sich das BSI direkt an Diensteanbieter für den sicheren Betrieb von Web-Diensten und fixiert in der dazugehörigen Checkliste relevante Parameter.

Wie können diese Sicherheitseigenschaften überprüft werden? Mit genügend Fachwissen ist z. B. eine manuelle Prüfung möglich. Allerdings ist das zeitaufwändig und meist nicht reproduzierbar. Ideal wäre eine vollautomatische Prüfung.

TLS Checklist Inspector

Kostenloser Website-Check gemäß BSI-Vorgaben

achelos bietet mit der Produktneuheit TLS Checklist Inspector die kostenfreie automatische Sicherheitsprüfung von Websites über ein Web-Portal an. Angesprochen sind Unternehmen jeglicher Größe, die den Nachweis einer sicheren TLS-Netzwerkverbindung gemäß den Anforderungen der Checkliste des Bundesamts für Sicherheit in der Informationstechnik (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.

Heinfried Cznottka
Director Security Solutions

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.

Das erste Testergebnis (Testreport) ist visuell aufbereitet, sofort am Bildschirm verfügbar und kostenfrei. Detailreports erhalten Interessierte auf Anfrage und gemäß Aufwandsentschädigung.

Insbesondere in der aktuellen Situation ist eine sichere digitale Präsenz des Unternehmens von entscheidender Bedeutung, sie dient als Signal für Kunden und als Schutz für sensible Unternehmensdaten.

Aktuell ist der TLS Checklist Inspector von achelos die einzige am Markt verfügbare Lösung, um die Erfüllung des BSI-Standards auf einfache Weise nachzuweisen.

Link zum TLS Checklist Inspector:
www.tls-check.de

Sicherheit für vernetzte Lösungen in Industrie und Verkehr

Eine auf Public-Key-Infrastrukturen basierende Cybersicherheit bildet die Grundlage für die intelligente Vernetzung von Geräten, Maschinen und Produkten, sei es im industriellen Umfeld zur Digitalisierung von Prozessen (Industrie 4.0) oder bei der Entwicklung zukünftiger vernetzter Verkehrslösungen.

PKI System Consulting

Gemeinsam eine optimale und individuelle PKI-Lösung gestalten

achelos agiert partnerschaftlich und bietet umfassende Beratungsleistungen beim Aufbau neuer oder der Migration existierender Public-Key-Infrastrukturen. Das Angebot reicht von der Systemplanung über die Systembereitstellung bis hin zur Inbetriebnahme. Dabei berücksichtigt achelos anwendungs- und kundenspezifische Anforderungen und Standards sowie bestehende Prozesse und Zertifizierungen (z. B. ISO 27001).
Als zertifizierter Partner der Firma PrimeKey bietet achelos neben der Beratung auch Software, Hardware und Support.

achelos begleitet PKI-Projekte von Anfang an

Systemplanung:

- Anforderungs-Engineering: Erfassen und Verwalten funktionaler, technischer, organisatorischer Anforderungen
- Sicherheitsberatung: Erfassen der Sicherheitsziele und -anforderungen, Bedrohungsszenarien und Risikoanalyse, Rollenmodelle und Zertifikatsprofile
- IT-Lösungsarchitektur: Planung der IT-Erweiterung, PKI-Architektur, Migration, Verfügbarkeit und Backup
- Projektmanagement: Planung und Sicherstellen des Projekterfolges
- Proof of Concept

Systemlieferung:

- Kundenindividuelle Systemintegration der Registrierungs- und Validierungsinstanzen an verbundene Systemkomponenten
- Unterstützung bei der Systeminstallation und -konfiguration
- Trainings: Schulungen des Betriebspersonals und der IT-Administration

Inbetriebnahme:

- Qualitätssicherung durch Abnahmetests
- Dokumentation
- Übergabe der PKI-Lösung in den Betrieb

Weitere Informationen zum Thema PKI System Consulting:
www.achelos.de/de/pki-system-consulting.html

IT-Sicherheit und Datenschutz zählen zur DNA von achelos!

Das achelos-Team setzt sich aus anerkannten Sicherheits- und Technologie-Consultants mit globaler Projekterfahrung zusammen.
Gerne stellen wir Ihnen unser Expertenwissen zur Verfügung – sprechen Sie uns an! ■

Dr. Michael Jahnich
Director Business Development Mobility

Zwischen Schutz und Gefahr: das Home Office

Bisher war Home Office in vielen Unternehmen eher eine Ausnahme. Aufgrund der Schutzmaßnahmen zur Eindämmung von Covid-19 ist es derzeit zum Standard geworden. Gleichzeitig steigt allerdings das Risiko für die Unternehmenssicherheit.

Von Ann-Marie Struck, IT-BUSINESS

© CROCOTHERY/stock.adobe.com

Fast 50 Prozent der Arbeitnehmer arbeiten seit dem Ausbruch des Coronavirus im Home Office. So das Ergebnis einer Umfrage des Bitkom. Einerseits hat die Arbeit am heimischen Schreibtisch viele Vorteile wie länger schlafen, kürzere Arbeitswege und keine lauten Kollegen, andererseits bildet das Home Office ein Risiko für die IT-Sicherheit.

Diese Ansicht bestätigt auch Eric Kaiser, Product Executive bei Securepoint: „Grundlegend muss man verstehen, dass ein Home Office ein unsicherer Raum mit unbekanntem IT-Sicherheitsniveau ist. Dort lauern viele zusätzliche Sicherheitsrisiken in Form von privaten und ungesicherten Geräten, die sich im selben Netzwerk befinden. Das ist ein Problem, da die Netzwerkanbindung unzureichend abgesichert ist, ohne Verschlüsselung und Authentisierung. Vergrößert wurde das Risiko zudem durch die Geschwindigkeit, mit der in der Coronakrise auf Homeoffice umgestellt wurde. Dabei wurden viele sonst vorhandene gute Vorsätze über Bord geworfen."

Cyberkriminelle nutzen Krise aus

Gerade jetzt kommt es jedoch vermehrt zu Cyberangriffen, denn durch das isoliertere Arbeiten und die größere Distanz zu Kollegen und der Firmen-Infrastruktur sind Mitarbeiter attraktivere Ziele für Angriffe. Cyberkriminelle

versuchen mit Spam, Phishing, Malware, Identitätsdiebstahl und Datenklau leichte Beute zu machen. Diese Risiken sind jedoch einer Umfrage von AT&T unter 800 Cyber-Sicherheitsexperten in Großbritannien, Frankreich und Deutschland zufolge den IT-Verantwortlichen durchaus bewusst. Demnach haben 70 Prozent der großen Unternehmen in Europa mehr Cyberangriffe bei Remote-Arbeit befürchtet. Obwohl 88 Prozent der Befragten ihre IT-Security vorab für ausreichend hielten, sind nun 55 Prozent der Ansicht, dass die weit verbreitete Arbeit aus dem Home Office ihre Unternehmen mehr oder viel anfälliger für Cyberangriffe macht.

IT Security im Home Office

Trotz Krisensituation und schneller Home-Office-Umstellung sollten Unternehmen die IT Security daher nicht außer Acht lassen. Kaiser rät dazu, Vorkehrungen wie an jedem normalen IT-Arbeitsplatz zu treffen, also eine optimale Absicherung der Rechner sowie der Verbindungen mit Mehrfaktor-Authentisierung. Insbesondere stellen die diversifizierenden Zugangspunkte und Arbeitsplätze eine gesonderte Herausforderung an die IT Security dar. Dabei ist laut Kaiser das Wichtigste ein richtiges Konzept und die richtige Behandlung unterschiedlicher Geräte. „Das Zauberwort heißt Zero Trust", erklärt Kaiser. „Das bedeutet, dass niemand, nur weil er Benutzername und Passwort kennt, Zugang erhält. Jedes Gerät und jede Verbindung wird zunächst als nicht vertrauenswürdig eingestuft, und erst nach einer mehrstufigen Bestätigung wird der Zugriff auf Unternehmensressourcen freigegeben. Unternehmensressourcen werden so niemals direkt aus dem Internet zugänglich gemacht."

Sichere Kommunikation am Arbeitsplatz

Eine weitere Sicherheitslücke bilden auch die Kommunikationstools, denn neben der klassischen Telefonie kommen im Home Office nun auch vermehrt Kollaborationslösungen zum Einsatz. Doch sowohl UCC als auch IP-Telefonie benötigen Sicherheit. Um die IT-Sicherheit am modernen Arbeitsplatz langfristig zu verbessern, hat der IT-Security-Hersteller Securepoint eine Partnerschaft mit dem Hersteller von IP-Telefonanlagen und -Kommunikationslösungen Starface geschlossen. „Wir bündeln unsere Kräfte, indem wir Partner-übergreifende Vertriebsunterstützung, gemeinsame Schulungen und Produkt-Bundles zur Verfügung stellen", erläutert Kaiser.

Bild: Securepoint

Eric Kaiser, Product Executive bei Securepoint: „Wenn ich IT-Sicherheit einkaufe, ist das vor allem eine Frage des Vertrauens in den Hersteller. ‚IT Security made in Germany' steht als Garant für eine freiheitliche Gesellschaft."

Siegel für Sicherheit in unsicheren Zeiten

Dabei spielt in Krisenzeiten vor allem Vertrauen eine große Rolle, vor allem bei IT Security. Das TeleTrusT-Vertrauenszeichen „IT Security made in Germany" soll Anwendern eine Orientierung geben, wie Kaiser veranschaulicht: „Wenn ich IT-Sicherheit einkaufe, ist das vor allem eine Frage des Vertrauens in den Hersteller, denn in die Produkte kann man meist nicht reinschauen. In Zeiten von Edward Snowden, der uns gezeigt hat, dass Regierungen Daten mitlesen, und in Zeiten, in denen der EUGH klargestellt hat, dass die Datenschutz-Vereinbarung mit den USA keine Gültigkeit hat, steht ‚IT Security made in Germany' als Garant für eine freiheitliche Gesellschaft." □

VPN-Software für „VS-NfD“ nach BSI-Richtlinien

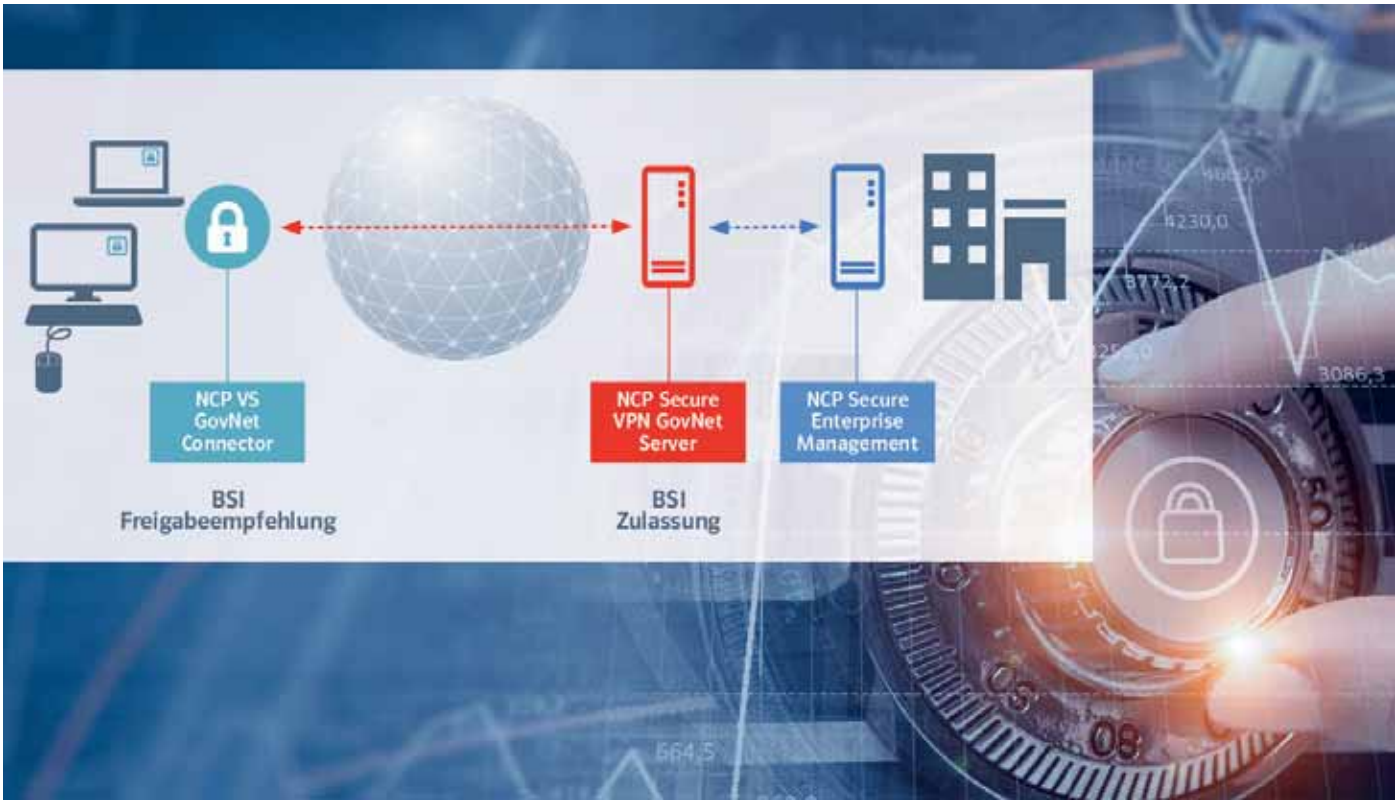
Corona hat in diesem Jahr vor allem im Public Sector das Thema Home Office und die Digitalisierungsstrategien vorangetrieben. Gerade Behörden, Ämter und geheimschutzbetreute Unternehmen übermitteln bei der täglichen Kommunikation sensible Daten mit höchst schützenswerten Informationen von Bürgern oder hochsensiblen Projekten.

NCP SECURE COMMUNICATIONS

Bei der sicheren Kommunikation von „Verschlusssachen – Nur für den Dienstgebrauch“ (VS-NfD) spielt die Sicherheit aller eingesetzten Hardware- und Softwarekomponenten eine besonders große Rolle. So auch bei der unter anderem für Home Office eingesetzten VPN-Lösung, die den Empfehlungen und Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen muss.
Regierungsbeamte, Verwaltungsangestellte und Mitarbeiter müssen in der Lage sein, auf die für sie bereitgestellten Netzwerkressourcen und Daten schnell und einfach, aber vor allem sicher zuzugreifen. Der **NCP VS GovNet Connector** hat als Software-Client eine Freigabeempfehlung vom BSI, der **NCP Secure VPN GovNet Server** verfügt über eine BSI-Zulassung. Beide Softwarekomponenten können im Einsatzverbund zur sicheren Bearbeitung und Übertragung von VS-NfD eingesetzt werden.
In Kombination mit dem **NCP Secure Enterprise Management (SEM)** profitieren Anwender durch Vorteile der zentralen Administrierbarkeit. Der Einsatz nach VS-NfD ist in Abstimmung mit dem BSI möglich.

IT Security Made in Germany für den Public Sector

NCP verfolgt das Motto „IT Security Made in Germany“ auch als Qualitätsanspruch und setzt auf modernste Technologien und Standards für Verschlüsselung (ECC) sowie starke Authentisierung. Praxisnahe Features wie die sichere Hot Spot-Anmeldung, die VPN Path Finder Technology (Fallback IPsec/HTTPS) und Funktionen im Rahmen der Network Access Control (Endpoint



Policy) ermöglichen sicheres und gleichzeitig störungsfreies Arbeiten von zuhause oder unterwegs.
Das NCP SEM automatisiert und vereinfacht zahlreiche Administrationsabläufe wie schnellen Rollout, ein zentrales Rechte- und Konfigurationsmanagement sowie eine einfache Umsetzung von Richtlinienänderungen. Seamless Roaming sorgt dafür, dass „Always On“ hält, was es verspricht: unterbrechungsfreies Arbeiten trotz Wechsel des Übertragungsmediums.

VS-NfD auf Standard Windows 10-Rechnern

Anwender können durch den Einsatz der NCP Software mit Windows 10-Rechnern von jedem Standort weltweit auf das zentrale Datennetz zugreifen und dieses auch VS-NfD sicher bearbeiten. Durch Standard-Schnittstellen ist die Kombination mit vom BSI zugelassener Authentisierungshardware (beispielsweise SmartCard-Leser) oder Software (z.B. Festplattenverschlüsselung) problemlos möglich.
Die vom BSI geforderte Verifizierung der Signatur nach dem Prinzip elliptischer Kurven (Elliptic Curve Cryptography) wird ebenso unterstützt wie Zertifikate bzw. SmartCards in einer PKI (Public Key Infrastructure). Optional können OTP-Lösungen (One Time Passwort) oder eine biometrische Authentisierung genutzt werden, z.B. über Fingerabdruck- oder Gesichtserkennung. ■

Informieren Sie sich über die Einsatzmöglichkeiten und weitere Funktionen wie Quality of Service oder die im Client integrierte Personal Firewall unter **www.ncp-e.com**.

Home Office mit dem privaten Computer – kann das sicher sein?

Seit Mitte März 2020 befindet sich die deutsche Wirtschaft in einer Ausnahmesituation, die es per Anordnung des Infektionsschutzgesetzes (IfSG) erforderlich macht, die Mitarbeiter von Firmen soweit physisch voneinander zu trennen, dass von einer Minimierung der Ansteckungsgefahr durch Corona-Viren ausgegangen werden kann.

Von Thomas Scholz, Linogate

Dem kam man nach, indem man einige Mitarbeiter samt firmeneigenen Laptops mit vorinstallierten VPN-Clients nach Hause schickte. Viele Firmen stießen so jedoch bald an ihre Grenzen, denn es standen manchen Unternehmen schlicht nicht genug Laptops zur Verfügung.

Heute gilt: Das IfSG ist noch immer in Kraft, man hat sich jedoch eingestellt auf den Umgang mit den Home-Office-Anbindungen. Trotzdem scheut so mancher Unternehmer die Kosten, um jeden potenziellen Home-Office-Kandidaten mit einem Laptop auszustatten.

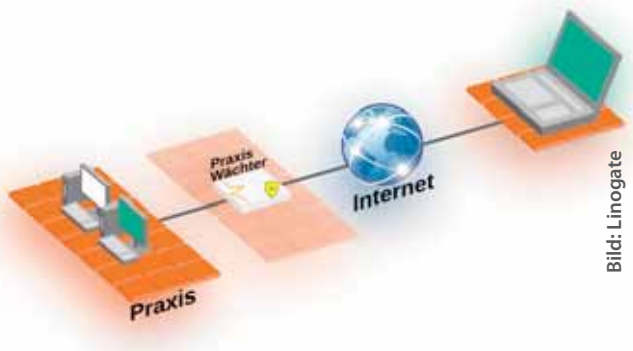


Bild: Linogate

Beispiel einer Arztpraxis, auf die über einen Laptop mit Web-Client von außerhalb sicher zugegriffen wird.

Home Office ohne VPN – und trotzdem sicher?

Manche Mitarbeiter wären in dieser außergewöhnlichen Situation auch bereit, ihren privaten Rechner für die Home-Office-Verbindung zur Firma zu nutzen. Zur Installation des benötigten VPN-Clients den Kollegen aus der IT-Abteilung an den privaten Rechner zu lassen, ist dann aber doch nicht jedermanns Sache. Alternativ dazu müsste der Mitarbeiter die VPN-Installation selbst in Angriff nehmen – für IT-Laien jedoch eine kaum zu lösende Aufgabe.

Es gibt jedoch auch eine andere, ebenfalls sichere Möglichkeit, mit jedem Rechner, der einen HTML5-fähigen Browser betreiben kann, über den Internet-Anschluss zuhause Zugriff auf Server in der Firma zu erhalten: den „Web-Client“. Um ihn zu betreiben, ist auf dem privaten Rechner keinerlei Installation von Software nötig, denn beim Web-Client handelt es sich um eine reine Browser-Anwendung. Der dafür eingesetzte Browser sollte lediglich auf den aktuellsten Stand gebracht werden, um HTML5 sicherzustellen. Der zentrale Sammelpunkt für alle per Web-Clients angeschlossenen Home

Offices befindet sich in der Firma auf einer Linux-basierten Internet-Firewall.

Wodurch ist die Home-Office-Verbindung gesichert?

Diese Firewall beinhaltet eine Reverse-Proxy-Funktion, welche als Verbindungsstelle für jeden Web-Client zur Authentifizierung mit hinterlegten Client-Zertifikaten konfiguriert werden kann. Die Proxy-Funktion agiert ähnlich wie ein Pförtner, welcher bestimmt, wer passieren darf und wer abgewiesen wird. Die Erstellung der Zertifikate erfolgt direkt auf der Firewall durch eine residente PKI. Die so erstellten Verbindungen können RDP-, VNC- und SSH-fähige Anwendungen über SSL verschlüsselt übertragen.

Welche Computer kann man zum Home-Arbeitsplatz machen?

So ist es möglich, fast alle PCs, Tablets und Smartphones mit gängigen Betriebssystemen wie Windows, MAC-OS, Linux und Android als Arbeitsplatz im Home Office zu betreiben. Zum Verbindungsaufbau aus dem Home Office gibt man im Adressfeld des Browsers folgendes ein:
https://Ziel-IP-Adresse der Firma/webclient
Danach werden Username und Passwort abgefragt, und man ist verbunden.

Wie ist die Arbeit über den Web-Client verglichen mit der Arbeit direkt in der Firma?

Der Administrator legt auf der Firewall in der Firma die Zugriffe für alle Web-Clients aus den Home Offices individuell so fest, dass jeder Mitarbeiter seine gewohnte Umgebung vorfindet, fast so, als ob er sich im Firmen-LAN befinden würde.
Bei der Nutzung des RDP-Protokolls für Zugriffe auf Terminal-Server, Arbeitsplatz-PCs oder zur Fernwartung sind ein paar Funktionen aufgrund des Sicherheitsmodells der Webbrowser nicht direkt möglich. Hier kommen Emulationen zum Einsatz, um auch solche Funktionen wie Zwischenablage für Text, Druck- und Dateiübertragungsfunktion trotzdem nutzbar zu machen.
Beim Einsatz des VNC-Protokolls auf MACs ist auch ein passiver Modus ohne Interaktionsmöglichkeit konfigurierbar, falls man User bewusst einschränken möchte.
Für SSH-Verbindungen kann der Benutzername vorgegeben werden und verschiedene Farbschemata und Schriftarten / Schriftgrößen können eingestellt werden.

Sicherheit durch 2-Faktor-Authentifizierung – es muss nicht immer VPN sein

Das Sicherheitsniveau einer IPSec-Authentifizierung ist sicherlich höher zu bewerten als eine Proxy-Authentifizierung über Client-Zertifikat. Um vergleichbare Sicherheit für den Web-Client zu erreichen, kann man als zweite Authentifizierung zeitbasierte Einmalpasswörter (TOTP) erzeugen (u. a. mit Google Authenticator).
Der große Vorteil gegenüber VPN zeigt sich auf der Home-Office-Seite, denn hier ist zur Nutzung des Web-Clients überhaupt keine Einrichtung nötig! Manche Firmen steigen bereits auf Web-Client um, obwohl sie genügend Firmen-Laptops haben: „Einfach, weil es einfacher ist.“ □

Der Autor


Bild: Linogate

Dipl. Ing. Thomas Scholz wurde im Jahre 2000 zum Geschäftsführer der Linogate GmbH berufen, als eine Neuausrichtung der GmbH zum Hersteller von Internet Firewalls vorgenommen wurde. Zugleich ist er Gesellschafter von Linogate.

So behalten Unternehmen die Kontrolle über eingehende E-Mails

Der neue Retarus-Service Predelivery Logic ermöglicht regelbasierte E-Mail-Workflows und -Policies aus der Cloud und bietet zudem weit mehr als eine bloße Policy Engine.

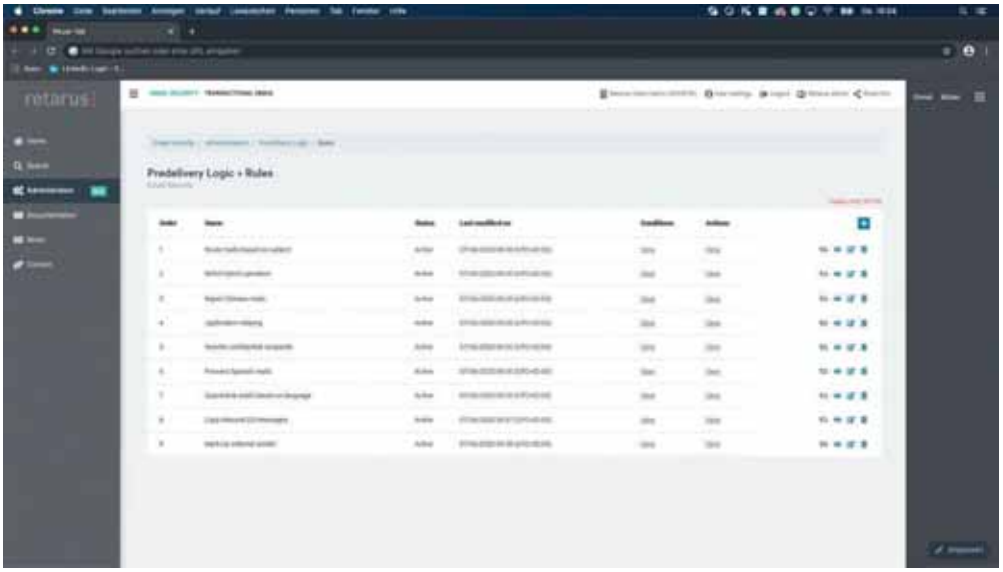
retarus:

E-Mail mit all ihren technischen und organisatorischen Herausforderungen stets unter Kontrolle zu behalten, stellt immer höhere Anforderungen an IT-Verantwortliche. Nicht nur, was das Routing innerhalb von Firmennetzen angeht. Auch Themen wie Prozessautomatisierung lassen sich immer weniger mit den Mitteln standardisierter Lösungen abdecken. Unternehmen benötigen mehr Kontrolle über den eingehenden E-Mail-Verkehr, idealerweise schon vor der Zustellung an die eigene Infrastruktur. Dafür hat der Münchner Cloud-Dienstleister Retarus den Service Predelivery Logic entwickelt.

Retarus Predelivery Logic analysiert anhand individueller Regelwerke E-Mails, leitet diese gegebenenfalls um und optimiert sie, bevor sie an die Unternehmensinfrastruktur weitergeleitet werden. Damit ermöglicht der Service IT-Verantwortlichen, den gesamten eingehenden E-Mail-Verkehr auf der Grundlage selbst definierter Regeln, jeweils bestehend aus Bedingungen und Aktionen, zu kontrollieren, zu organisieren, umzuleiten oder anzupassen. Flexible Kombinationsmöglichkeiten solcher Regeln ermöglichen nahezu unbegrenzte Einsatzszenarien. Dabei spielt es keine Rolle, ob das Unternehmen seine E-Mail-Infrastruktur on-premises oder als Cloud Service betreibt.

Workflow Automation: Mehr als nur Policy Engine

Mit der Predelivery Logic geht Retarus im Funktionsumfang deutlich über das hinaus, was im Markt gemeinhin als Policy Engine bezeichnet wird. Die Lösung bietet zwar ebenfalls ein User-abhängiges Routing von E-Mails an bestimmte Server beziehungsweise Standorte des Firmennetzes oder an Tochterfirmen. Jedoch liefert die Predelivery Logic darüber hinaus einen entscheidenden Beitrag zur Automatisierung und Beschleunigung von Geschäftsprozessen. So ist es beispielsweise möglich, E-Mails anhand ihres Inhalts oder ihrer Sprache weiterzuverarbeiten. Dadurch können zum Beispiel an den Support oder das Contact Center eingehende Nachrichten automatisch vor-



Mit Hilfe der Retarus Predelivery Logic lassen sich E-Mails zum Beispiel anhand ihres Inhalts, ihrer Herkunft oder ihrer Sprache weiterverarbeiten.

sortiert und an die richtige Abteilung in der entsprechenden Landesgesellschaft geroutet werden. Ebenso ist es möglich, E-Mails abhängig von aufgestellten Regeln vollautomatisch zu bearbeiten, etwa die E-Mail-Adresse umzuschreiben oder Schlagwörter in die Betreffzeile einzufügen.

Optimierte Infrastruktur, mehr Sicherheit

Mit Retarus Predelivery Logic lassen sich aber auch Regeln definieren, die über standardisierte Sicherheitsfunktionen hinausgehen. Beispielsweise können E-Mails, die von Absendern aus Ländern oder Regionen kommen, mit denen eigentlich keine Geschäftsbeziehungen bestehen, automatisiert an eine bestimmte Person zur Prüfung oder direkt in die Quarantäne weitergeleitet werden.

Maximale Kontrolle über eingehende E-Mails

„Wenn wir heute in Projekten mit unseren großen Enterprise-Kunden sprechen, ist das Feedback eindeutig. Zur Bewältigung der immer höher werdenden Komplexität ist ein intelligenterer und flexibler Ansatz gefragt. Gerade bei der Migration der E-Mail-Kommunikation in die Cloud“, sagt Martin Hager, Gründer und Geschäftsführer von Retarus. „Unternehmen möchten mehr Kontrolle über eingehende E-Mails, und zwar so früh wie möglich. Idealerweise lassen sich Regeln bereits vor der Zustellung an die eigene Infrastruktur anwenden. Denn für die Umsetzung vieler Regelwerke und Maßnahmen ist es meist zu spät, wenn betreffende E-Mails bereits unverarbeitet an die Server eines Unternehmens, Applikationen oder Postfächer zugestellt wurden.“

Weitere Informationen zur Retarus Predelivery Logic finden Sie unter www.retarus.de/predelivery-logic ■

Retarus auf der it-sa 365!

Treffen Sie uns vom 6. bis 8. Oktober 2020 virtuell auf itsa365.de.

Besuchen Sie auch unseren Vortrag: „Privacy Shield down! DSGVO-konforme Kommunikation aus der Cloud“

So holen CISOs mehr aus ihren Security-Budgets heraus

Bislang stiegen die Security-Budgets von Jahr zu Jahr stetig weiter an. Das scheint in unsicheren wirtschaftlichen Zeiten nicht mehr zu gelten. Jetzt müssen die CISOs jeden Cent drei Mal umdrehen, um vielleicht sogar mit weniger mehr zu erreichen. Auf was müssen CISOs ihr Augenmerk dabei richten?

Von Dipl. Betriebswirt Otto Geißler

Bild: Andrey Popov/stock.adobe.com

Einem großen Teil des deutschen Mittelstands sind die Bedrohungen durch Hacker-Angriffe noch immer nicht vollständig bewusst. Zu diesem Ergebnis kam die Studie „Cyber Security im Mittelstand" von Deloitte.

Gerade für Mittelständler können solche Angriffe besonders schnell existenzbedrohend werden. Insgesamt 42 Prozent der Befragten gaben an, dass das Thema IT Security für sie nur eine mittlere bis sehr niedrige Priorität besitzt. Dem gegenüber stiegen die Cyber-Kriminalität im Zusammenhang mit Covid-19 und die daraus entstandenen Schäden weltweit stark an. Budgetkürzungen werden das Dilemma nicht

verbessern. An welchen Stellen können CISOs ansetzen, um die Performance zu optimieren?

Automatisierung erhöhen

Für die Beschleunigung von Prozessen und die Verbesserung der Effizienz sollten sich IT-Abteilungen der robotergestützten Prozessautomatisierung (RPA) zuwenden. Denn dadurch wird es den Mitarbeitern in der Regel erspart, sich mit ständig wiederholenden Aufgaben zu beschäftigen, während gleichzeitig das Personal seinen Fokus auf höherwertige Aufgaben verlagern könnte.

Die Automatisierung von Teilen des Identitäts- und Zugriffsmanagements (IAM), bei dem in der Regel intensive manuelle Aufgaben anfallen, liefert besonders gute Ergebnisse, ebenso wie die Automatisierung der Reaktionen auf manche Vorfälle. Ein Nebeneffekt: Die Automatisierung trägt dazu bei, einige der Herausforderungen bei der Suche nach qualifizierten Security-Experten zu erleichtern, was zu weiteren finanziellen Einsparungen führen kann.

Risiken überprüfen und sich neu ausrichten

Es ist angezeigt, die größten Risiken, denen Unternehmen ausgesetzt sind, zu identifizieren und regelmäßig neu zu bewerten sowie die Investitionen für die IT Security auf diese Risiken neu auszurichten. Das heißt, die Unternehmen müssen sich auf ihre Hauptrisiken fokussieren und ihre Budgets darauf konzentrieren, weil es in diesem Bereich den größten Nutzen bringt.

Vorhandene Security-Produkte neu bewerten

Angesichts der sich abschwächenden Konjunktur könnten die CISOs die verwendeten Security-Produkte neu bewerten und bestimmen, welche davon am wichtigsten sind, welche den besten Nutzen bieten und welche es tatsächlich wert sind, für bessere Bedingungen und günstigere Preise eingekauft zu werden. Vielleicht ist gerade jetzt ein guter Zeitpunkt, sich am Markt umzusehen: Gibt es neue Produkte? Gibt es interessante Produkt-Erweiterungen? Gibt es spezielle günstige Angebote?

Ausgliederung des Security-Budgets von der IT

Wenn das Security-Budget einem größeren IT-Budget untergeordnet ist, das in der Regel von einem CIO verantwortet wird, so stehen die allgemeinen IT-Ziele und Aufgaben meist im Vordergrund. Daher ist es angeraten, dass sich CISOs für einen autonomen Security-Haushalt stark machen, um verlässlichere Ausgabenpläne und Zielsetzungen erstellen sowie längerfristige Investitionen in Personal und Technologie tätigen zu können.

Das heißt, es muss eine Planung erstellt werden, die nicht nur dazu beiträgt, gute Vertragsbedingungen und ein qualifiziertes Team zu erhalten, sondern auch die Erreichung der Security-Ziele gewährleistet.

Verstärkt externe Ressourcen nutzen

Die meisten CISOs klagen über Personalprobleme, da viele Teams entweder chronisch unterbesetzt sind oder neue, noch nicht besetzte Stellen aufweisen. Talente sind nicht nur schwer zu finden, sondern auch teuer und nicht leicht zu halten. CISOs, die ihr Budget optimieren wollen, sollten ihren Personalbedarf prüfen und feststellen, ob einige Positionen oder Funktionen eventuell ausgelagert werden könnten.

Zum Beispiel können CISOs feststellen, dass die Berufung von Managed Service Providern für einige hochspezialisierte Aufgaben, die nicht in Vollzeit benötigt werden, Kosten reduzieren kann. Zudem wäre zu überlegen, ob nicht spezialisiertes Fachwissen oder bestimmte Dienstleistungen von bestehenden Anbietern als Teil bereits bestehender Verträge übernommen werden könnten. ⇨

Vorhandene Tools optimieren

Warum nicht bei dieser Gelegenheit noch einmal die Tools und Systeme überprüfen, die bereits im Einsatz sind? Nicht wenige davon werden betrieben, nur um ein „Kästchen in einer Liste anzukreuzen“ oder irgendeine Art von Anforderung zu erfüllen. Aber woher weiß man eigentlich, wie effizient sie tatsächlich funktionieren? Daher sollte man sie erneut testen, bewerten und sicherstellen, dass sie das tun, was sie eigentlich tun sollen. Der CISO kann so feststellen, dass es vielleicht Lösungen gibt, welche die gleiche Aufgabe besser oder billiger erfüllen. Da in manchen Produktkategorien immer mehr Anbieter die Märkte betreten, hat man auch zusehends mehr Einfluss bei den Kostenverhandlungen.

Bild: Olivier Le Moal/stock.adobe.com

Automatisierung entlastet nicht nur das bestehende Security-Team, sondern kann auch die Suche nach neuen Fachkräften vermindern.

Wechsel zu Best-of-Suite

Seit Jahren suchen IT-Security-Abteilungen nach Best-of-Breed-Tools für die verschiedenen Funktionen innerhalb ihrer Sicherheitsumgebung. Wobei ein Best-of-Suite-Ansatz, bei dem nur ein Produkt gleich mehrere Tools umfasst, durchaus die bessere finanzielle Option sein kann. Das heißt, der Best-of-Suite-Ansatz könnte nicht nur die Kosten dämpfen, sondern auch die Zeit für die Schulung der Mitarbeiter verkürzen, da sie dafür nur ein Produkt – und nicht mehrere oder viele – zu erlernen brauchen. Dies hätte die Konsequenz, dass die CISOs gegebenenfalls auch weniger Personal (und damit weniger Kosten) für die Überwachung und Verwaltung eines einzigen Best-of-Suite-Produkts gegenüber mehreren Best-of-Breed-Lösungen beschäftigen müssten.

Überprüfung auf zusätzliche Sicherheitskosten

Viele Unternehmen, insbesondere größere Organisationen, integrieren oft ihre Security-Tools auf Abteilungsebene und nicht an zentralen Stellen. Das kann zu einem mehrfachen Einsatz von gleichen Security-Systemen innerhalb des Unternehmens führen. Das bedeutet, dass sie oft mehrfach erworben wurden, was die Kosten schnell in die Höhe treibt.

Das heißt aber auch, dass in den einzelnen Abteilungen oder Standorten eines Unternehmens unterschiedliche Sicherheitsteams mit den gleichen Tools für verschiedene Funktionen arbeiten. Die Zentralisierung des Erwerbs und der Verwaltung von Security-Tools wird nicht nur die Kosten deutlich senken, sondern auch die Verhandlungsbasis für den Erwerb der Tools entscheidend verbessern.

Ein ähnliches Szenario ist häufig bei Cloud-Implementierungen der Fall, wofür verschiedene Abteilungen ihre eigenen Cloud-Dienste oder SaaS-Angebote mit integrierten Security-Funktionen und Tools erworben haben. Die einzelnen Security-Teams verwalten diese Tools natürlich dann selbst, was für sie wiederum zusätzliche Komplexität und Kosten bedeutet. Die CISOs können in all diesen Fällen den Bestand auf Abteilungsebene überprüfen und dann Mehrfach-Anschaffungen und Komplexitäten eliminieren. Gleichzeitig sollten die CISOs Standards und Rahmenbedingungen schaffen, die den Geschäftsführern dabei helfen, zusätzliche Kosten in Zukunft zu vermeiden. □

Mobiles Arbeiten – ohne Kompromisse bei der Sicherheit

Sicheres Arbeiten mit der SINA Workstation S von secunet am Büro-Schreibtisch, zu Hause oder unterwegs.

Beim Thema Mobile Office stehen Behörden und Unternehmen vor einem Dilemma: Unter dem Blickwinkel der Informationssicherheit gilt es, eine Vielzahl von Maßnahmen umzusetzen – was einer schnellen und einfachen Projektumsetzung zuwiderläuft. Um die nötigen Sicherheitsanforderungen umzusetzen, ist üblicherweise eine Vielzahl von Komponenten nötig, die alle einzeln administriert werden müssen. Wenn dies zu aufwändig ist, aber die Reduzierung der Sicherheit keine Option ist, steht eine bewährte Lösung bereit: die SINA Workstation S. Sie ist Teil des Krypto-Systems SINA, das secunet im Auftrag des BSI entwickelt hat. Bereits seit Jahren stellt die SINA Workstation S den Standardarbeitsplatz in zahlreichen Bundes- und Landesbehörden, darunter auch in mehreren Bundesministerien. Bislang wurden bereits mehr als 100.000 Exemplare ausgeliefert.

Die Lösung erlaubt es, bestehende Systeme einfach in die sichere SINA Umgebung zu migrieren. Die Nutzer arbeiten dann ohne Einschränkungen in ihrer gewohnten Umgebung weiter, zum Beispiel in MS-Windows, und greifen sicher auf das Behörden- oder Unternehmensnetzwerk zu. Auch das Desktop-Telefon kann die SINA Workstation S ersetzen, indem sie sichere Telefonate per Voice over IP (VoIP) ermöglicht. Für einen schnellen Rollout und eine erleichterte Administration stehen automatisierte Tools zur Verfügung.

Die SINA Workstation S ist in verschiedenen Formfaktoren – Desktops, Laptops, Tablets – verfügbar, die alle für den Umgang mit Verschlusssachen der Einstufung VS-NfD zugelassen sind. Je nach Anforderungen steht als Alternative zum Fat Client mit vollwertigem PC-Arbeitsplatz auch eine schlanke Terminal-Server-Lösung (Thin Client) zur Wahl. Allen Varianten gemein ist, dass der Nutzer auch zu Hause oder unterwegs so arbeiten kann, als säße er am gewohnten Büro-Schreibtisch – und das, ohne die Informationssicherheit zu gefährden. ■

Darf Awareness-Training Spaß machen? Mitarbeitersensibilisierung auf Basis von Lernpsychologie

Ein Interview mit Dr. Niklas Hellemann, Diplom-Psychologe und Managing Director bei SoSafe Cyber Security Awareness

SoSafe
Cyber Security Awareness

Dr. Niklas Hellemann

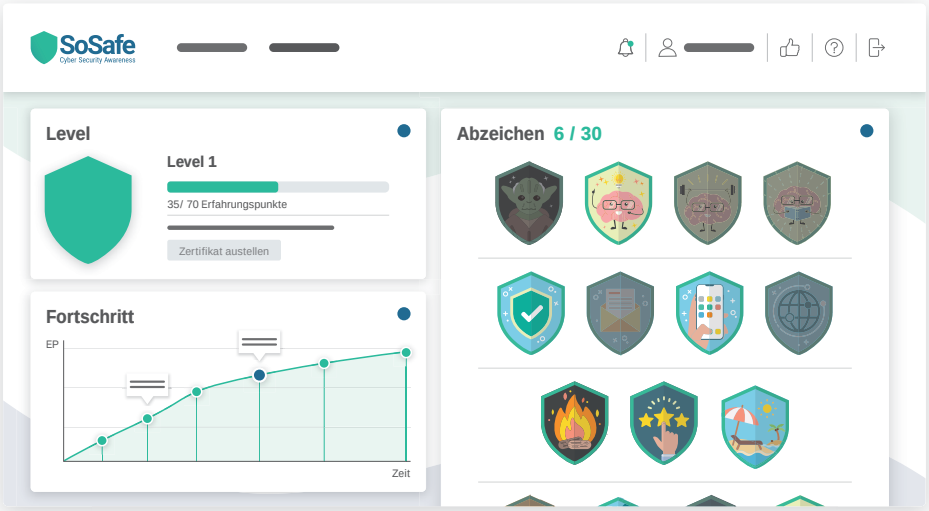
Die Awareness-Plattform von SoSafe sensibilisiert Mitarbeiter zahlreicher Unternehmen, wie Vattenfall, Aldi oder Avira, für IT-Sicherheits-Themen. Micro-Lernmodule und simulierte Phishing-Angriffe sorgen nicht nur für eine nachhaltige Wissensvermittlung, sondern auch für eine messbare Risikominimierung und Erfüllung der Compliance-Pflichten. Dank eines Full-Service-Ansatzes laufen Implementierung und Anwendung nahezu automatisch. Ein Gespräch über die psychologischen Mechanismen von modernem Awareness-Training.

Warum ist der Mensch das größte Sicherheitsrisiko beim Thema Cyber-Security?

Also erst einmal, der Mensch ist kein Risiko – so eine Aussage tut mir als Psychologe in der Seele weh! Es stimmt, dass laut BSI 9 von 10 erfolgreichen Cyberangriffen auf Unternehmen beim Mitarbeiter starten. Einfach, weil es der effizienteste Weg in die Systeme ist, wie spektakuläre Ransomware-Fälle, z.B. bei dem Touristik-Unternehmen CWT, zeigen. Gleichzeitig finden gerade aktuelle Taktiken à la „Emotet“ immer wieder Wege durch die technischen Filter – wie das Sicherheitsunternehmen Avanan berichtet, sogar in 25% aller Fälle! Eine moderne IT-Sicherheitsstrategie bezieht daher immer mehrere Ebenen der Verteidigung ein – eben auch den Nutzer. Mitarbeiter können, wenn sie richtig sensibilisiert werden, ein aktiver Teil der Verteidigung sein.

Viele Unternehmen haben Richtlinien in Bezug auf die IT-Sicherheit veröffentlicht. Wieso reicht das nicht aus, um die Mitarbeiter zu sensibilisieren?

Richtlinien sind natürlich ein erster Schritt, um Mitarbeiter allgemein zu informieren, aber einen großen Effekt im Sinne einer Risikominimierung darf man dadurch nicht erwarten. Modernes Awareness-Training zielt auf das nachhaltige Erlernen von Routinen ab, um Risiken messbar zu reduzieren. Als Tool zur effektiven Sensibilisierung sind beispielsweise Phishing-Simulationen sehr



Gamification auf der SoSafe-Awareness-Plattform: Abzeichen und Punkte sorgen für zusätzliche Motivation.

gut geeignet. Die Mitarbeiter werden so laufend mit realistischen Angriffsszenarien konfrontiert und lernen spielerisch, besser auf echte Phishing-Mails zu achten. Ein wichtiger Aspekt hierbei: Die simulierten Angriffe sollten anonym ausgewertet und auf deutschen Servern verarbeitet werden – gerade vor dem Hintergrund der neuesten Privacy-Shield-Entscheidung des EuGH begibt man sich sonst rechtlich in eine gefährliche Grauzone.

Welche lernpsychologischen Maßnahmen kann man ergreifen, um den Mitarbeiter zu einem umsichtigen Umgang mit Cybergefahren zu schulen?

Die Psychologie kennt verschiedene Arten des Lernens. Die „klassische“ lineare Wissensvermittlung ist gängige Praxis in der Security Awareness – nur nicht sehr effektiv. So haben Lernende bei dieser Vermittlung bereits nach sechs Tagen 75% der Inhalte vergessen. Bei unseren Lösungen setzen wir dagegen auf verteiltes Lernen in Form von Micro-Modulen. Die Inhalte können in nur wenigen Minuten Bearbeitungszeit erschlossen werden. Das Wissen wird zudem nicht nur über die E-Learning-Module, sondern auch auf anderen Kanälen vermittelt, etwa über Voice-Phishing-Anrufe oder via Messenger wie Microsoft Teams.

Sie setzen auf Gamification als Methode gegen Cyberkriminalität. Welchen Lerneffekt versprechen Sie sich davon?

Gamification, also die Anwendung von spieltypischen Elementen, motiviert zur Auseinandersetzung mit einem „trockenen“ Thema wie IT-Sicherheit. Wir verwenden beispielsweise Storylines, interaktive Elemente und Charaktere zur Vermittlung. Unsere Hauptfiguren Jan und Clara begleiten die Lernenden durch die Themenbereiche und bieten so eine Identifikationsfläche. Auch unser Dashboard ist stark gamifiziert. Mitarbeiter erhalten für das Absolvieren von Lerneinheiten oder das Erkennen von Phishing-Mails Punkte und Abzeichen. Gesteigerte Komplettierungsraten unterstreichen diesen Ansatz. Außerdem macht das den Anwendern großen Spaß, wie unser gutes Feedback zeigt.

Weitere Informationen zur Awareness-Plattform von SoSafe unter **www.sosafe.de**. Kostenfreie Awareness-Materialien für die Sicherheit im Home Office finden Sie zudem unter **www.sosafe.de/home-office/**. ■

Was bei der IT-Sicherheits-strategie auf Dauer verändert werden muss

Die Corona-Krise hat Schwachstellen in Security-Konzepten offengelegt. Viele Unternehmen hatten zum Beispiel in ihren Notfallkonzepten nicht an eine Arbeit im Home Office gedacht. Doch nicht nur für Krisenzeiten sollten die richtigen Security-Maßnahmen verfügbar sein. Die Security braucht generell eine Veränderung, denn die Unternehmen verändern sich dauerhaft.

Von Oliver Schonschek

Bild: Halfpoint/stock.adobe.com

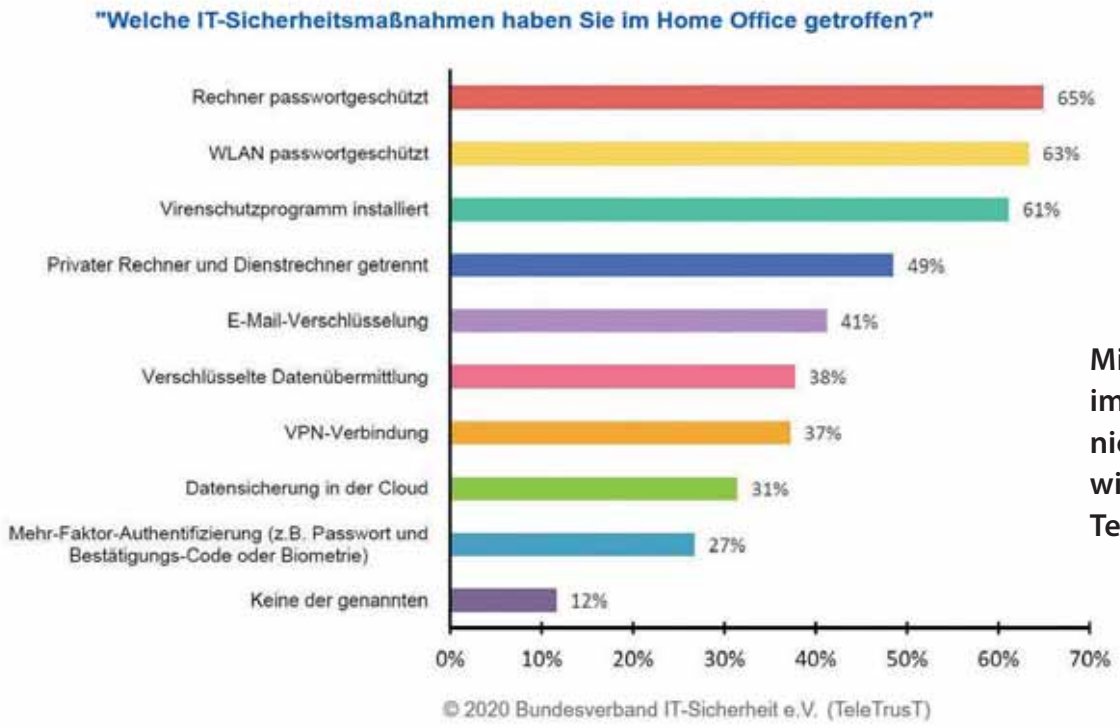
Digitalisierung hat einen Schub bekommen

CISOs sollten nicht nur überlegen, wie sich die IT-Sicherheit für die restliche Zeit, in der Beschäftigte im Home Office tätig sind, verbessern lässt, und auch nicht nur, wie sich die Home-Office-Arbeitsplätze wieder auflösen und sicher zurück in die Büros verlagern lassen.

Die Digitalisierung entwickelt sich auch nach der Krise weiter und hat sogar eine Beschleunigung erfahren durch die Maßnahmen zur Krisenbewältigung. Wenn jetzt also Security-Konzepte überarbeitet werden, sollte auch an die Anforderungen für die Zeit nach der Corona-Krise gedacht werden.

Der Digitalverband Bitkom nennt Beispiele für andauernde Veränderungen: Cloud statt Aktenschrank, Online-Meeting statt Geschäftsreise, Bestellungen und Rechnungsversand über Kundenportale statt per Brief und Fax.

Wie eine Umfrage von Eco – Verband der Internetwirtschaft e.V. ergab, wollen rund ein Drittel der Angestellten (32,6 Prozent) auch in nächster Zeit vermehrt mithilfe von Videokonferenzen mit Kunden und Kollegen kommunizieren. Über 20 Prozent wollen mehr Tools zur Online-Projektarbeit im Team nutzen. Rund 10 Prozent



Mit der IT-Sicherheit im Home Office ist es nicht so gut bestellt, wie eine Umfrage von TeleTrusT ergab.

setzen vermehrt auf digitale Weiterbildungsangebote. Diese Entwicklungen müssen in den Security-Konzepten Berücksichtigung finden.

Folgen der Home-Office-Erfahrung

Die Studie „Veränderung der Arbeitswelt durch Corona“ von YouGov hat untersucht, wie die Tätigkeit im Home Office nach der Corona-Krise aussehen kann. 68 Prozent der Beschäftigten wünschen sich eine Lockerung der Regelungen. Sie wollen entweder mindestens einen Tag in der Woche von Zuhause arbeiten (29 Prozent) oder flexibel entscheiden können, ob sie im Heimbüro oder in der Dienststelle tätig sind (31 Prozent). Acht Prozent der Mitarbeiter können sich sogar ein Arbeitsleben ohne festen Arbeitsplatz im Firmengebäude vorstellen.

Offensichtlich müssen sich CISOs darauf einstellen, dass es mehr Arbeit im Home Office und entsprechend mehr Bedarf an geeigneter Endpoint Security geben könnte. Ebenso sollte man damit rechnen, dass die virtuelle Zusammenarbeit und der Einsatz entsprechender Tools an Beliebtheit gewonnen haben. Nicht zuletzt können auch neue Wünsche entstanden sein, in Zukunft andere Endgeräte und Applikationen im Unternehmen zu verwenden, die den privaten Geräten und Anwendungen im Home Office ähnlicher sind.

Generelle Änderungen in der Endpoint Security sinnvoll

Es zeigt sich: Die Corona-Krise hat einen Digitalisierungsschub bzw. Digitalisierungszwang ausgelöst. Viele Maßnahmen wie die Einrichtung von Home Offices mussten überstürzt erfolgen und liefen ohne ausreichende Sicherheitsmaßnahmen ab. Zur Krisenvorsorge, aber auch um der steigenden Digitalisierung zu entsprechen, sollten CISOs prüfen, wie sie die Endpoint Security unabhängig vom Standort sicherstellen können, damit Arbeitsplätze flexibel aufgebaut und abgebaut werden können und damit die zunehmende virtuelle Zusammenarbeit nicht zur Bedrohung, sondern zu einem Motor im Unternehmen werden kann. □

„Made in Germany“ – eine Qualitätskultur, die uns auszeichnet

Ein Kommentar des Digitalexperten Michael Pickhardt

Wir leben in einem Land, das erstaunlich ungewöhnliche Voraussetzungen hat, um wirtschaftlich Erfolg zu haben. Im internationalen Vergleich gibt es bei uns sehr hohe Sozialleistungen, wir nehmen eine Spitzenreiterrolle in Feier- und Urlaubstagen ein und wir leisten uns eine Jahresarbeitszeit, die laut Erhebung der OECD von 2018 so niedrig ist, dass sie ihresgleichen sucht. Wir sind Vorreiter in Sicherheitsstandards, Umweltschutz und Nachhaltigkeit. Das wollen wir – bei aller Freude daran, Probleme zu suchen, zu finden, zu lamentieren – einfach mal so stehen lassen und, ja, auch wertschätzen. Nur: Haben Sie sich schon einmal gefragt, wie es unser relativ kleines Land dennoch schafft, einen Top-Platz unter den Nationen einzunehmen, die den höchsten Nettoexport verzeichnen – und Export-Vizeweltmeister im Jahr 2020 ist, nach China und vor Russland?

Eine entscheidende Antwort auf die Frage nach dem Geheimnis dieser Erfolgsgeschichte ist meines Erachtens der Begriff „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 ver-

Bild: Marina Geckeler/TDT AG

standen wird: „Made in Germany“ steht für eine Qualitätskultur – und dafür, dass die jeweilige Ware in Deutschland entwickelt und gefertigt wird.

Ich bewege mich mit meinem Unternehmen seit Jahrzehnten im Bereich der Telekommunikation. Auch wenn es in unserer globalisierten „Billigheimer“-Welt leider nur noch schwer möglich ist, bei der Fertigung von Produkten ganz auf Teile aus dem Ausland zu verzichten – es ist umso wichtiger, bei den eigenen Lieferanten auf „Made in Germany“ zu setzen. Bei uns kommen über 90% unserer Zulieferer aus der direkten Umgebung. Diese kurzen Wege und Lieferketten sind auch im Sinne von Nachhaltigkeit und Umweltschutz eine mehr als nur wirtschaftliche Lösung.

Anders gefragt: Wie verantwortungsvoll ist es eigentlich für Unternehmer, wenn sie die eigene IT-Infrastruktur mit vermeintlich günstigem Fernost-Equipment ausrüsten? Obwohl doch heute jedem klar ist, dass diese Importprodukte, falls überhaupt, Software-Sicherheitsupdates nur in zeitlich sehr begrenztem Rahmen bieten. Von möglichen Qualitätsmängeln oder Service-Wünschen ganz zu schweigen, die man dann als Kunde meist mit Maschinen besprechen darf – wenn man Glück hat. Bei genauerer Betrachtung stellt sich heraus, dass vergleichbare Produkte aus dem professionellen Bereich, die hierzulande gefertigt werden, nicht zwingend teurer sind. Ich kann nur dazu raten, nicht den Fehler zu machen, Fire-and-Forget-Consumer-Produkte mit professionellem IT-Equipment gleichzusetzen und preislich zu vergleichen.

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. ■

Der Autor

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.

Was an der DSGVO geändert werden soll und kann

Die letzten Monate haben sich sowohl Wirtschaftsverbände und Datenschutz-Vereinigungen als auch die Aufsichtsbehörden für den Datenschutz zu ihren Erfahrungen und Wünschen geäußert, was an der Datenschutz-Grundverordnung geändert werden sollte. Einiges davon hätte man bereits angehen können, anderes müsste den langen Weg der EU-Gesetzgebung gehen.

Von Oliver Schonschek

Bild: Sir_Oliver/stock.adobe.com

Bei der Kritik, die an der Datenschutz-Grundverordnung (DSGVO) im Vorfeld und seit ihrer Anwendung geübt wurde, wäre es erstaunlich gewesen, wenn die Evaluation der DSGVO durch Wirtschaftsverbände keinen Änderungsbedarf ergeben hätte. Doch auch die Politik, verschiedene Datenschutz-Vereinigungen und die Aufsichtsbehörden für den Datenschutz sehen Bedarf für Veränderungen an der DSGVO. Die DSGVO sieht auch selbst eine Evaluierung vor: „Bis zum 25. Mai 2020 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verord-

nung vor. Die Berichte werden öffentlich gemacht", findet man in Artikel 97 DSGVO.
Es hat zwar einen Monat länger gedauert, doch die EU-Kommission klopft sich auf die eigene Schulter: Die DSGVO habe die meisten ihrer Ziele erreicht, sei zeitgemäß und stärke die Rechte der EU-Bürger. Ganz so voll des Lobes sind deutsche Aufsichtsbehörden nicht.

Was die Aufsichtsbehörden sagen

Insgesamt hat sich gezeigt, dass die Verantwortlichen in Baden-Württemberg sich in vielen Bereichen alltagstauglichere Lösungen wünschen und einige Vorschriften nur schwer auf datenverarbeitende Tätigkeiten kleiner Unternehmen oder ehrenamtlicher Arbeit anwendbar sind, erklärte zum Beispiel der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg. Im Vordergrund stehen demnach vor allem Fragen rund um eine mögliche Entlastung bei den Informations-, Transparenz- und Auskunftspflichten, aber auch bei Fragen der gemeinsamen Verantwortlichkeit und der Auftragsverarbeitung.
Interessant ist dabei auch diese Aussage der Aufsichtsbehörde: Die Datenschutzaufsicht in Baden-Württemberg orientiert sich am Leitsatz „Wenn es nicht sinnvoll ist, dann ist es kein Datenschutz".
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Professor Ulrich Kelber, führt aus: „Meine Kollegen und ich halten groß angelegte gesetzliche Änderungen an der DSGVO für verfrüht. Wir sehen aber Bedarf für Verbesserungen bei der praktischen Umsetzung. Das gilt insbesondere im Bereich der Zusammenarbeit der Datenschutzaufsichtsbehörden in grenzüberschreitenden Verfahren. Unterschiede in den nationalen Verwaltungsverfahren dürfen nicht dazu führen, dass die Effektivität der Durchsetzung der DSGVO gegenüber Unternehmen, die Datenschutzverstöße begangen haben, beeinträchtigt wird."
Im Hinblick auf den internationalen Datenverkehr betont der Europäische Datenschutzausschuss (EDSA) die Bedeutung der Angemessenheitsbeschlüsse der Europäischen Kommission. Er fordert die Kommission auf, die Beschlüsse über EU-Standardvertragsklauseln für Datenübermittlungen in Drittstaaten zu überarbeiten.

Verbände beklagen Bürokratiehürden

Trotz großer anfänglicher Sorgen hat sich die DSGVO nach rund zwei Jahren als grundsätzlich taugliches Regulierungsinstrument etabliert, so der Verband der Internetwirtschaft Eco. Gleichzeitig ergeben sich für den Verband der Internetwirtschaft bei der Umsetzung noch zu viele ungelöste Rechtsfragen und praktische Probleme. Dies gilt insbesondere für Entwickler und Anbieter KI-basierter Systeme.
Dazu sagt Eco-Geschäftsführer Alexander Rabe: „Bürokratische Hemmnisse und Rechtsunsicherheiten im Datenschutz können nur durch einen ganzheitlichen europäischen Ansatz überwunden werden. Die DSGVO kann jedoch nur dann zum Game-Changer für Europa werden, wenn ein präziser und einheitlicher Rechtsrahmen besteht. Unsicherheiten, wie sie aktuell noch bei der Verarbeitung von KI-Trainingsdaten sowie Transparenz- und Informationsverpflichtungen bei automatisierten Entscheidungsfindungen auftreten, müssen beseitigt werden. Zu viele bürokratische Hemmnisse sorgen derzeit dafür, dass die DSGVO in ihrer jetzigen Form weder innovationsfreundlich noch marktgerecht ist."
Auch der Digitalverband Bitkom hat eine Bewertung abgegeben: „Nach der geplanten Evaluierung der Datenschutzregeln muss die EU den grundsätzlichen Geburtsfehler beseitigen", so Bitkom-Präsident Achim Berg. „Die DSGVO reglementiert jeden einzelnen Datenverarbeitungsvorgang und jede Datenerhebung. Vereine, Startups und Großkonzerne werden über ⇨

denselben Kamm geschoren und nicht differenziert behandelt. Die in der DSGVO vorgesehenen Ausnahmen für kleinere Unternehmen kommen in der Praxis so gut wie nie zum Tragen. Dabei sollten Art und Umfang der Datenverarbeitungen ausschlaggebend für die Verpflichtungen sein, auch sollte man die Regeln grundsätzlich vereinfachen. In der Forschung sollten der Datennutzung weniger Hürden in den Weg gestellt werden – insbesondere für EU-weite Projekte im Gesundheitsbereich."

Unklarheiten beseitigen, Vorgaben schärfen

Trotz umfangreicher Aufklärungsangebote und Hilfestellungen gebe es bei den Rechtsanwendern noch immer zahlreiche Fragen und Unsicherheiten, so auch Bayerns Innenminister Joachim Herrmann bei einer Konferenz mit den bayerischen Industrie- und Handelskammern und der Wirtschaftskammer Österreich.

Es gebe in der Anwendung noch grundsätzlichen Klärungsbedarf. So werden laut Herrmann beispielsweise einige der neu eingeführten Instrumente bisher in der Praxis nur vereinzelt genutzt. Als Beispiele nannte er die Verhaltensregeln, die Zertifizierung, die Einführung eines Europäischen Datenschutzsiegels oder auch das Kohärenz-Verfahren. „Die Kommission muss dringend analysieren, woran die Zurückhaltung in diesem Bereich liegt und Vorschläge für eine Abhilfe vorlegen", forderte der Minister.

Vorhandene Werkzeuge sollten besser genutzt werden

Die vom Bayerischen Innenminister vorgebrachte Kritik, einige der neu eingeführten Instrumente würden bisher in der Praxis nur vereinzelt genutzt, ist sehr angebracht und wichtig. Betrachtet man die Änderungswünsche, die von verschiedenen Stellen genannt werden, sind durchaus Punkte darunter, die sich ohne jede Änderung an der EU-Verordnung angehen ließen. Es versteht sich, dass alle Punkte, die tatsächlich die DSGVO verändern würden, nicht kurzfristig zu realisieren sind.

Es ist deshalb sinnvoll, alle Erfahrungen und Änderungswünsche dahingehend zu überprüfen, ob sich denn nicht schon heute etwas verändern lassen könnte, ohne weitere Gesetzgebungsinitiativen, also im Rahmen der bestehenden DSGVO.

Wenn zum Beispiel konkretere Vorgaben zur Umsetzung der Datenübertragbarkeit gewünscht werden, dann könnte dies auch heute schon geschehen, über Verhaltensregeln.

Verbände und andere Vereinigungen, die „Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten", können Verhaltensregeln ausarbeiten oder ändern oder erweitern und der zuständigen Aufsichtsbehörde zur Genehmigung vorlegen, so Artikel 40 DSGVO. Dazu gehören Bereiche wie „Ausübung der Rechte betroffener Personen". Genau hierunter fällt das Recht auf Datenübertragbarkeit. Es ist also in der heutigen DSGVO bereits vorgesehen, dass es dazu Verhaltensregeln geben könnte, ebenso zu den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen, auf die ebenfalls von den Wirtschaftsverbänden hingewiesen wird.

Fazit

Es lohnt sich, alle bisherigen Möglichkeiten und Instrumente der DSGVO zu betrachten und wirklich zu nutzen, um den Datenschutz voranzubringen und die Umsetzung der DSGVO zu optimieren. Die Ausarbeitung und Genehmigung von Verhaltensregeln zum Beispiel wird einige Zeit in Anspruch nehmen, doch man kann sich vorstellen, dass hier schneller Erfolge zu sehen sind als im Rahmen der komplexen EU-Gesetzgebung. Die gegenwärtige DSGVO kann mehr und bietet mehr, als bisher genutzt wird. □

Thüringer Aufbaubank führt neue IAM-Lösung ein

Die regulatorischen Anforderungen der MaRisk nehmen eher zu denn ab. Mit ihrer bisherigen IAM-Lösung konnte die Thüringer Aufbaubank diese nicht mehr bewältigen.

betasystems

Deshalb hat das Unternehmen im Jahr 2019 einen Schwenk vollzogen und arbeitet jetzt mit dem GARANCY Identity Manager der Beta Systems Software AG. Er erlaubt insbesondere die vorher nur wenig praktizierte Umsetzung eines Rollenkonzeptes, mit dem sich das Prinzip „Kein Recht ohne Rolle“ konsequent anwenden lässt.

Eine Prüfung nach §44 KWG gab den Anstoß: Das bisherige IAM-Konzept sollte überdacht, eine neue Lösung angeschafft werden. Tommy Grimmer, Leiter der Abteilung IT-Steuerung bei der Thüringer Aufbaubank: „Wichtig war uns, dass sie eine gute Usability mitbringt und alle jetzigen und kommenden Anforderungen der MaRisk und BAIT – soweit absehbar – erfüllt. Deshalb entschieden wir uns für die Software von Beta Systems, nicht zuletzt, weil eine Reihe anderer Banken bereits mit Garancy arbeitet und uns positive Erfahrungen berichteten.“

„Kein Recht ohne Rolle“ bedeutet: Rechte werden nur über Rollen beantragt, die Vergabe von Einzelrechten erfolgt nur in Ausnahmefällen. „Erst mit Beta Systems werden die Rollen wirklich auf Fachlichkeit, Stellen und Funktionen geschnitten“, erklärt Cindy Schöneweck, Compliance-Referentin in der

Foto: Zscheile

IT-Steuerung der Aufbaubank, und fügt hinzu: „Wir schätzen an Beta Systems, dass wir hier stets feste Ansprechpartner haben und auch der Support sehr gut erreichbar ist.“

Die MaRisk-Novelle 2017 hat neue Anforderungen mit sich gebracht, die sich in bankinternen Prozessen und Abläufen niederschlagen. Und die regulatorischen Anforderungen durch die BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) werden künftig kaum sinken. „In der Umsetzung der Anforderungen in den eigenen Prozessen muss allerdings die Frage gestellt werden, wie viel mehr Sicherheit immer konkretere Anforderungen wirklich bringen und inwieweit hier das Proportionalitätsprinzip noch eingehalten wird“, so Tommy Grimmer. „Wir sehen uns mit der aktuellen Lösung jedoch gut aufgestellt.“

www.betasystems-iam.com ■

Keine Chance für Phishing-Mails

Sie treten massenhaft auf und sehen oft täuschend echt aus: Phishing-Mails sind für Cyberkriminelle eine lukrative Angriffsmethode. Oft fallen Mitarbeiter in Unternehmen auf die betrügerischen Nachrichten rein und öffnen den Angreifern damit die Tür zur IT-Infrastruktur. Abhilfe schaffen zielgerichtete Trainings für die Mitarbeiter, bei denen sie für Cyberrisiken sensibilisiert werden. Die G DATA Awareness Trainings leisten dies.

G DATA TRUST IN GERMAN SICHERHEIT

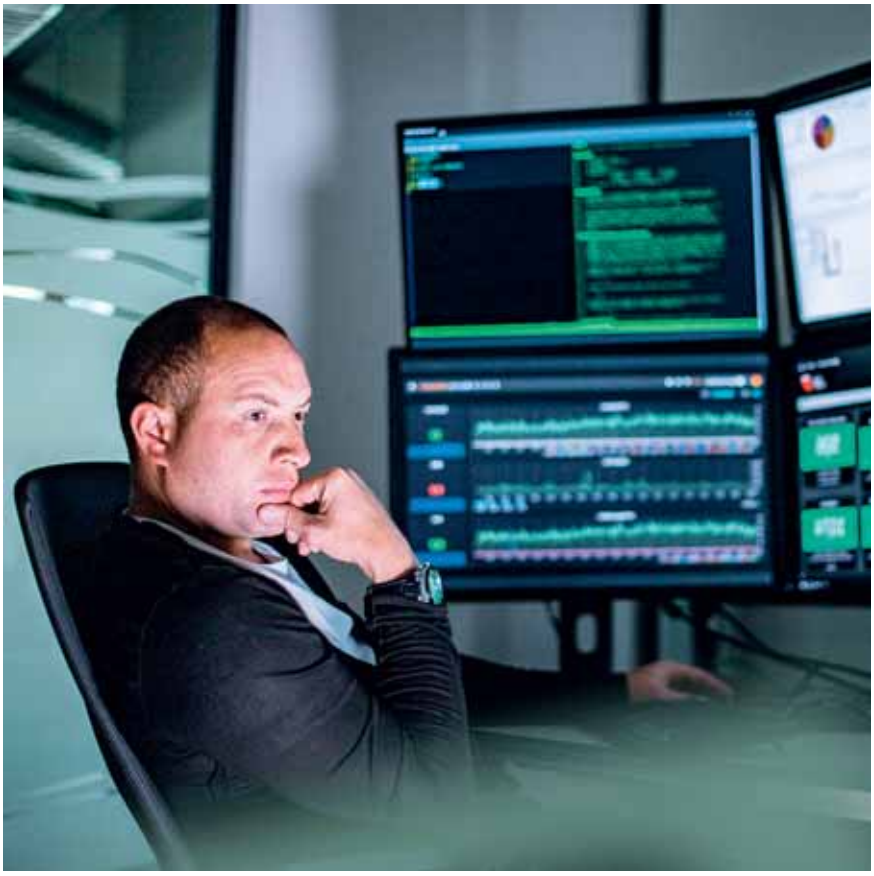
E-Mails sind im Unternehmensumfeld ein wichtiges Kommunikationsmittel, jeden Tag werden unzählige Nachrichten verschickt und gelesen. Im digitalen Postfach landen dabei oft auch Phishing-Mails mit verseuchten Dateianhängen oder Links auf betrügerische Webseiten. Schnell fallen die Empfänger darauf rein. Oft reicht schon ein falscher Klick auf eine dieser Nachrichten aus, um im schlimmsten Fall das gesamte Netzwerk lahmzulegen. Abhilfe schaffen die G DATA Awareness Trainings, mit denen Mitarbeiter alles Wichtige lernen, um die betrügerischen Mails zu erkennen und richtig zu reagieren.

Oft ist es für Cyberkriminelle leichter, einen Angriff auf das Unternehmensnetzwerk nicht allein auf der technischen Ebene durchzuführen, sondern über den Mitarbeiter zu gehen. Dieser lässt sich einfacher in die Irre führen: Der Mailempfänger hat es oft mit Phishing-Nachrichten zu tun, die täuschend echt gestaltet sind und authentisch wirken. Ein Beispiel sind angebliche Bewerbungen auf tatsächlich ausgeschriebene Stellen, die dringend besetzt werden sollen. Im alltäglichen Arbeitsstress bleibt die Vorsicht zusätzlich oft auf der Strecke. Dann reicht im Regelfall ein Klick, und die Kriminellen haben ihr Ziel erreicht – mit der ungewollten Hilfe eines Mitarbeiters.

Trainingsmaßnahmen verhindern erfolgreiche Attacken

Mitarbeiter müssen daher mit dem nötigen Wissen ausgestattet werden, um Angriffe

abzuwehren und ihr Unternehmen zu schützen. Der alleinige Einsatz technischer Sicherheitslösungen reicht heute im Unternehmensumfeld nicht mehr aus, um einen umfänglichen Schutz vor Cyberattacken sicherzustellen. Mitarbeiter müssen Teil des Konzepts sein und für die Risiken sensibilisiert sein.
Zielführend ist der Einsatz von Awareness Trainings von G DATA CyberDefense. Hier lernen Angestellte, wie sie die Gefahren erkennen und damit umgehen können, um sich und das Unternehmen zu schützen. Mit einer optional erhältlichen Phishing-Simulation stellt G DATA Angriffe über E-Mails realistisch nach, sodass die Mitarbeiter künftig nicht mehr auf entsprechende Nachrichten hereinfallen.



Security Awareness messen

Eine Simulation im Unternehmen sollte im Idealfall mehrere Wochen andauern und die Mitarbeiter mit Nachrichten in verschiedenen Schwierigkeitsgraden konfrontieren. So sind einige Nachrichten etwa durch grobe Rechtschreibfehler und fehlende direkte Anrede auf den ersten Blick erkennbar. Bei anderen Mails wird der Adressat beispielsweise direkt angesprochen, sodass die Gefahr erst auf den zweiten Blick erkennbar ist. Auch die zeitliche Komponente, also die Zeit des Versands sollte variieren. Denn die Aufmerksamkeit der Mitarbeiter ist nicht konstant.

Am Ende liefert die Simulation wertvolle Erkenntnisse über das IT-Security-Bewusstsein der Belegschaft, und IT-Verantwortliche können die Schulungsmaßnahmen der G DATA Security Awareness Trainings gezielt planen. Einfache Videos oder Hinweise haben dabei keinen nachhaltigen Nutzen und reichen daher nicht aus, um Mitarbeiter fit für IT-Sicherheit zu machen. IT-Verantwortliche, die nach einem Trainingsblock eine zweite Phishing-Simulation durchführen lassen, können die Ergebnisse miteinander vergleichen und den Erfolg messen.
Generell muss IT-Sicherheit ganzheitlich betrachtet werden. Mitarbeiter müssen genau lernen, wie sie die betrügerischen E-Mails und andere Cyberbedrohungen entlarven und dabei Erfahrungen sammeln – nur so werden sie zum wertvollen Teil der Cyberabwehr.

Mehr Informationen unter
secure.gd/partner-info ■

Business Messaging App: Ein kommunikativer Brückenschlag

Ob für stationäre oder mobile Mitarbeiter: Die interne Kommunikation muss reibungslos erfolgen, um Themen nicht nur schnell, flexibel und ortsunabhängig besprechen, sondern auch die Zusammenarbeit effektiver gestalten zu können. Für eine ganzheitliche Team-Kommunikation braucht es geeignete und vor allem DSGVO-konforme Lösungen, wie etwa eine Business Messaging App.

Von Tobias Stepan, Teamwire

Bild: Teamwire

Das Virus Covid-19 und die darum ergriffenen Schutzmaßnahmen haben die Nachfrage nach digitalen Lösungen, wie etwa Webmeeting-Anwendungen, Kollaborationstools und Echtzeit-Messengern, rasant in die Höhe schießen lassen. Um dezentrales Arbeiten besser gestern als morgen umsetzbar zu machen, war schnelles Handeln gefragt. Unternehmen, die

überwiegend Non-Desk-Worker wie Produktionsmitarbeiter, Logistikkräfte, Pflege- oder Krankenhauspersonal beschäftigen, stehen nicht erst seit der Corona-Pandemie vor der Herausforderung, eine produktive und sichere Team-Kommunikation zu ermöglichen. Oft greifen sie auf Consumer Apps zurück – allen voran WhatsApp –, um sich intern abzustimmen. Stellt das Unternehmen geschäftliche Devices, können IT-Administratoren die Nutzung unterbinden. Aber gerade bei Firmen, die auf ein BYOD-Konzept (Bring your own Device) setzen, entsteht dadurch eine gefährliche Schatten-IT. Denn: Eine Consumer App ist nicht für einen sicheren und Compliance-gerechten Informationsaustausch im Business-Bereich geeignet – insbesondere nicht bei Unternehmen mit kritischer Infrastruktur, Behörden mit vertraulichen Informationen oder Organisationen mit schützenswerten personenbezogenen Daten. Auch ist eine solche App nicht auf eine professionelle IT-Steuerung ausgerichtet. Aber auch bei Business-Tools sind Datenschutz und -sicherheit nicht immer zu hundert Prozent gewährleistet. Doch das sollte in der digitalen internen Kommunikation kein Nice-to-have, sondern eine unverzichtbare Standard-Anforderung sein.

Die Gretchenfrage: Wie hast du's mit dem Datenschutz?

Erst unlängst ist eine hitzige Debatte um namhafte Videokonferenz-Lösungen sowie Consumer Apps und deren Einsatz im Business-Bereich entfacht: Vertreter mehrerer Aufsichtsbehörden, darunter Ulrich Kelber, der Bundesbeauftragte für Datenschutz, und Maja Smoltczyk, die Berliner Landesdatenschutzbeauftragte, haben Empfehlungen und Warnungen herausgegeben, was die Nutzung dieser Dienste betrifft. Hinzu kommt, dass der Europäische Gerichtshof (EuGH) das Privacy Shield für ungültig erklärt hat. Dieses transatlantische Abkommen erlaubte US-Unternehmen, Daten von EU-Nutzern zur Verarbeitung und Speicherung in die USA zu übermitteln. Grund für die Entscheidung des EuGH war, dass US-Behörden auf personenbezogene Daten innerhalb von US-Firmen ungehindert zugreifen konnten. Demnach waren auch personenbezogene Daten von EU-Bürgern nicht gemäß DSGVO geschützt.

Sicheres und einfaches Messaging nicht gegeben

Neben zentralen Fragen nach Datenschutz und -sicherheit, die insbesondere bei Lösungen von US-Anbietern oftmals offenbleiben, sind Kollaborationstools, wie beispielsweise Microsoft Teams und Slack, nicht primär auf das Echtzeit-Messaging zwischen mobilen Mitarbeitern einerseits und stationären Kollegen andererseits ausgelegt. Die Anwendungen bringen zahlreiche Features und Funktionen mit, die für neue flexible Arbeitsmodelle relevant sein können. Für mobile Mitarbeiter eignen sich solche Lösungen nur bedingt, da die vielen Anwendungsmöglichkeiten für ihre Arbeit nicht brauchbar sind. Vielmehr benötigen sie eine business-taugliche WhatsApp-Alternative mit Funktionen, die ihre Anwendungsszenarien weitgehend abdecken und kommerziellen Messaging Apps hinsichtlich Benutzerfreundlichkeit in nichts nachstehen. Das erhöht zum einen die Akzeptanz für die Nutzung solcher Tools und steigert zum anderen die Produktivität.

Kurze Chat-Nachrichten anstatt langwieriger E-Mail-Kommunikation

Schon allein die Tatsache, dass mobile Mitarbeiter für die Team-Kommunikation WhatsApp wählen, anstatt ihre Kollegen anzurufen oder eine E-Mail über ihr Smartphone zu schreiben, verdeutlicht den unaufhaltbaren Wandel in der Team-Kommunikation: Die private Gewohnheit, über Messenger Apps zu kommuni- ⇨

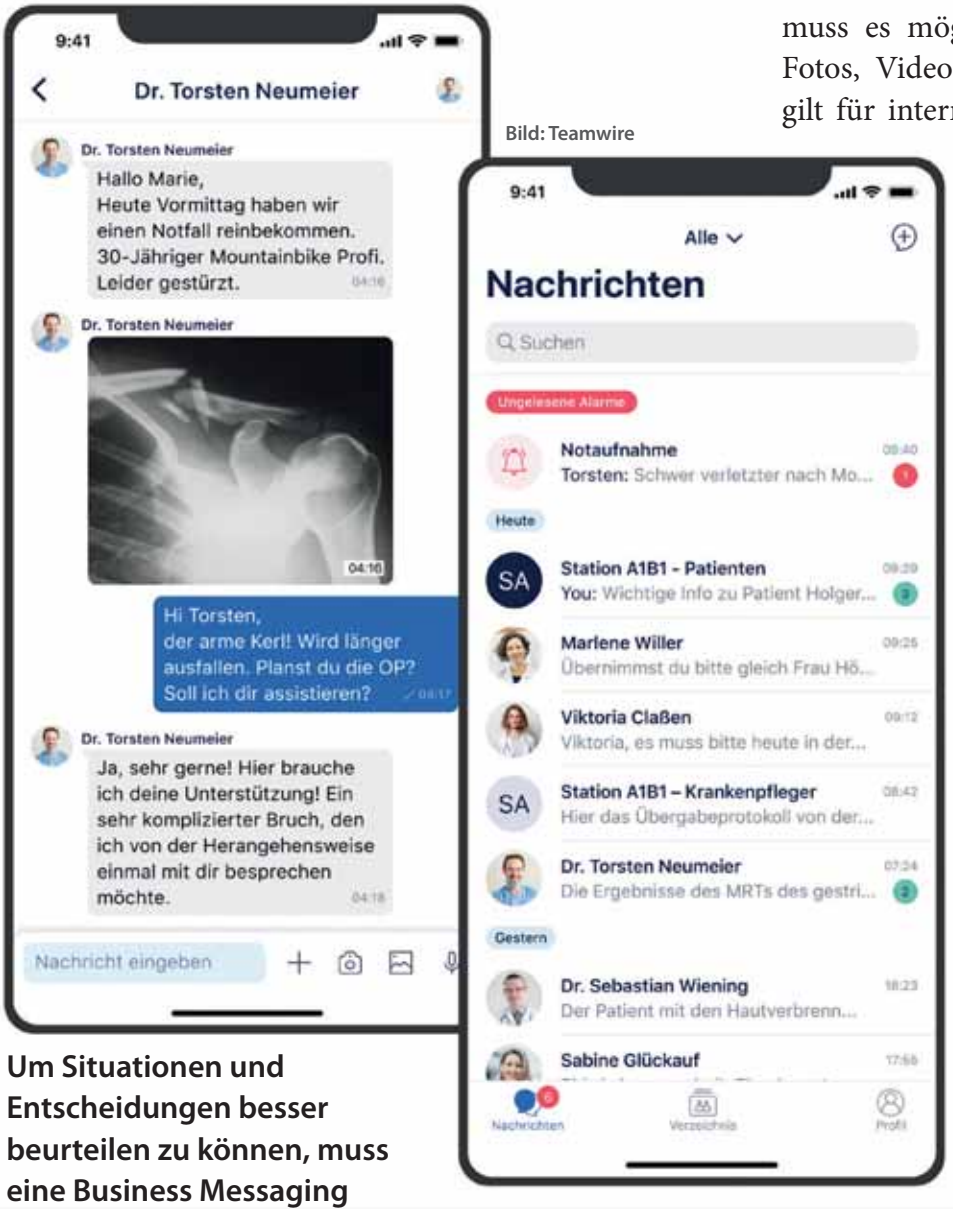


Bild: Teamwire

Um Situationen und Entscheidungen besser beurteilen zu können, muss eine Business Messaging App auch digitale Inhalte, etwa Fotos, Videos und PDFs, teilen können. Zudem sind Alarmierungs-Funktionen essenziell.

↪ zieren, hält Einzug in den beruflichen Alltag. Anders als bei E-Mails gehen Nachrichten in einer Business Messaging App nicht in einem überfüllten Postfach unter, und die Antwortzeit ist wesentlich kürzer. Um Situationen und Entscheidungen besser beurteilen zu können, muss es möglich sein, digitale Inhalte, etwa Fotos, Videos und PDFs, zu teilen. Gleiches gilt für interne Umfragen, die man direkt im Chat erstellen kann. Zudem sind Alarmierungs-Funktionen sehr hilfreich, um im Falle eines kritischen Ereignisses, etwa einer Kundeneskalation, eines Serverausfalls oder Feueralarms, ausgewählte Teams, Abteilungen oder die gesamte Organisation zu informieren.

Business Messaging App: Das technische A und O

Nicht nur die funktionalen Möglichkeiten sind entscheidend. Die interne Kommunikation darf IT-Administratoren kein Dorn im Auge sein. Vielmehr sollten sie schnell und einfach in der Lage sein, ihren Kollegen eine praktikable und unternehmensweit nutzbare Lösung zur Verfügung zu stellen. Zugunsten einer professionellen und vor allem DSGVO-konformen Team-Kommunikation sind eine Reihe technischer Aspekte zu beachten:

Kompromissloser Datenschutz: Um die Daten, die in einer Business Messaging App entstehen, zu schützen, muss Datensouveränität und -sparsamkeit gegeben sein. Wenn die Daten in einem IS027001-zertifizierten Rechenzentrum mit Standort in Deutschland oder On premises, also vor Ort in den eigenen Räumlichkeiten, gespeichert werden, ist man hier auf einem guten Weg. Wichtig ist zudem, dass vollständig verschlüsselt wird und so wenig wie möglich Meta-Daten, wie etwa Standort, Datum und Uhrzeit, erfasst werden. Daneben muss die

Business Messaging App auch das „Privacy by Design"-Konzept der DGSVO erfüllen.

Applikationsbereitstellung mittels Container: Nur wenn sich eine Business Messaging Anwendung als sichere Container App betreiben lässt, ist dafür gesorgt, dass alle Daten auf dem Endgerät geschützt sind und die volle Datenkontrolle beim Unternehmen liegt. Der Container steuert den erlaubten Datenzugriff durch Nutzer und den möglichen Datenaustausch mit anderen Applikationen. Zugleich gewährleistet er, dass auf dem Endgerät gespeicherte Daten per Routine automatisiert reduziert und bei Bedarf aus der Ferne komplett gelöscht werden können.

Vollumfängliche Verwaltung per Dashboard: Mittels eines professionellen Administratorenportals behält die IT jederzeit die Hoheit über die Software. Es ist essenziell, um die Benutzerverwaltung und die Rechteverteilung zu steuern. Über ein Dashboard lassen sich beispielsweise Kommunikationsrichtlinien festlegen sowie Nachrichten und Daten revisionssicher archivieren. Um Benutzer oder auch Gruppen direkt aus bestehenden Verzeichnissen, wie etwa dem Active Directory, bequem zu importieren und laufend zu synchronisieren, sollte sich die Lösung bedarfsgerecht integrieren lassen. Auch sollte das Dashboard ermöglichen, Multi-Mandanten zu verwalten und mehrere Domains zu nutzen.

Vollständige Integration in das IT-Ökosystem: Idealerweise verfügt eine Business Messaging App über eine offene API-Schnittstelle, welche die Anbindung von Drittsystemen, etwa CRM und ERP, erlaubt. Eine derartige Integration hilft, nicht nur den Informationsaustausch – durch automatisierte Prozesse und beschleunigte Workflows – zu verbessern, sondern steigert auch die Produktivität erheblich. Über eine zusätzliche WhatsApp Business API können die Mitarbeiter mit Kunden, Partnern und Dienstleistern kommunizieren – das unterstützt insbesondere im Kundenservice.

Direkte Anbindung an das UEM-System bzw. die MDM-Umgebung: Dadurch ist es möglich, die App auf den Geräten der Mitarbeiter automatisch auszurollen und eine nutzerfreundliche Registrierung zu unterstützen. UEM bzw. MDM stellt sicher, dass nur autorisierte Endgeräte auf Ressourcen hinter der Firewall des Unternehmens zugreifen dürfen und Daten bei einem Geräteverlust nicht in unbefugte Hände gelangen.

Den kommunikativen Brückenschlag wagen

Eine ganzheitliche interne Kommunikation im Sinne eines mobilen Büros ist bereits heute mit einer Business Messaging App möglich. Damit die Mitarbeiter eine solche Lösung akzeptieren und in vollem Umfang in der Team-Kommunikation nutzen, müssen IT-Administratoren neben den technischen Anforderungen auch die Mitarbeiter-Bedürfnisse im Blick haben. So gelingt nicht nur der kommunikative Brückenschlag zwischen den Mitarbeitern, sondern auch mit der IT-Abteilung. □

Der Autor

Bild: Teamwire

Tobias Stepan ist Gründer und Geschäftsführer der Teamwire GmbH (www.teamwire.eu), die sich auf sicheres und souveränes Instant-Messaging für Unternehmen, Behörden und das Gesundheitswesen spezialisiert hat. Er engagiert sich für die mobile Digitalisierung und ein starkes, europäisches IT-Ökosystem.

Der Bank-Verlag

Die Bank-Verlag GmbH ist weder nur ein Verlag, noch sind nur Banken ihre Kunden. Seit seiner Gründung als Fachverlag im Jahr 1961 hat sich der Bank-Verlag mehrheitlich als IT-Dienstleister etabliert und betreibt hochsichere IT-Systeme und Anwendungen für die Abwicklung des elektronischen Zahlungsverkehrs und zur Einhaltung von Compliance-Anforderungen.

Das Unternehmen verfügt über langjährige Erfahrung in den Bereichen Debit- und Kreditkarten sowie E-Banking und hat darauf aufbauend sein ganzheitliches Angebot an Dienstleistungen zur Cyber-Security kontinuierlich weiterentwickelt.

Die Security-Kompetenz des Bank-Verlags

Der Bank-Verlag hat nicht nur an den heutigen E-Banking-Standards und den dazugehörigen Sicherheitsverfahren wie HBCI, FinTS, EBICS, Elektronische Unterschrift, mobileTAN, chipTAN etc. aktiv mitgearbeitet, er betreibt seit 20 Jahren eine hochsichere Online-Banking- und Firmenkunden-Banking-Plattform, dazu ein internationales Netzwerk zu Banken, Ermittlungs- und Strafverfolgungsbehörden sowie eine sichere Kommunikationsplattform für den Informationsaustausch zwischen Banken. Der Bank-Verlag ist aktiv in den Sicherheitsgremien des Bankenverbands und der Deutschen Kreditwirtschaft.

Mit seinen Produkten und Dienstleistungen setzt der Bank-Verlag fortlaufend neue Maßstäbe, u.a. in den Kompetenzbereichen

- Security
- Trusted Services & Digital ID
- Cards & Payment Solutions
- Mobile & Online Banking.

Dazu einige Beispiele:

BV Secure – die zentrale Authentifikationsplattform

Mithilfe dieser Authentifizierungslösung können Unternehmen sichere Zwei-Faktor-Verfahren für ihre Anwendungen umsetzen. Die Plattform umfasst alle gängigen und modernen Authentifikationsverfahren wie mobile TAN, photoTAN und pushTAN. Die verschiedenen Verfahren lassen sich einfach und flexibel in die eigenen Anwendungen integrieren. Der Bank-Verlag stellt eine hochverfügbare, schnelle und sichere Lösung zur Verfügung, die permanent auf dem Stand der Technik und den gesetzlichen Anforderungen gehalten wird.

BV Detect – das Online-Betrugserkennungssystem

Das Fraud-Prevention-Tool für Online- und Mobile-Banking prüft in Echtzeit einzelne

Transaktionen gegen alle verfügbaren Sensoren. Der modulare Aufbau mit technischen und qualitativen Sensoren, die individuell parametrisiert werden können, ermöglicht einen hoch individuellen Einsatz. Dabei werden Datenbasen von IP-Adressen, Mobilfunknummern etc. von mit Schadcode infizierten Kundensystemen laufend aktualisiert. BV Detect liefert revisionssicher volle Transparenz durch nachvollziehbare Entscheidungsbäume.

Trusted Services & Digital ID

Bündelung aller Services rund um elektronische Signaturen / Siegel und Identifizierung.

BVsign – qualifizierte elektronische Signatur

Mit der elektronischen Signatur wird die medienbruchfreie und papierlose Abwicklung von Geschäftsprozessen ermöglicht. Der Fernsignatur-Service BVsign lässt sich ganz einfach über eine Schnittstelle (API) an die vorhandenen Prozesse des Unternehmens anbinden, es wird kein weiteres Medium oder Software beim Endkunden benötigt.
Die qualifizierte elektronische Signatur hat die höchste Sicherheitsstufe und ist nach der eIDAS-Verordnung genauso rechtwirksam wie die handschriftlich erstellte Unterschrift und darüber hinaus europaweit rechtlich anerkannt. Der Bank-Verlag ist ein durch die Bundesnetzagentur zugelassener Vertrauensdiensteanbieter für die Erstellung qualifizierter Zertifikate für elektronische Signaturen.

BVseal – qualifiziertes elektronisches Siegel

Das elektronische Siegel ist der EU-weit anerkannte digitale Stempel für juristische Personen und wurde unter eIDAS neu eingeführt. Er weist den Ursprung (Authentizität) und die Unversehrtheit (Integrität) von Dokumenten nach; damit können Unternehmen und Behörden ihre Prozesse digital abwickeln und somit die Dokumentenherkunft

bestätigen. Auch die Unveränderlichkeit von Dokumenten kann somit vollständig sichergestellt werden.
BVseal kann überall dort eingesetzt werden, wo eine persönliche Unterschrift nicht notwendig, aber der Nachweis der Authentizität gewünscht ist.

BVident – eID Services

Mit der Online-Ausweisfunktion des Personalausweises identifizieren sich die Nutzerinnen und Nutzer sicher online oder offline. Damit können Behördengänge oder geschäftliche Angelegenheiten einfach und sicher erledigt werden und einem Identitätsdiebstahl wirksam begegnet werden. Der Bank-Verlag bietet in Kooperation mit der Governikus KG eID-Dienste für die Online-Ausweisfunktion und das Vor-Ort-Auslesen des Ausweises an.

Der Bank-Verlag – ein starker Partner für Banken und andere Unternehmen – bietet ein umfangreiches Portfolio von skalierbaren Security-Anwendungen, die jedem Nutzer hochaktuelle, sichere und vollständig digitale Prozessabläufe ermöglichen. ■

China als Datenschutzvorreiter: Unglaublich? Unglaublich!

Unsere Privatsphäre liegt uns allen am Herzen und im Grunde gehen wir davon aus, dass Unternehmen und Behörden unsere sensiblen Daten entsprechend behandeln. Sorgen müssen wir uns ja keine machen, da die DSGVO Unternehmen und Behörden dazu verpflichtet, unsere sensiblen Daten auf beste Art und Weise zu schützen, oder?

Von Elmar Eperiesi-Beck, eperi

Bild: tanaonte/stock.adobe.com

Was nutzt die DSGVO, wenn die Instanzen, die eigentlich für deren Einhaltung sorgen sollten, Absprachen treffen, welche die DSGVO unterlaufen? So geschehen im Falle der „Privacy Shield" genannten Übereinkunft zwischen den USA und der EU. Privacy Shield erlaubte es, personenbezogene Daten von EU-Bürgern, gegen die Bestimmungen der DSGVO, in die USA zu übertragen. Dass es dabei nicht mit rechten Dingen zuging, hat der Europäische Gerichtshof (EuGH) bestätigt und „Privacy Shield" für ungültig erklärt. Das stellt einerseits Unternehmen

vor Probleme, die nahezu allesamt Produkte der amerikanischen Technologieriesen nutzen und davon ausgehen müssen, dass sie den von der DSGVO geforderten Schutz ihrer Kundendaten nicht gewährleisten können. Andererseits verdeutlicht es selbst dem wohlwollendsten Beobachter, dass es sich bei Privacy Shield ohnehin bestenfalls um ein Deckmäntelchen handelte. Das kann schon darum nicht verwundern, weil es bereits der zweite Versuch eines solchen Abkommens war, das der Prüfung durch den EuGH nicht standhielt. Privacy Shield war ja lediglich alter „Safe Harbour"-Wein in einem neuen Schlauch.

China als Vorreiter

Die chinesische Regierung scheint gerade den Schutz der personenbezogenen Daten ihrer Bürger ernster zu nehmen als die EU. Es mag den ein oder anderen verwundern, dass die chinesische Regierung überhaupt einen Gedanken an den Schutz personenbezogener Daten verschwendet.

Tatsächlich hat China im Vergleich zu den USA und der EU auch erst spät entsprechende Gesetze erlassen. China betrachtet den Schutz sensibler Daten als Unterteil der nationalen Sicherheit. Der Schutz personenbezogener Daten ist darum gegen den Missbrauch (ausländischer) Unternehmen und Staaten gerichtet. Wirklich interessant wird diese Tatsache im Zuge der aktuellen Antikorruptionsbemühungen in China. Konnten sich Unternehmen bisher gerüchteweise von der Verpflichtung loskaufen, personenbezogene Daten nur in China zu speichern und zu verarbeiten, wird dies nun zunehmend unmöglich. Die Entscheidung über die Nutzung wird nicht mehr zentral, sondern dezentral getroffen, von sogenannten Data Review Boards (DRB). Ein wesentlicher Unterschied zwischen China und Europa besteht darin, dass Unternehmen in Europa in der Regel zunächst mit Daten umgehen dürfen, wie sie es für richtig halten, solange dies nicht explizit gegen geltende Regeln verstößt. In China hingegen müssen Unternehmen geplante Datentransfers ins Ausland zunächst durch die DRB prüfen und freigeben lassen. Häufig genug erhalten sie negative Bescheide.

Unternehmen im Regen stehen gelassen

Unternehmen, die in China Geschäfte betreiben wollen, stehen somit vor einem massiven Problem. Sie sind weitgehend abhängig von den Cloud-Lösungen US-amerikanischer Anbieter, die Vieles können, aber bestimmt nicht die Sicherheit personenbezogener Daten in den USA garantieren.

Ausländische Unternehmen mit Geschäftsstellen in China können daher US-amerikanische Cloud-Technologie nicht mehr mit kritischen Daten nutzen, und auch auf dem Heimatmarkt findet diese Nutzung häufig zumindest in einer (Dunkel-)Grauzone statt, die durch den Fall des Privacy Shield entstanden ist. Der Verzicht auf Cloud-Lösungen wie Microsoft 365 oder Salesforce kann in dieser Situation nicht der Ausweg sein. Leistungsstarke Alternativen sind einfach nicht zu finden.

Einfache Lösung

Die Lösung der Datenschutz- und Datensicherheitsprobleme liegt auf der Hand und ist seit vielen Jahren bekannt, scheint aber mit einem Wahrnehmungs- bzw. Imageproblem zu kämpfen zu haben.

Wie sonst ist zu erklären, dass Datenanonymisierung und -pseudonymisierung nicht flächendeckend eingesetzt werden, obwohl sie doch in der EU-DSGVO in Artikel 4 explizit als Lösung genannt werden?

Auch das Chinese Cybersecurity Law (CSL) spricht in §42 von „de-identification"-Techniken, welche im chinesischen Standard „The Information Security Technology – Guide for ⇨

De-Identifying Personal Information“ als Pseudonymisierung erklärt werden.
Der deutsche Hersteller für entsprechende Software-Lösungen – die eperi GmbH – hat in Kooperation mit einer führenden chinesischen Anwaltskanzlei für seine Kunden umfangreiche Freigaben für den Einsatz von amerikanischen Cloud-Lösungen erhalten. Die eperi Lösung stellt sicher, dass alle kritischen Daten pseudonymisiert in der Cloud gespeichert werden.

Anonymisierung und Verschlüsselung – aber richtig

Zunächst ist zu betonen, dass hier nicht von einer Verschlüsselung von Daten durch den Cloud Provider gesprochen wird. Um Daten verschlüsseln zu können, muss der Provider zunächst Zugriff auf die unverschlüsselten Daten haben. Für den Schutz personenbezogener Daten und die Einhaltung entsprechender Richtlinien ist so nichts gewonnen. Unternehmen müssen ihre Kundendaten selbst anonymisieren und pseudonymisieren, bevor sie diese in die Cloud übertragen. Der besondere Vorzug dieser Techniken besteht darin, dass Unbefugte mit den gesicherten Daten nichts anfangen können, selbst dann nicht, wenn es ihnen gelingen sollte, unrechtmäßigen Zugriff darauf zu erlangen.

Vorbehalte und Vorurteile

Wie gesagt scheint es gegen diese Vorgehensweise etliche Vorbehalte zu geben, denn sie findet aktuell noch lange nicht die Verbreitung, die nötig und wünschenswert ist. Zunächst einmal leiden Technologien zur Anonymisierung und Pseudonymisierung an einem allgemeinen Image-Problem, das sie mit anderen Sicherheitstechnologien teilen: Sie werden als Belastung empfunden, keinesfalls als Wettbewerbsvorteil. Das scheint ein eklatanter Fehler. Gerade in einem Land wie Deutschland, wo Umfragen immer wieder belegen, wie wichtig Konsumenten der Schutz ihrer Privatsphäre ist, sollten Unternehmen die Chance nutzen, sich offensiv als Organisation zu positionieren, denen dieser Schutz wirklich am Herzen liegt.
Auch auf technischer Ebene bestehen Vorurteile und Missverständnisse, wenn es um Datenanonymisierung und -pseudonymisierung geht. So gilt die Technologie als komplex. Ebenso wird ihr unterstellt, dass sie Prozesse inakzeptabel verlangsame. Ein modernes Kryptographie-Gateway allerdings widerlegt diese Unterstellungen. Dieses verschlüsselt die Daten und leitet sie erst dann an den Cloud-Anbieter weiter. Das Gateway übernimmt auch die Entschlüsselung der Daten aus der Cloud. Die Performance der jeweils genutzten Cloud-Anwendung bleibt aus Benutzersicht davon nahezu unbeeinträchtigt. Auch ist ein Kryptographie-Gateway alles andere als komplex. So bietet der Hersteller eperi für sein Gateway beispielsweise kostenlose Testumgebungen an, die innerhalb von lediglich vier Stunden im Unternehmen einsatzbereit sind. Einfacher geht’s kaum.
Ein anderer Vorbehalt gegen Anonymisierung und Kryptographie entbehrt erst einmal nicht

Der Autor


Bild: eperi

Elmar Eperiesi-Beck leitet die 2014 gegründete eperi GmbH als CEO & Gründer. In seinem Bestreben die IT-Welt sicherer zu machen, bringt er sich als Gründungsmitglied der Allianz für Cyber-Sicherheit sowie als Mitglied des Bundesverbands für IT-Sicherheit e.V. (TeleTrusT) aktiv in aktuelle Diskussionen rund um das Thema Cloud-Sicherheit ein. Eine seiner Kernkompetenzen ist die Beratung von Unternehmen in Bezug auf die Reduktion der Anwendbarkeit der europäischen Datenschutzgrundverordnung (EU-DSGVO) – speziell bezogen auf die Speicherung personenbezogener Daten in der Cloud.

Bild: eperi

Ein Kryptographie-Gateway verschlüsselt personenbezogene Daten, schon bevor sie in die Cloud-Anwendung gelangen.

einer gewissen Berechtigung. So sorgen Anonymisierung und Pseudonymisierung grundsätzlich für eine Funktionseinschränkung. Bei vielen Anonymisierungs- und Pseudonymisierungs-Lösungen sind wichtige Funktionen wie z.B. Suchen und Sortieren stark eingeschränkt. Dieses Problem ist allerdings alles andere als unüberwindlich. Auch hier bietet ein modernes Kryptographie-Gateway Abhilfe. Ein solches Gateway ver- und entschlüsselt bzw. tokenisiert Daten nicht nur, es indiziert diese auch für spätere Durchsuch- und Sortierbarkeit. Praktisch kommt es so zu keinen relevanten Einschränkungen für die Nutzer der jeweiligen Cloud-Anwendung.

Unternehmen sollten handeln – jetzt!

Gerade im Lichte der neuesten Entwicklungen rund um die DSGVO, den Privacy Shield und staatliche Datenschutzmaßnahmen, wie denen der chinesischen Regierung, sollten Unternehmen sich mit dem Thema „Kryptographie-Gateway“ näher auseinandersetzen. Werden personenbezogene Daten nicht nach dem aktuellen „Stand der Technik“ (siehe bspw. TeleTrusT) pseudonymisiert, haftet das Management persönlich. Dabei ist ein solches Gateway in Standardkonfiguration für die meisten Cloud-Anwendungen „von der Stange“ erhältlich. Zudem besteht die Möglichkeit, das Gateway individuell an jede gewünschte Cloud-Anwendung anzupassen.

Natürlich sind nicht alle Gateways gleich beschaffen. Unternehmen sollten darauf achten, dass wirklich alle Cloud-Anwendungen abgedeckt sind. Insbesondere sollten sie auf Multi-Cloud-Unterstützung durch das Gateway achten, denn die wenigsten Unternehmen nutzen lediglich eine Cloud-Anwendung. Gerade in der aktuellen Situation, mit einem intensiven Gebrauch von Kooperations- und Videokonferenzlösungen wie Microsoft Teams, sollte ein Gateway diese Lösungen nicht nur unterstützen, sondern sicherstellen, dass die wichtigen Funktionen für den Anwender erhalten bleiben. Unternehmen sollten aufhören, Datenschutz als notwendiges Übel zu begreifen und stattdessen die Wettbewerbsvorteile nutzen, die ein fortschrittlicher Umgang mit personenbezogenen Daten bietet. So machen sie sich zudem unabhängig vom gesetzgeberischen Hin und Her und halbgaren internationalen Datenschutzabkommen. □

Cloud VPN as a Service „Made in Germany“ by ucs und NCP!

Managed Security Services, Cloud Services und das Outsourcing von wichtigen IT-Leistungen generell sind bei über 50% der deutschen Unternehmen bereits in der Praxis angekommen. **ucs** und **NCP** bieten abhörsichere Kommunikation als zukunftsweisende Advanced Cloud VPN-Lösung „Made in Germany“ an.

Geeignet ist die **Advanced Cloud VPN-Lösung** für KMU und Konzerne gleichermaßen. Die Vorteile liegen unter anderem in der zentralen Verwaltbarkeit, hoher Skalierbarkeit und Bandbreiten sowie einem nutzungsabhängigen, transparenten Preismodell (Pay per Use), das sich am individuellen Bedarf orientiert.

Nutzer der rein softwarebasierten Lösung sparen letztendlich eigene IT-Ressourcen und profitieren von der großen Expertise der deutschen IT-Spezialisten ucs und NCP. Angeboten werden zwei Modelle, die **Shared Platform** und **Dedicated Platform** auf Wunsch für jeden Kunden einzeln.

Shared Platform

Kunden werden als autarke Mandanten auf einer gemeinsamen Plattform betreut, die ucs inklusive 1st und 2nd Level Support hostet und betreibt. Der Bedarf an VPN Clients kann monatlich variabel reduziert oder erhöht werden.

Dedicated Platform

Auf Wunsch können Kunden eine vollkommen getrennte NCP Infrastruktur beziehen. Sämtliche Enterprise VPN-Komponenten inklusive aller Supportdienstleistungen werden dabei zur Verfügung gestellt und nach tatsächlicher Nutzung abgerechnet.

NCP engineering GmbH

Die NCP engineering GmbH mit Hauptsitz in Nürnberg ist ein weltweit führender Software-Hersteller für hochsichere Lösungen in den Bereichen Remote Access, Endpoint Security und Industrie 4.0 / IIoT. Namhafte, global agierende Großkonzerne, mittelständische Unternehmen, Ministerien und Behörden setzen seit über 30 Jahren auf die Lösungen „Made in Germany“, um ihre IT-Infrastrukturen vor den aktuellen Bedrohungssituationen zu schützen. Zum Portfolio gehören auch vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Lösungen. Skalierbarkeit und Mandantenfähigkeit der Software-Lösung von NCP zum Einsatz bei Managed Service Providern für Tausende von Anwendern.
www.ncp-e.com

ucs datacenter GmbH

Die ucs datacenter GmbH bietet ganzheitliche ITK-Dienstleistungen sowie zukunftsweisende Cloud-Lösungen für Unternehmen an, die durch Skalierbarkeit, Flexibilität und kalkulierbare Preisstrukturen in der dynamischen Arbeitswelt vieler Mittelständler punkten. Von Colocation über Cloud Back-up bis hin zu Everything as a Service werden mittelstandstaugliche Cloud-Lösungen aus dem eigenen Düsseldorfer Rechenzentrum angeboten.
Als Teil der unilab Unternehmensgruppe beschäftigt ucs ca. 15 Mitarbeiter an drei Standorten in NRW (Hauptsitz in Mönchengladbach, Rechenzentrum in Düsseldorf sowie die Verwaltungsgesellschaft unilab in Paderborn).
www.ucs.cloud

NCP
SECURE COMMUNICATIONS

u c s

Neugierig geworden?

TeleTrusT-Leitfaden zur E-Mail-Verschlüsselung

Die TeleTrusT-Arbeitsgruppe „Cloud Security“ hat eine umfangreiche Informationsbroschüre zu E-Mail-Verschlüsselung erstellt. Die Publikation einschließlich illustrierter Handlungsanleitungen richtet sich sowohl an IT-Experten als auch an IT-Interessierte.

Von Peter Schmitz, Security-Insider

Kommunikation über E-Mail mit Kunden und Geschäftspartnern gehört zum Tagesgeschäft der meisten Unternehmen und Organisationen. Viele Nutzer wissen allerdings nicht, dass die Versendung einer E-Mail dem Transport einer Postkarte durch Unbekannte entspricht. Nur 60 Prozent der E-Mails werden transportverschlüsselt (SSL) übertragen. Der Anteil verschlüsselter E-Mails (PGP oder S/MIME) geht sogar gegen Null.

Jedes zweite Unternehmen in Deutschland und Österreich hatte dagegen bereits einen konkreten Spionageangriff auf ihre EDV-Systeme oder zumindest Verdachtsfälle zu beklagen. Dabei handelt es sich vor allem um Hackerangriffe sowie um abgefangene elektronische Kommunikation: In Deutschland stellten 41,1 Prozent, in Österreich 40,0 Prozent derartige Aktivitäten fest. Doch nur ein Bruchteil setzt auf Verschlüsselung.

Es waren unter anderem diese Zahlen aus der Studie „Industriespionage 2014 – Cybergeddon der Wirtschaft durch NSA & Co.?“, die die TeleTrusT-Arbeitsgruppe „Cloud Security“ zum Anlass nahm, einen Leitfaden zur E-Mail-Verschlüsselung zu veröffentlichen. Der mehr als 70 Seiten umfassende Leitfaden erläutert E-Mail-Verschlüsselungs- und Signaturmechanismen, legt Funktionsweise, Relevanz und technischen Hintergrund der E-Mail-Verschlüsselung dar und gibt konkrete Handlungsempfehlungen.

E-Mail-Verschlüsselung ist längst nicht mehr so komplex

„Da die Kommunikation per E-Mail in zahlreichen Organisationen und Unternehmen Kommunikationsmittel Nummer Eins ist, ist die Verschlüsselung von E-Mails einer der wesentlichen Schritte in der Kommunikationssicherheit“, sagt Patrycja Tulinska, Geschäftsführerin der PSW Group. Der Anbieter von E-Mail-Zertifikaten ist als Mitglied der Arbeitsgruppe „Cloud Security“ an der Publikation beteiligt. „E-Mail-Verschlüsselung macht aus einer für alle lesbaren Postkarte einen versiegelten Brief, den nur der berechtigte Empfänger lesen kann“, betont Tulinska und sagt weiter: „E-Mail-Verschlüsselung ist wichtig, weil zum einen bestimmte Daten und Informationen schlichtweg geheim gehalten werden sollen. Zum anderen müssen Compliance-Richtlinien erfüllt werden. Mit der Datenschutz-Grundverordnung macht

der Gesetzgeber auch konkrete Vorgaben zum Umgang mit personenbezogenen Daten."

So zeigt die neue TeleTrust Publikation unter anderem Technologien auf, die das Verschlüsseln von E-Mails ermöglichen. Vorgestellt werden praxisnahe Lösungen, etwa die Verschlüsselung direkt im Client des Anwenders sowie alternative Gateway-Lösungen. „In Zeiten von Schwachstellen wie Efail, Industriespionage und Hackerangriffen stellt die verschlüsselte Übertragung von E-Mails einen immens wichtigen Baustein zur IT-Sicherheit dar. Nur verschlüsselte Kommunikation kann als sicher und vertrauenswürdig angesehen werden", betont Tulinska und ergänzt: „Da gängige E-Mail-Programme die Verschlüsselung unterstützen und mit Gateway-Lösungen der Aufwand nicht beim User, sondern in der IT-Abteilung liegt, gibt es auch keine Ausreden: E-Mail-Verschlüsselung ist längst nicht mehr so komplex wie häufig angenommen."

Peter Hansemann, Leiter des TeleTrusT-Arbeitskreises „Mail Security": „Ungeachtet der wachsenden Nutzung von Messengern bleibt E-Mail trotz aller Sicherheitsdefizite das meist genutzte Medium der elektronischen Kommunikation. TeleTrusT bietet mit der nunmehr 3. Auflage des Leitfadens zur E-Mail-Sicherheit eine praxisorientierte Handreichung für Unternehmen, aber auch für private Anwender, um ihre E-Mail-Kommunikation sicherer zu gestalten."

Unterschiedliche Verschlüsselungsansätze

Bei der Verschlüsselung über den E-Mail-Client des Users können E-Mail-Zertifikate auf einem Token oder als Softkey vorhanden sein. So lässt sich die Verschlüsselung Ende-zu-Ende realisieren. Die E-Mails liegen auch auf dem Mailserver sowie im internen Unternehmensnetz immer verschlüsselt vor. Die E-Mail-Verschlüsselung über S/MIME wird von gängigen E-Mail-Programmen wie Outlook unterstützt, während für PGP in aller Regel zusätzliche Programme benötigt werden. Für Verschlüsselungs-Gateways wird hingegen zentral konfiguriert, welche E-Mails ausschließlich verschlüsselt übertragen werden. Entsprechende Prozesse innerhalb der IT-Administration nehmen die Komplexität der Verschlüsselung dem einzelnen User ab. Ein Gateway kann sicherstellen, dass bestimmte Kommunikation grundsätzlich verschlüsselt wird, außerdem lassen sich Mail-Inhalte vor dem Verschlüsseln und nach dem Entschlüsseln auf Malware oder kritische Inhalte prüfen.

„Welcher dieser Ansätze im rechtlichen, organisatorischen und technischen Kontext für welches Unternehmen geeignet ist, muss jede Organisation für sich entscheiden. Denkbar ist auch ein Mix: Bestimmte Mitarbeiter verschlüsseln am Client, die restliche Belegschaft nutzt die Verschlüsselungsfunktion des Gateways", rät Patrycja Tulinska. □

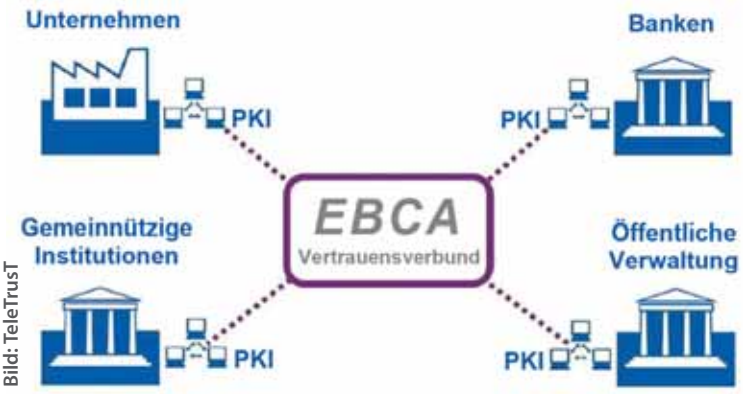


Bild: TeleTrusT

Mit der European Bridge CA (EBCA) hat TeleTrusT eine Initiative ins Leben gerufen, die für Nutzer den sicheren und komfortablen Austausch verschlüsselter Daten ermöglicht. Sie ist ein Zusammenschluss einzelner, gleichberechtigter Public-Key-Infrastrukturen (PKIen) zu einem PKI-Verbund und ermöglicht eine sichere und authentische Kommunikation zwischen den beteiligten Unternehmen, Institutionen und öffentlichen Verwaltungen.

Managed Email Security *Made in Germany*: einfach buchen

E-Mail-Sicherheit erfordert immer mehr Spezial-Know-how, das die meisten Unternehmen intern nicht vorhalten können. Umso sinnvoller ist es, dieses Thema als Service in Expertenhände zu legen. Wir erklären anhand von NoSpamProxy Cloud, wie das geht und worauf man dabei achten sollte.

Angriffe auf die E-Mail-Kommunikation werden immer professioneller und die Angriffsszenarien immer gezielter und raffinierter. Diese Angriffe zu erkennen und abzuwehren, erfordert immer mehr Detail-Know-how und technischen Aufwand.

Da das Thema E-Mail-Sicherheit natürlich nur eines von vielen dringlichen Themen der internen IT-Verantwortlichen darstellt, ist es für die meisten Unternehmen ausgesprochen unwahrscheinlich, dass sie auf Dauer im Wettlauf mit den Angreifern gewinnen können. Wie kaum ein anderes Thema in der IT eignet sich E-Mail-Sicherheit dazu, als Managed Service aus der Cloud bezogen und so in externe Expertenhände gelegt zu werden. Besonders einfach ist die Umstellung, wenn man seine Postfächer ohnehin bereits durch Microsoft Office 365 bezieht. Vielen Kunden reichen die Schutzmaßnahmen von Microsoft Office 365 zur Einhaltung von Datenschutz- und Compliance-Auflagen nicht aus und sie suchen nach passenden Ergänzungen.

Für Managed Cloud Services sprechen insbesondere vier Argumente:

1. Sofort einsatzbereit – ohne Installation

NoSpamProxy Cloud ist ohne Installation sofort verfügbar und nutzbar. Kunden profitieren direkt von wirkungsvollem Spam- und Malware-Schutz, sicherer E-Mail-Verschlüsselung und einfachem Versand großer Dateien.

2. Bester Schutz durch stets aktuelle Konfiguration

Wir sorgen dafür, dass die Lösung stets für den Kunden optimal konfiguriert ist. Neueste Features und Schutzmechanismen sind sofort nutzbar und Kunden so bestmöglich vor neuen Bedrohungen geschützt.

Der Autor

Stefan Cink ist E-Mail-Security-Experte bei Net at Work und Business Unit Manager für die integrierte E-Mail-Security-Suite NoSpamProxy. Er engagiert sich im TeleTrust EBCA Lenkungsgremium und Arbeitskreis E-Mail-Security und wurde für seine Vorträge und Workshops von der Vogel IT-Akademie mehrfach als Best Speaker für IT-Security ausgezeichnet.

3. Entlastung der IT-Abteilung

Die interne IT kann sich sofort wertschöpfenden Projekten widmen. Oft entsteht durch den Umstieg auf Managed Cloud Services auch direkter Zusatznutzen wie eine praktikable E-Mail-Verschlüsselung.

4. Geringe, kalkulierbare Kosten & hohe Skalierbarkeit

Kunden vermeiden hohe Anfangsinvestitionen für Software und Hardware. Die monatlich geringen Kosten sind absolut transparent kalkulierbar und die Lösung skaliert problemlos mit dem tatsächlichen Bedarf.

Dabei ist der Umstieg in vier Schritten denkbar einfach: Man meldet sich mit seinem Microsoft-Konto bei NoSpamProxy Cloud an, konfiguriert die entsprechende Domain, fügt die Benutzer ein und richtet das E-Mail-Routing ein. Für einzelne Empfänger oder Gruppen, aber auch für bestimmte Absendergruppen kann mit den drei Leveln SOFT, MEDIUM und STRICT intuitiv und einfach die Schärfe der Prüfungen festgelegt werden. Von NoSpamProxy und dem Expertenteam wird dies dann in ein detailliertes Regelwerk umgesetzt und aktuell gehalten. Während der Konfiguration der Domain wird auch die Pflege der DKIM-Schlüssel an die Experten delegiert. Damit ist der aus Sicherheitsgründen regelmäßig erforderliche Schlüsselaustausch sichergestellt.

Mit NoSpamProxy Cloud erhalten Kunden bestmöglichen Schutz vor Spam, Malware, Phishing und CEO-Fraud durch die detaillierte Prüfung der Sender- und Empfängerreputation mit über 20 unterschiedlichen Prüfungen, inklusive SPF, DKIM und DMARC. Das intelligente Anhangs- und URL-Management blockiert schädliche Links in E-Mails und Anhängen oder wandelt diese in unkritische PDF-Dateien um. Die sichere E-Mail-Verschlüsselung stellt Rechtssicherheit und Vertraulichkeit her und garantiert gleichzeitig volle DSGVO-Konformität. Auch Empfänger ohne Verschlüsselungsinfrastruktur können mit passwortgeschützten PDF-Dateien sicher erreicht werden.

Die webbasierten Funktionen zur Analyse und Nachrichtenverfolgung gehen weit über das Angebot von Microsoft Office 365 hinaus und erlauben einen detaillierten Überblick über den E-Mail-Verkehr. Nicht umsonst wurde NoSpamProxy im unabhängigen User Ranking wiederholt von Nutzern zum Champion gewählt. Kostenloser Test unter **www.nospamproxy.de/cloud** ■

5 Tipps zur Auswahl eines cloudbased Managed Service für E-Mail-Sicherheit

1. **Produkte und Services Made in Germany nutzen, um höchstmögliche Konformität mit deutschen Datenschutz- und Compliance-Auflagen zu garantieren.**
2. **Ein integriertes Produkt, das auch E-Mail-Verschlüsselung und File Transfer bietet, sorgt für weniger Abhängigkeiten und eine deutlich erhöhte Sicherheit.**
3. **Höchste Leistungsfähigkeit im Reputationsmanagement bedeutet höchsten Schutz auch vor CEO-Fraud und Social Engineering.**
4. **Selbstlernendes White-Listing sorgt für minimale False Positives und damit geringstmöglichen Aufwand.**
5. **Nutzung von Schwarm-Intelligenz und KI zur Erkennung neuer Angriffsmuster schafft Zukunftssicherheit.**

IT-Sicherheitsexperten entdecken Schwachstellen in Mailto-Links

Forscher des Labors für IT-Sicherheit der FH Münster haben für Mailto-Links auf Webseiten bei einigen E-Mail-Programmen Sicherheitslücken entdeckt. Hacker könnten dadurch die privaten Schlüssel für OpenPGP oder S/MIME erlangen und dadurch Zugriff auf verschlüsselte Nachrichten bekommen.

Von Peter Schmitz, Security-Insider

Bild: peshkov/stock.adobe.com

Wer jemandem von einer Webseite aus eine E-Mail schicken möchte, kann dies häufig direkt mit einem Klick auf die dort veröffentlichte E-Mail-Adresse – schon öffnet sich im E-Mail-Programm automatisch das Nachrichtenfenster an den gewünschten Empfänger. Prof. Dr. Sebastian Schinzel und Damian Poddebniak vom Labor für IT-Sicherheit der FH Münster haben für diese sogenannten Mailto-Links nun bei einigen E-Mail-Programmen Sicherheitslücken entdeckt. Hacker könnten dadurch zum Beispiel Zugriff auf verschlüsselte Nachrichten bekommen.

Prof. Schinzel erklärt zum Problem mit Mailto-Links und Verschlüsselungen: „Gemeinsam mit Wissenschaftlern der Ruhr-Universität Bochum untersuchen wir im Labor für IT-Sicherheit bereits seit 2018 unterschiedliche Sicherheitslücken im Kontext von E-Mail-Verschlüsselungen. Dabei geht es um die Sicherheit der Verschlüsselungstechnologien OpenPGP und S/MIME, wie sie zum Beispiel von Journalisten und politischen Aktivisten, aber auch von Unternehmen und Behörden eingesetzt werden. In unserer neuesten Studie haben wir einen kreativen und zugleich sehr simplen Angriff untersucht. Wir haben gezeigt, wie erschreckend einfach man sich über Mailto-Links den privaten Schlüssel von Absendern zuschicken lassen kann. Mit diesem privaten Schlüssel kann man verschlüsselte OpenPGP- oder S/MIME-Nachrichten entschlüsseln."

Wie genau funktioniert der Angriff?

„Beim Erstellen eines Mailto-Links auf Webseiten können über HTML-Befehle bestimmte Inhalte der E-Mail vorgegeben werden", erläutert Prof. Schinzel. „Neben der E-Mail-Adresse des Empfängers und dem Betreff erzwingen manche E-Mail-Programme, eine vorausgewählte Datei anzuhängen und mitzuschicken. Damit das funktioniert, muss der Hacker den exakten Namen der Datei und ihren Speicherort auf dem Computer eines Absenders kennen. Das ist bei den meisten persönlichen Dateien natürlich schwierig herauszufinden. Der private E-Mail-Schlüssel hingegen hat bei OpenPGP und S/MIME immer den gleichen Namen und wird üblicherweise über einen Standardpfad auf dem Computer gespeichert."

Bild: FH Münster/Wilfried Gerharz

IT-Sicherheitsexperte Prof. Dr. Sebastian Schinzel hat gemeinsam mit Doktorand Damian Poddebniak und Forschern der Ruhr-Universität Bochum Sicherheitslücken in Mailto-Links gefunden.

Fällt es nicht auf, wenn man ungewollt einen Anhang mitschickt?

Prof. Schinzel erklärt: „Ein aufmerksamer Absender kann das sehen, aber die meisten Leute achten in der Eile einfach nicht darauf – sie wollen schließlich nur schnell und unkompliziert eine E-Mail verschicken. Die Hersteller von E-Mail-Programmen sind daher in der Pflicht, dieses Problem zu beheben. Vorausgefüllte E-Mail-Adressen und der Betreff sind unproblematisch, aber es sollte gar nicht erst möglich sein, Dateianhänge in Mailto-Links einzubinden. Wir haben die Mailbetreiber vor unserer Veröffentlichung über die Sicherheitslücke informiert, sodass mittlerweile Updates verfügbar sind." □

PSW GROUP

SSL-Zertifikate | S/MIME | Code Signing

Ihr Marktplatz für digitale Verschlüsselung!

www.psw-group.de/console

AUTOMATISIERUNG

REST-API | Plesk-Plugin | WHMCS-Plugin
Zertifikatsverlängerung | Großbestellungen

ZERTIFIKATSMANAGEMENT

Bestellung | Austausch | Verlängerung | Echtzeit-Überblick
Kundenverwaltung | Zugriff auf alle gängigen CAs & Produkte

SERVICELEISTUNGEN

Zertifikate-Wiki | Reminder bei Laufzeitende | Installationsservice
CSR-Generator & Decoder | Zertifikat-Konverter, Abgleich & Decoder

*Einlösbar in unserer PSW Konsole unter www.psw-group.de/console (Couponcode im Feld Gutscheincode angeben), gültig bis 31.12.2020. Nicht mit anderen Sonderaktionen oder Vorteilscoupons kombinierbar.

- Kauf auf Rechnung, PayPal oder per SEPA
- Kompetenter Support auf DE/EN/PL
- Große Auswahl aller gängigen Certificate Authorities
- 20 Jahre Erfahrung mit digitaler Verschlüsselung

Telefonischer Support

+49 661 480 276 10

COUPON 20% RABATT*

Einlösbar auf www.psw-group.de

IHR KENNENLERNCODE: HELLO-PSW

Unser Produktportfolio

- SSL-Zertifikate
- E-Mail-Verschlüsselung
- Code Signing Zertifikate
- Managed PKI
- Legal Entity Identifier (LEI)
- IoT-Zertifikate**
- PDF Signierung
- Dokumenten-Signierung
- Digitale Signaturen**

**Produkt auf Anfrage

TRUSTED SHOPS GUARANTEE

GEPRÜFTER ONLINE-SHOP EHI

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

Allianz für Cyber-Sicherheit

Externe verschlüsselte Datenträger: sicher oder nicht?

Datenträger wie USB-Sticks und Festplatten sind praktisch, jedoch bergen diese in sich zugleich ein hohes Risiko. Fast ein Viertel der verlorenen Daten geht auf den Verlust mobiler Endgeräte zurück.

Von Robert Nutsch, Digittrade

Die Folgen von Datenverlusten können für Unternehmen weitreichend sein: Beträchtliche Imageschäden, sinkendes Kundenvertrauen mit einhergehender Verschlechterung der Wettbewerbsfähigkeit und finanzielle Einbußen durch sinkende Umsätze, Vertragsstrafen von Handelspartnern, Strafen bei Compliance-Verstößen und Schadenersatzforderungen.
Mit der Einführung der DSGVO im Jahre 2018 wurden die Anforderungen im Umgang mit sensiblen und personenbezogenen Daten noch weiter verschärft. Die Entscheider sind verpflichtet, unter Berücksichtigung des Stands der Technik die geeigneten technischen und organisatorischen Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei Verstößen gegen diese Bestimmungen werden Geldbußen von bis zu 10.000.000 EUR verhängt. Um Fehler zu vermeiden, werden deshalb in immer mehr Unternehmen und Behörden USB-Slots an Dienstcomputern gesperrt und der Einsatz von externen Datenträgern wird untersagt.

Gibt es sichere mobile Datenträger?

Gibt es überhaupt sichere mobile Datenträger, die für die Speicherung sensibler Informationen geeignet sind? Was ist bei der Wahl eines geeigneten externen Datenträgers zu beachten? Wie erkenne ich, dass ein verschlüsselter Datenträger dem Stand der Technik entspricht?
Der einfachste und sicherste Weg ist, sich eine Antwort beim Bundesamt für Sicherheit in der Informationstechnik (BSI) telefonisch oder online zu holen. Es ist die einzige Stelle in Deutschland mit der Befugnis, offizielle Aussagen über die Sicherheitseigenschaften von IT-Produkten zu treffen und diese für die Erhebung und Aufbewahrung sensibler Informationen mittels Zertifizierungen oder Zulassungen freizugeben. Mit anderen Worten, das BSI nimmt Ihnen die Entscheidung ab, ob ein externer Datenträger über ein ausreichendes Schutzniveau für bestimmte Dateninhalte verfügt. Dazu gehört unter anderem die Wahrung der Vertraulichkeit von Daten bei logischen wie physischen Angriffen, wenn der Datenträger gestohlen oder entwendet wird – oder verloren geht.

Das BSI ist zuständig

Eine kurze Recherche auf der Website des BSI genügt bereits. Dort findet man neben den Anforderungskatalogen auch Produkte, für welche das BSI eine Zertifizierung nach Common

DIGITTRADE HS256 S3 – externe verschlüsselte High-Security-Festplatte mit BSI-Zertifizierung (BSI-DSZ-CC-0825-2017)

Bild: Digittrade

Criteria (BSI-CC) oder eine Zulassung für die Speicherung der Informationen mit unterschiedlichen Geheimhaltungsstufen (z.B. VS-NfD oder GEHEIM) erteilt hat. Unter anderem sind hier die zertifizierten Festplatten High Security HS256 S3 sowie die VS-NfD zugelassenen Datenträger KOBRA DRIVE VS und KOBRA Stick VS des deutschen Herstellers Digittrade zu finden. Seit 2005 entwickelt und produziert das Unternehmen externe verschlüsselte Festplatten und USB-Sticks mit dem Vertrauenszeichen „IT-Security Made in Germany“ von TeleTrusT.

In Europa oft stark beworben, dennoch rechtlich für deutsche Unternehmen und Behörden eher unbedeutend, sind die nach FIPS 140 zertifizierten Datenträger ausländischer Hersteller. FIPS 140-2 („Federal Information Processing Standard Publication 140-2“) ist ein US-amerikanischer Sicherheitsstandard der US-Regierung, der zur Genehmigung kryptografischer Module verwendet wird. Im Unterschied zu BSI-Zertifizierungen handelt es sich bei diesen FIPS-140-Zertifizierungen um die Bewertung der Kryptomodule und Verschlüsselungsalgorithmen. Die Beurteilung anderer Sicherheitsmechanismen findet indessen nicht statt.

Für die korrekte Einstufung der Sicherheitseigenschaften ist es jedoch zu empfehlen, das Schutzniveau der wichtigsten Sicherheitsmechanismen eines verschlüsselten Datenträgers zu bewerten: die Verschlüsselung, Zugriffskontrolle, Schlüssel- und Benutzer-Verwaltung. Die Gesamtsicherheit kann letztendlich nicht höher eingestuft werden als das Schutzniveau der schwächsten Komponente.

Für die Verschlüsselung von Daten ist zu empfehlen, die AES-Verschlüsselung mit einer Schlüssellänge von 256-Bit in einem verketteten Block-Modus (z.B. CBC oder XTS) zu verwenden. Dabei können im XTS-Modus gleichzeitig zwei 256-Bit-Kryptoschlüssel verwendet ⇨

KOBRA Stick VS – externer verschlüsselter USB-C-Speicherstick mit VS-NfD-, Nato- und EU-Zulassung (BSI-VSA-10338)

werden. Der „Advanced Encryption Standard" (AES) ist ein symmetrisches Kryptosystem, das beispielsweise in den USA auch für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen ist.

Verschlüsselung auf Software- oder Hardwarebasis

Zudem kann die Verschlüsselung auf Software- oder Hardwarebasis erfolgen. Im Gegensatz zu einer (oft frei verfügbaren) Softwareverschlüsselung, arbeiten hardwarebasierte Verschlüsselungsverfahren dabei, hinsichtlich ihrer Anwendung durch Laien, unkompliziert und verschlüsseln bereits im Moment der Datenübertragung auf das Speichermedium. Während des gesamten Verschlüsselungsvorgangs treten weder Performance- noch Zeitverluste auf. Da die hardwarebasierte Verschlüsselung außerdem betriebssystemunabhängig ist, eignet sie sich ideal für mobile Anwendungen. Ein weiterer Grund, weshalb die Hardware- der Softwareverschlüsselung vorzuziehen ist, liegt schlicht am Sicherheitsfaktor Mensch. Denn bei der Softwareverschlüsselung hängt die Sicherheit der Daten von der Komplexität und Länge des durch den Anwender vergebenen Passworts ab, welches den geheimen Schlüssel sichert.
Benutzer sitzen im Zusammenhang mit der Verschlüsselung jedoch immer wieder einem populären Irrtum auf: Sie meinen, eine Verschlüsselung ihrer Daten würde ausreichende Sicherheit vor unbefugtem Zugriff und Datenklau bieten. Doch selbst die besten Verschlüsselungsverfahren sind für Datendiebe kein echtes Hindernis, wenn keine effektive Zugriffskontrolle existiert. Denn die Vertraulichkeit von Daten auf mobilen Speichermedien, wie beispielsweise mobilen Sicherheitsfestplatten, kann nur durch eine Kombination von Zugriffskontrolle und Ver-

schlüsselung garantiert werden. Während die Verschlüsselung die Vertraulichkeit der Daten speziell bei physischen Angriffen auf den Speicher sicherstellt, werden mittels einer Zugriffskontrolle nicht authentisierte Zugriffsversuche auf den Speicher auf Hardware-Ebene geblockt.

1-Faktor-Authentisierung reicht nicht aus

Die einfachste Zugriffskontrolle erfolgt durch eine 1-Faktor-Authentisierung. Dabei bieten die Passwort- oder PIN-Eingabe über eine PC-Tastatur einen guten Basisschutz für Privatanwender. Die Zugangskontrolle per Radio Frequency Identification (RFID), per Fingerprint (biometrisches Verfahren) oder durch die PIN-Eingabe über die Tastatur des Datenträgers leisten in Kombination mit einer AES-Hardwareverschlüsselung schon deutlich mehr Zugriffsschutz, entsprechen aber als „ein-stufige" Verfahren dem aktuellen Stand der Technik noch nicht und sind für die hohen Ansprüche von Unternehmen und Behörden immer noch nicht ausreichend.

Im Hinblick auf den Schutz personenbezogener und sensibler Daten werden biometrische Verfahren zudem als durchaus kritisch betrachtet: Der Benutzer kann es kaum vermeiden, dass er biometrische Spuren hinterlässt (z.B. Fingerabdrücke), die zur Reproduktion seines biometrischen Authentisierungsmerkmals genutzt werden könnten.

Höchste Datensicherheit ist erst durch eine mehrstufige, komplexe Authentifizierung gewährleistet. Nach dem Prinzip „Besitzen und Wissen" ist etwa die Zwei-Faktor-Authentifizierung mittels Smartcard und PIN aufgebaut. Dabei stellt die PIN sicher, dass nur der berechtigte Anwender den kryptografischen Schlüssel von der Smartcard übertragen kann und Zugang zum Speichermedium erhält. Bei Verlust oder Diebstahl kann der kryptografische Schlüssel weder aus dem Sicherheitsmedium selbst noch aus dessen Gehäuse ausgelesen werden. Des Weiteren ist die Verwaltung des Krypto-Schlüssels selbst ein Sicherheitsmechanismus, der mit Blick auf höchste Datensicherheit unbedingt zu beachten ist. Wie wird der Krypto-Schlüssel erzeugt? Wo wird er aufbewahrt? Sind möglicherweise Kopien vorhanden? Wer kann wann den Verschlüsselungsschlüssel vernichten? Das sind die kritischen Fragen. Denn die stärkste Verschlüsselung mit der besten Zugriffskontrolle ist schnell geknackt, wenn der Schlüssel frei zugänglich aufbewahrt wird oder gar Unbefugte im Besitz von Zweitschlüsseln sind. Um höchsten Sicherheitsanforderungen gerecht zu werden, darf der für die Ver- und Entschlüsselung der Daten benötigte kryptografische Schlüssel weder auf der Festplatte, noch im Flash-Speicher oder im Gehäuse abgelegt werden.

Fazit

Durch die BSI-Zertifizierung oder -Zulassung entsprechender Produkte brauchen sich Anwender nicht länger auf die bloßen Behauptungen von Herstellern über das Sicherheitsniveau der von ihnen produzierten Speichermedien verlassen. Sie sollten vielmehr jegliche Lösungen für ihre Datensicherheit anhand der in diesem Artikel genannten Hauptkriterien selbst bewerten und dabei auch die Ergebnisse von Zertifizierungsprozessen mit einbeziehen. □

Der Autor

Bild: Digittrade

Robert Nutsch arbeitet seit 2019 als Direktor Business Development bei Digittrade. Seit 2002 arbeitet er durchgehend in der Speicherindustrie – sowohl bei namhaften Unternehmen als auch als selbstständiger Berater.

ALLES IM BLICK. Blitzschnell und extrem anpassungsfähig

keepbit
IT-SOLUTIONS

KEEPBIT –
IHR PARTNER FÜR

- Informationssicherheit
- IT-Lösungen
- Innovationen

www.keepbit.de/leistungen

keepbit
IT-SOLUTIONS GmbH
Brixener Straße 8
86165 Augsburg
T +49 (0) 821 450 444 0
E info@keepbit.de

Was tun, wenn es brennt? Wie Firmen nach einer Cyberattacke wieder arbeitsfähig werden

Cyberangriffe werden immer professioneller, intensiver und gefährlicher. Oft haben es die IT-Verantwortlichen in Unternehmen dabei mit einem gezielten Angriff zu tun. Nötig ist im Falle einer Infektion dann der Einsatz von Spezialisten für die Bewältigung des Cyberangriffs.

Von Kathrin-Beckert-Plewka, GDATA CyberDefense

GDATA CyberDefense ist auf Grund seiner Kompetenzen im Bereich Incident Response mit seiner hundertprozentigen Tochter GDATA Advanced Analytics vom Bundesamt in der Informationstechnik (BSI) in die Liste der qualifizierten APT-Response-Dienstleister aufgenommen worden. Der Cyber-Defense-Spezialist hat viele Unternehmen nach einer Attacke wieder arbeitsfähig gemacht.

Lange Zeit galt ein Paradigma in der IT-Sicherheit: Sicherheitsvorfälle müssen um jeden Preis verhindert werden. Dabei gibt es trotz einer gut konfigurierten IT-Security-Architektur keinen hundertprozentigen Schutz. Die Frage ist daher, was machen Unternehmen, wenn sie angegriffen wurden?

Bei Incidents sind Firmen oft auf externe Hilfe angewiesen

Tritt ein Incident, also ein Sicherheitsvorfall auf, ist die Not beim Unternehmen oft groß: Die IT-Systeme sind mit Schadcode verseucht und nicht mehr funktionstüchtig. Im schlimmsten Fall steht das Geschäft still und jede Stunde dieses Stillstandes kostet bares Geld. In der Regel können die Firmen einen Incident nicht allein bewältigen, weil das nötige Personal oder Know-how fehlt. Die Security-Experten des eingesetzten Incident Response-Teams machen das Unternehmen dann wieder so schnell wie möglich arbeitsfähig und erforschen die Gründe für die erfolgreiche Attacke, um Firmen bei der Aufarbeitung des Vorfalls zu helfen.

Um Unternehmen bei der Auswahl des richtigen APT-Response-Dienstleisters zu unterstützen, hat das Bundesamt für Sicherheit in der Informationstechnik eine Liste qualifizierter Unternehmen zusammengestellt. GDATA ist über seine hundertprozentige Tochterfirma GDATA Advanced Analytics als APT-Response-Dienstleister nach §3 des BSI-Gesetzes qualifiziert – und damit eines von derzeit nur 12 Unternehmen in Deutschland. „Die Behörde bestätigt damit unsere Kernkompetenzen im Bereich der Malware-Analyse, der IT-Forensik und im Bereich Incident Response“, erklärt

Dr. Tilman Frosch, Geschäftsführer der G DATA Advanced Analytics.


Bild: G DATA

Vorsorge ist Trumpf

Noch besser als einen guten Partner für Incident Response zu haben, ist es allerdings, sich schon vorher mit dem Thema zu befassen und Vorkehrungen zu treffen. Sinnvoll ist der frühzeitige Abschluss eines Rahmenvertrages für Security- und Incident-Response bei einem Dienstleister, also ein Retainer-Vertrag für IT-Sicherheitsdienstleistungen. Durch die Vereinbarung lassen sich feste Zeitkontingente für den Einsatz von externen Security-Experten und Absprachen für den Notfall festlegen. Die Kosten im Schadensfall sind so besser kalkulierbar. Ist ein Einsatz des Dienstleisters über den vereinbarten Rahmen hinaus nötig, sind die Tagessätze stark reduziert im Vergleich zu einer spontanen Beauftragung.

Langfristige Vorteile für Unternehmen

Zu Beginn einer Dienstleistungsvereinbarung erfolgt außerdem eine Bestandsaufnahme der IT-Systeme. So können die Security-Experten direkt konkrete Verbesserungsvorschläge unterbreiten, um für mehr IT-Sicherheit zu sorgen – und den Ernstfall möglichst zu vermeiden. Unternehmen profitieren langfristig von einem Retainer-Vertrag: Sie investieren kontinuierlich in die IT-Sicherheit und bekommen konkrete Verbesserungsvorschläge an die Hand. Der Dienstleister unterstützt hier seinen Kunden bedarfsgerecht mit seiner fachlichen Expertise – auch bei kurzfristigen Fragen.

Tritt ein Sicherheitsvorfall ein, sind die Dienstleister kurzfristig verfügbar – und innerhalb einer vorher vereinbarten Zeit einsatzbereit. Zudem kennen sie das Netzwerk und die wichtigsten Ansprechpartner bereits und können so zielgerichtet mit der Arbeit beginnen.

Umfassendes Angebot für Unternehmen in allen Cybersecurity-Lebenslagen

G DATA CyberDefense hat ein breites Portfolio an IT-Sicherheitsdienstleistungen für Unternehmen und hilft nicht nur, einen erfolgreichen Cyberangriff zu bewältigen. „Mit Security-Awareness-Trainings, Penetration-Tests und Red-Teaming bieten wir unseren Kunden umfassende Sicherheit in Ergänzung der klassischen Endpoint Security und machen sie verteidigungsfähig“, erklärt Kai Figge, Mitgründer und Vorstand von G DATA CyberDefense. □

Die Autorin

Kathrin Beckert-Plewka ist Public Relations Managerin bei der G DATA CyberDefense AG in Bochum.


Bild: G DATA

Ganzheitliche IT-Sicherheit

Für kleine und mittlere Unternehmen

- **Überall**
- **Einfach**
- **Verlässlich**

Lösungen für
Netzwerksicherheit, VPN,
E-Mail und Mobile Devices

SECUREPOINT

Gestalten Sie IT-Sicherheit aktiv mit

Securepoint ist einer der größten deutschen Hersteller von IT- Sicherheitsprodukten mit Sitz in der Metropolregion Hamburg. Mit uns können Sie viel bewegen und gemeinsam erfolgreich sein.

Wir wachsen weiterhin und benötigen Verstärkung zum nächstmöglichen Zeitpunkt:

- **Softwareentwickler Android App** (m/w/d)
- **Fachinformatiker – Systemintegration oder Anwendungsentwicklung** (m/w/d)
- **PHP-Softwareentwickler** (m/w/d)
- **DevOps Engineer** (m/w/d)

Details und alle offenen Stellenangebote finden Sie auf:
www.securepoint.de/jobs

Securepoint GmbH
Personalabteilung
Bleckeder Landstraße 28
21337 Lüneburg

Tel.: 0 41 31 / 24 01-0
Web: www.securepoint.de
E-Mail: jobs@securepoint.de

SecurITy made in Germany

Was digitale Souveränität für die Security bedeutet

Digitale Souveränität bezeichnet die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum. Möglich wird dieses erklärte Ziel für Deutschland und die EU aber nur, wenn die Cybersicherheit selbstbestimmter, eigenständiger und unabhängiger wird, denn Security ist die Grundlage der Digitalisierung. Noch ist dafür aber einiges zu tun, wie eine Bestandsaufnahme zeigt.

Von Oliver Schonschek

Der Startschuss für die Agentur für Innovation in der Cybersicherheit GmbH („Cyberagentur") im August 2020 ist ein wichtiger Schritt zu mehr Technologie-Souveränität in der Cybersicherheit, so Bundesverteidigungsministerin Annegret Kramp-Karrenbauer und Bundesinnenminister Horst Seehofer. „Kernaufgabe der Cyberagentur ist es, die Entwicklung innovativer Technologien der Cybersicherheit voranzutreiben. Wir wollen damit auch unsere digitale Souveränität stärken", so Bundesinnenminister Horst Seehofer.

Die Cyberagentur soll Innovationen auf dem Gebiet der Cybersicherheit identifizieren und konkrete Aufträge für die Entwicklung von innovativen Lösungsmöglichkeiten vergeben. Hierbei plant, steuert und priorisiert die Cyberagentur einzelne Programme und führt sie zu-

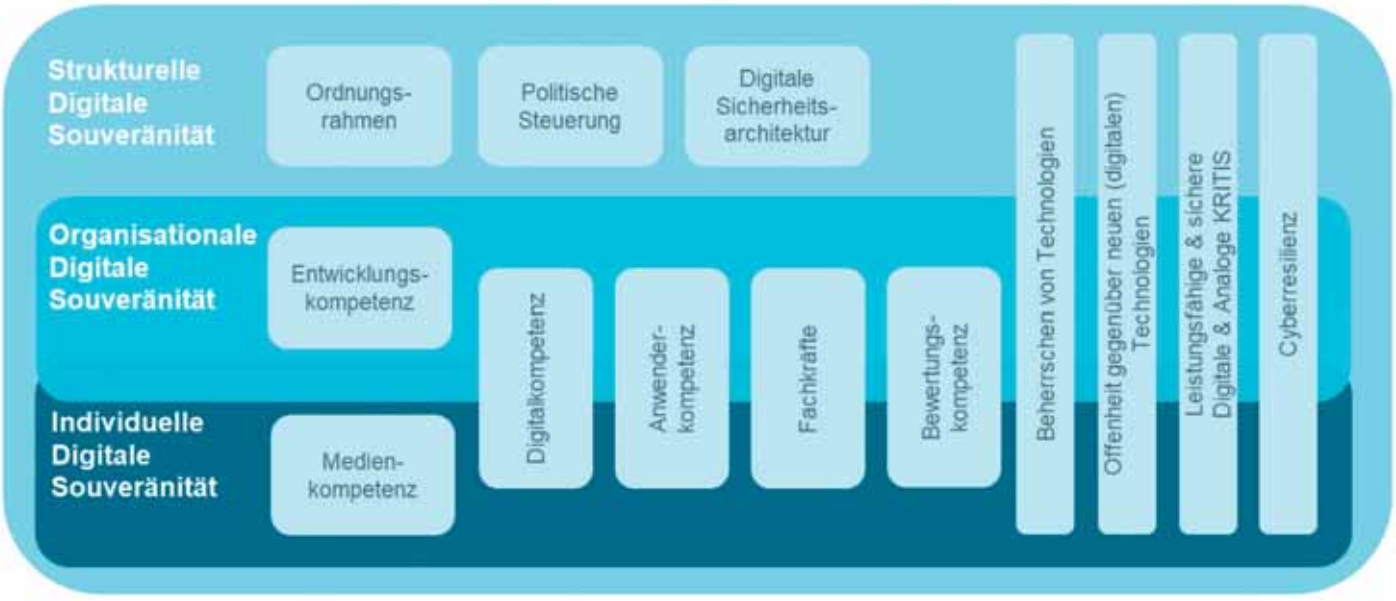


Bild: BDI

Das Ebenenmodell der digitalen Souveränität zeigt die vielschichtige Bedeutung der Cybersicherheit.

sammen. Die gewonnenen Ergebnisse wertet die Cyberagentur aus und stellt diese der Bundesregierung zur Verfügung.
Solche Maßnahmen für mehr Eigenständigkeit in der Cybersicherheit sind kein Selbstzweck, sie dienen dem Gesamtziel der Digitalisierung.

Souveränität für und durch Cybersicherheit

„IT-Sicherheit ist die notwendige Bedingung für digitale Souveränität", sagte Isabel Skierka, European School of Management and Technology, bei einer öffentlichen Anhörung des Bundestagsausschusses Digitale Agenda zum Thema „IT-Sicherheit von Hard- und Software" im Dezember 2019. Die Sachverständige plädierte dafür, Schlüsseltechnologien und Kompetenzen in Deutschland und Europa massiv zu stärken und die regulatorischen Anforderungen an IT-Sicherheit zu verbessern, deren Einhaltung die Hersteller dann nachweisen müssten.
Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Arne Schönbohm erklärte, dass technologische Souveränität eine Voraussetzung für mehr Cybersicherheit ist. „Entscheidend ist, die Soft- und Hardware getrennt zu betrachten", sagte Schönbohm. Er plädierte für einen holistischen Ansatz, der nicht nur Produkte, sondern auch Prozesse betrachtet, um Risiken zu verringern.
Offensichtlich benötigt Cybersicherheit mehr Souveränität, um dann Garant einer digitalen Souveränität sein zu können.

Souveränität bei KI und in der Cloud nur mit souveräner Security

Wie wichtig die Security zum Beispiel für die digitale Souveränität bei KI-Lösungen ist, beschreibt die Expertengruppe „Plattform Innovative Digitalisierung der Wirtschaft": Die Fähigkeit, sichere künstliche Intelligenz (KI) zu entwickeln, ist demnach elementar für die digitale Souveränität Deutschlands und Europas. Dazu gehören vertrauenswürdige Netz-Infrastrukturen, sichere Soft- und Hardware sowie Cloud- und Verschlüsselungstechnologien auf höchstem Sicherheitsniveau.
Cybersecurity unterstützt die Digitale Souveränität maßgeblich, indem die IT-Sicherheitskriterien zur Erreichung eines angemessenen Schutzniveaus bei wichtigen Entscheidungen mit einbezogen werden, so auch der VDMA (Verband Deutscher Maschinen- und Anlagenbau). Zu den Herausforderungen der Cybersecurity gehöre es, harmonisierte Produktanforderungen über Unternehmensgrenzen und Länder hinweg zu schaffen, die die gesamte Supply-Chain sowie den gesamten Produktlebenszyklus betreffen.
Auch der BDI (Bundesverband der Deutschen Industrie) unterstreicht die Bedeutung der Sicherheit für die Digitale Souveränität und erklärt: „Die Diskussionen um vertrauenswürdige 5G-Anbieter und Cloud-Provider im letzten Jahr sowie die aktuellen Auswirkungen der Corona-Pandemie verdeutlichen, dass eine erfolgreiche und sichere Digitalisierung das Beherrschen vertrauenswürdiger IT-Lösungen voraussetzt. Dafür braucht es ein sehr hohes Maß an digitaler und technologischer Resilienz. Dies ist nur möglich mit: eigenen Kompetenzen, eigenständig entwickelten Technologien sowie einem ganzheitlichen Ökosystem."
Bisher jedoch sehen IT-Experten eine zu hohe Abhängigkeit von außereuropäischen Anbietern. Gerade in der Corona-Pandemie organisieren viele Angestellte ihre Arbeits- und Abstimmungsprozesse mithilfe digitaler Tools und Technologien. Dabei setzen die Unternehmen stark auf Dienste von Anbietern außerhalb Europas. Ein Großteil der IT-Experten in Deutschland bewertet diese Abhängigkeit als zu hoch – etwa bei Endgeräten (32,3 Prozent), Bürosoftware (31,7 Prozent), Netzwerk-Software (30,9 Prozent) und verschiedenen Cloud-Services (zwischen 20,4 und 26,6 Prozent). Das zeigt eine Umfrage unter 500 IT-Experten ⇨

des Markt- und Meinungsforschungsinstitutes Civey im Auftrag des Eco – Verbands der Internetwirtschaft.

„Politik und Wirtschaft müssen die Rahmenbedingungen schaffen, um die technologische Souveränität im Cyber-Raum gestalten zu können. Wir müssen das ‚IT Security made in Germany' zu einem anerkannten Qualitätssiegel machen", so Prof. Dr. Norbert Pohlmann, Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit e.V. (TeleTrusT).

Handlungsbedarf für mehr Eigenständigkeit in der Cybersecurity

Verbände wie der Bundesverband IT-Sicherheit e.V. (TeleTrusT) und der Digitalverband Bitkom haben in Positionspapieren zur „Digitalen Souveränität" aufgezeigt, wo sie Nachholbedarf sehen, damit Deutschland und die EU unabhängiger beim Handeln und Entscheiden im digitalen Raum und damit auch in der Cybersicherheit werden.

Der Digitalverband Bitkom nennt als Maßnahmen für mehr digitale Souveränität vor allem:

- Förderung von innovativen Technologien im Kontext der Sicherheit von Geräten, Infrastrukturen und Systemen, wie z. B. Verschlüsselungsalternativen zur Post-Quanten-Kryptographie sowie der Künstlichen Intelligenz zum Schutz von Netzwerken.
- Sicherstellung vertrauenswürdiger Wertschöpfungsketten für Kritische Infrastrukturen, die nach dem IT-Sicherheitsgesetz in Deutschland bzw. der NIS-Richtlinie oder dem Cybersecurity Act auf europäischer Ebene definiert sind.
- Sicherstellung vertrauenswürdiger Elektronik in Europa und Deutschland, um beispielsweise mögliche Backdoor-Funktionen in Importen auszuschalten.
- Bereitstellung der Kompetenz zur Identifikation, Spezifikation und Standardisierung der Architektur, der austauschbaren Kernkomponenten (Hard-/Software-Module) und der Schnittstellen zur Sicherstellung der technischen Kontrollhoheit über das System sowie Bereitstellung der Kompetenzen zur Zertifizierung sowohl auf Systemebene als auch auf Chipebene.
- Kompetenzen bestmöglich zur Schaffung und Aufrechterhaltung hinreichend verlässlicher Systeme und Technologien erhalten, anwenden und ausbauen.

Die Mehrheit der deutschen Unternehmen sind überzeugt: Digitale Souveränität sichert den Wirtschaftsstandort Deutschland.

Wenn also Deutschland gegenwärtig im Rahmen der EU-Ratspräsidentschaft die Digitale Souveränität als eines der Hauptziele ausgegeben hat, sollten Weichenstellungen für eine unabhängigere und eigenständigere Cybersicherheit in der EU nicht fehlen. Nur eine möglichst unabhängige Cybersicherheit kann die Grundlage selbstbestimmten Handelns und Entscheidens im digitalen Raum sein. □

Embrace Datacenter Technologies

Georg Gesek
Novarion Systems

»Quanteninformationstechnologie & Künstliche Intelligenz in Cloud & Edge«

Dr. Markus Pleier
Nutanix Germany

»5G als Basis für Cognitive IT – Edge Cloud als die nächste Herausforderung«

Dr. Thomas King
DE-CIX Management

»Internetknoten nah am Edge – ein neues Geschäftsmodell für Rechenzentren?«

Tor Björn Minde
Research Institute of Sweden

»Use of ML modeling and large-scale experiments to optimize performance of datacenters«

Dr. Ralph Hintemann
NeRZ

»Rechenzentren und Cloud Computing in Europa - effizient, nachhaltig, wettbewerbsfähig?

Eine Veranstaltung der
VOGEL IT AKADEMIE

DC DATACENTER DAY 2020

6. Oktober 2020 | VCC Würzburg

VIP-Ticket sichern:
» dc-day.de/vip

PREMIUM-PARTNER

Life Is On APC by Schneider Electric CORNING EATON Powering Business Worldwide FUJITSU

CLASSIC-PARTNER

Swegon LOGICALIS Business and technology working as one sachsenkabel

CLASSIC-PARTNER

VERTIV.

BASIC-PARTNER

ARROW AMD SUPERMICRO SDC SpaceNet Datacenter Telemaxx

MEDIEN- & TECHNOLOGIE-PARTNER

IT-BUSINESS CLOUDCOMPUTING INSIDER DATACENTER INSIDER VIRZ

Mit Mobile Security Hackern das Leben erschweren

Benötige ich eine App, um meine E-Mails von unterwegs abzurufen, meine Bankgeschäfte zu tätigen oder einfach, um online zu shoppen: Der App-Store – ob für Android oder iPhone – bietet eine umfassende Auswahl. Die App wird einfach installiert, den Datenschutzrichtlinien wird zugestimmt und schon kann es losgehen. Ob die Applikation wirklich sicher und gegen Cyberangriffe geschützt ist, erfährt der Nutzer erst dann, wenn es schon zu spät ist.

Von Torsten Leibner, Head of Product Management and Technology & Co-Founder von Build38 GmbH.

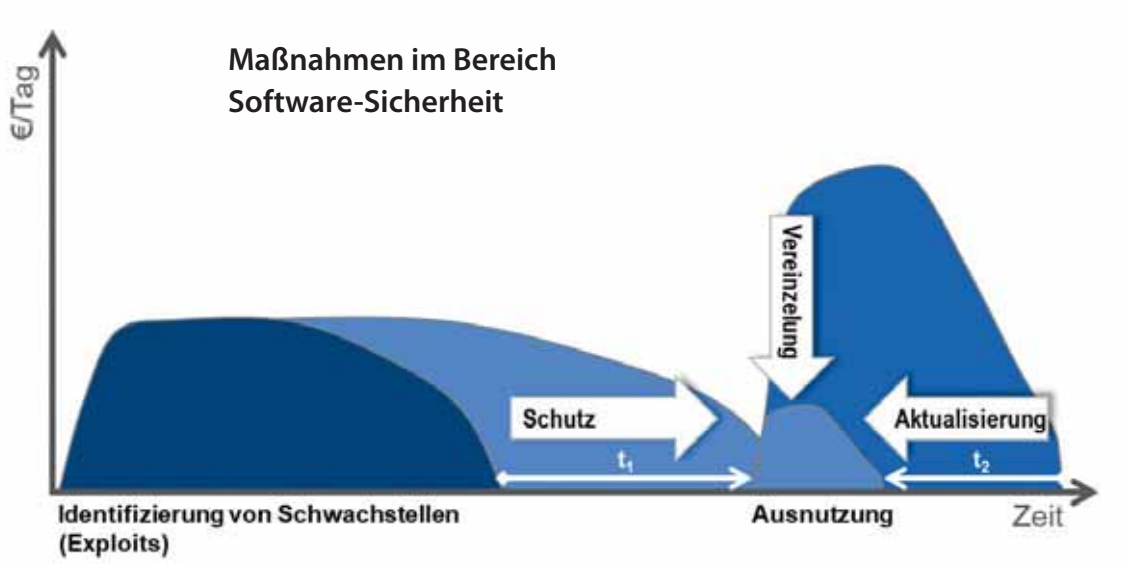
Um es nicht so weit kommen zu lassen und Daten sowie die Kommunikation stets zu schützen, muss das Thema Sicherheit bereits in der Entwicklung der Anwendung umfassend berücksichtigt werden. Dabei müssen diverse Faktoren berücksichtigt werden, um eine App sicher für alle Endgeräte bereitstellen zu können.

Ob für private oder berufliche Zwecke: Smartphones und Tablets werden täglich in den verschiedensten Situationen genutzt. Daher stellen branchenübergreifend Unternehmen ihren Kunden und Mitarbeitern mobile Anwendungen zur Verfügung, um einen umfassenden Service zu bieten und die Kommunikation möglichst einfach zu gestalten. Doch nicht nur Unternehmen reagieren auf die verstärkte Nutzung mobiler Geräte und Apps. Auch Cyberkriminelle setzen sich vermehrt zum Ziel, mit immer ausgefeilteren Techniken Zugriff auf diese Geräte zu erlangen, um persönliche und berufliche Daten abzugreifen.

Die Ziele von Software-Sicherheit

Je länger ein Angreifer benötigt, ein Ziel zu hacken, umso weniger wirtschaftlich wird es für ihn. Software-Sicherheit soll ihm daher letztlich das Leben erschweren und potenzielle Ziele so unattraktiv wie möglich machen.

Durch einen erweiterten Schutz sind Cyberkriminelle gezwungen, mehr Geld für Tools und Unterstützung auszugeben oder diese gegebenenfalls sogar selbst zu entwickeln. Denn hat er – bildlich gesprochen – die erste Tür geöffnet, sieht er sich drei neuen Türen gegenüber, die er untersuchen muss. Und erhält eine mobile Anwendung regelmäßig Updates, muss der Angreifer jedes Mal von vorne beginnen.



Das Ziel von Software-Sicherheit ist also die Minimierung der Industrialisierung, den Angriff möglichst zu einem „Einzelfall“ zu machen und die zeitliche Wirkung von Angriffen zu verkürzen (siehe Abbildung Pfeil t2). Darüber hinaus sollte eines der Hauptziele sein, den Zugang zum Unternehmensnetz abzusichern.

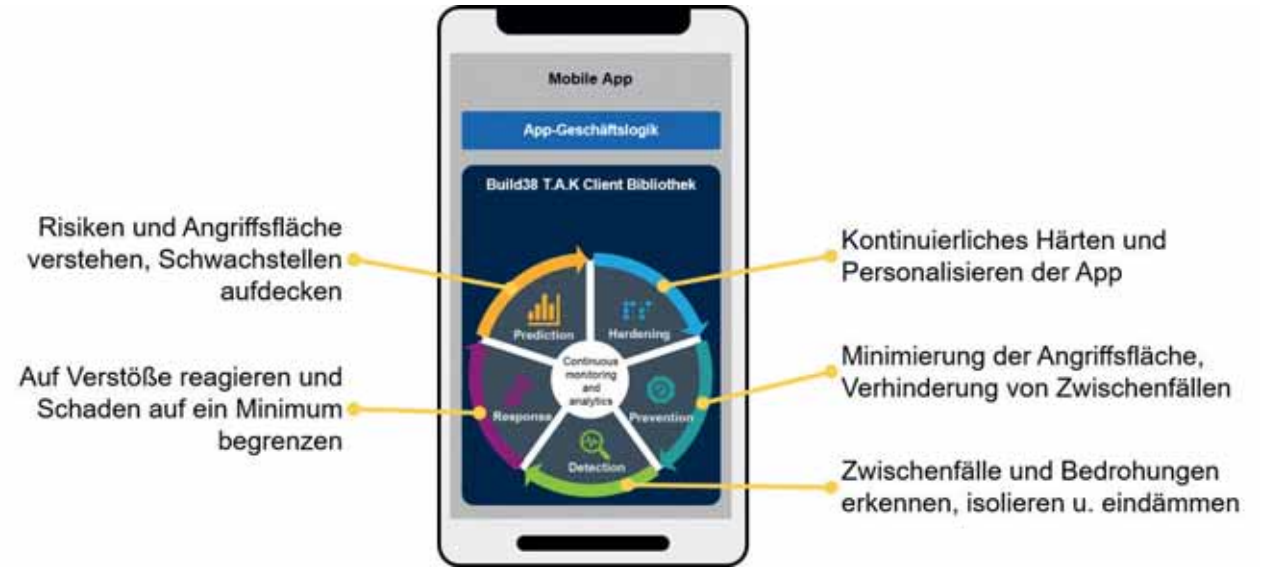
App-Sicherheit einfach integrieren

Während 2019 rund 204 Milliarden Apps aus den App-Stores heruntergeladen wurden, dürfte die Anzahl der Downloads bis 2022 auf rund 259 Milliarden pro Jahr ansteigen. Die Anzahl der Mitbewerber ist groß, daher wird auch Entwicklern immer klarer, dass Vertrauen ein zentraler Aspekt ist, um Kunden zu gewinnen und langfristig an sich zu binden. Denn um sie wirklich zu überzeugen, müssen Entwickler sichere und komfortable Apps bereitstellen.

Angemessene Sicherheitskonzepte erfordern eine breite Palette an Funktionen, die jeder Entwickler von (nativen) Apps implementieren muss. Neben erfahrenen Spezialisten benötigt die Integration dieser Sicherheitsfunktionen vor allem auch Zeit. Um die Mobile Security in der Entwicklung auf schnellem Weg zu realisieren, gibt es inzwischen separate Lösungskits in Form von mobilen Sicherheits-Frameworks. Indem diese eine unbefugte Analyse, Manipulation, Vervielfältigung und Nutzung der sicherheitsrelevantesten Teile einer App verhindern, unterbinden sie zugleich den Zugriff auf sensible Benutzerinformationen.

Auch Entwickler ohne spezifische Fachkenntnisse oder jahrelange Erfahrung können diese Kits einfach und schnell bereits während der Entwicklungsphase implementieren.

Das Build38 „T.A.K Insights Portal“, das Security- und Compliance-Teams des App-Publishers einen Überblick über den Gesundheitszustand und erfolgte Angriffe der App im Feld gibt.



Der Build38 T.A.K Client (als Sicherheitsmodul in der Android oder iOS App) mit einer High-Level-Beschreibung der Cybersecurity-Funktionen.

Dadurch sind Unternehmen nicht gezwungen, externe Spezialisten mit dem Projekt zu beauftragen. Diese sind rar auf dem Markt, was das Projekt und somit den Launch der App deutlich verzögern kann. Wurde ein externer Entwickler gefunden und hat er die Lösung programmiert, verlässt er das Unternehmen wieder – und nimmt natürlich sein Know-how mit. Benötigen Security-Features der App dann zukünftig ein Update, um Sicherheitslücken vorzubeugen oder zu schließen und so schwerwiegende Reputationsschäden des Unternehmens zu vermeiden, muss der externe Entwickler erneut beauftragt werden.

Durch ein Software-Kit lassen sich daher langfristig Folgekosten sparen, da dieses flexibel angepasst und zum Beispiel durch Managed Services des Anbieters jederzeit auf dem aktuellsten Stand gehalten wird.

Solche Lösungen lassen sich eigenständig oder zusammen mit anderen Sicherheitstechnologien einsetzen und können darüber hinaus die Nutzung anderer Technologien sicherer machen.

Da die Funktionen bereits als Baustein in die App integriert werden, bedeutet dies für den Anwender in der täglichen Nutzung: Er verwendet eine sichere Applikation, ohne es zu merken. ■

Build38 mit Hauptsitz in Deutschland ist ein führender Anbieter von App-Sicherheits- und Bedrohungsschutz-Lösungen für Smartphones. Das Softwareunternehmen bietet ein SDK an, das es allen App-Entwicklern ermöglicht, die Sicherheitsfunktionen von Build38 mit minimalem Aufwand in die App zu integrieren. Das Ziel der Lösung besteht darin, es Hackern und anderen Black-Hats nahezu unmöglich zu machen, auf App-Daten jeglicher Art zuzugreifen. Apps, die diese Technologien enthalten, können auch als „Self-Defending Apps“ bezeichnet werden.

Braucht die Security KI-Dienste aus den USA?

Künstliche Intelligenz soll dabei helfen, Security-Prozesse zu optimieren und Security-Analysten zu entlasten. Viele KI-Services stammen aber aus den USA. Werden personenbezogene Daten verarbeitet, müssen die Rechtsgrundlagen geklärt oder Alternativen aus der EU genutzt werden. Doch ist das bereits möglich? Gibt es schon KI-Alternativen für die Security aus Europa? Von Oliver Schonschek

Künstliche Intelligenz (KI) ist schon heute unterstützender Bestandteil vieler IT-Sicherheitsanwendungen und Abwehrstrategien. Dazu zählen etwa die Erkennung von Schadsoftware, von Anomalien im Netzwerkverkehr und von Angriffen auf biometrische Identifikationssysteme, so das Bundesamt für Sicherheit in der Informationstechnik (BSI).

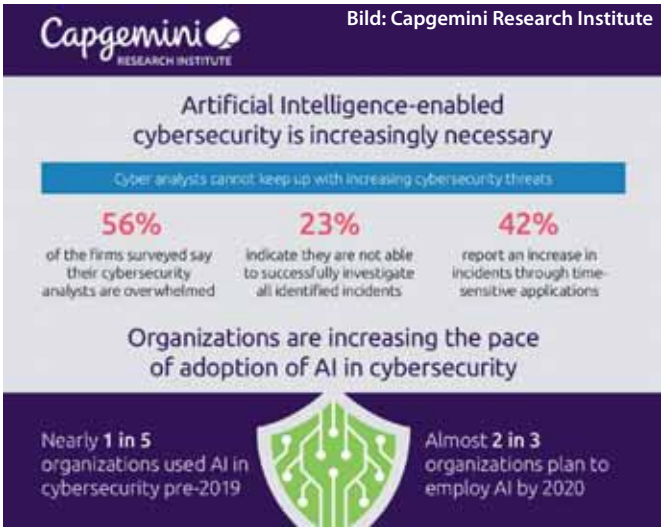


Bild: Capgemini Research Institute

Künstliche Intelligenz (Artificial Intelligence) hat bereits eine große Bedeutung in der Security erlangt.

Dabei ist KI für die Cybersicherheit zunehmend Pflicht und nicht Kür: Unternehmen halten es für zunehmend notwendig, die Cybersicherheit mit KI zu stärken – fast zwei Drittel glauben nicht, dass sie kritische Bedrohungen ohne KI identifizieren können, so die Studie „Reinventing Cybersecurity with Artificial Intelligence“ des Capgemini Research Institute.

Das Tempo der Einführung von KI in der Cybersicherheit steigt demnach, fast drei Viertel der Unternehmen testen KI in Anwendungsfällen der Cybersicherheit. Es gibt zudem einen starken Geschäftsnutzen für den Einsatz von KI in der Cybersicherheit: Drei von fünf Unternehmen sagen, dass der Einsatz von KI die Präzision und Effizienz der Cyberanalysten erhöht.

Große KI-Player kommen häufig aus den USA und Fernost

Der erfolgreiche Beitrag der KI zur Cybersicherheit hängt natürlich auch davon ab, welche KI-Lösung zum Einsatz kommt, also welche Algorithmen von welchem Anbieter, und mit welchen Trainingsdaten die KI angelernt wurde. ⇨

↪ Unter den KI-Anbietern dominieren bisher Unternehmen aus den USA und aus Asien. Da viele KI-Dienste aus der Cloud bezogen werden, spielen besonders die großen Public-Cloud-Provider eine zentrale Rolle. Auch KI-Dienste für die Security bekommt man aus der Cloud.
Bedenkt man aber, dass die Trainingsdaten und späteren Nutzungs- und Telemetriedaten, die die KI analysieren soll, um sicherheitsrelevante Informationen zu erzielen, personenbezogen oder personenbeziehbar sein können, stellt sich die Frage nach dem Datenschutzniveau des KI-Dienstes. Mit dem Aus für Privacy Shield als mögliche Rechtsgrundlage einer Datenübermittlung in die USA muss die Nutzung von KI-Cloud-Diensten aus den USA eine andere Rechtsgrundlage finden. Oder aber man nutzt KI-Dienste, die innerhalb der EU betrieben werden und keinen Zugriffen aus Drittstaaten unterliegen.

Was der Datenschutz zu KI-Diensten sagt

In den Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen der Datenschutzaufsichtsbehörden in Deutschland finden sich eine Reihe von Vorgaben an KI-Dienste aus der Cloud, die auch für KI-Dienste in der Security gelten:

- Man muss klären, welche Zugriffsmöglichkeiten der Cloud-Betreiber auf die Trainingsdaten und auf die Outputs und Zwischenergebnisse hat und wie diese organisatorisch geregelt sind.
- Ist die Möglichkeit der Kenntnisnahme der personenbezogenen Daten durch den Cloud-Betreiber zu risikobelastet für die Rechte und Freiheiten der betroffenen Person, so könnte eine Risikobetrachtung (bzw. die Datenschutzfolgenabschätzung) zum Ergebnis haben, dass das Training auf Geräten des Anwenderunternehmens durchgeführt werden muss. Wird das Training in einem Cloud-Bereich durchgeführt, müssen die Trainingsdaten, Testdaten und Verifikationsdaten auf verschlüsseltem Weg in diesen Bereich transportiert werden.
- Mit fortschreitender Technik ist zu erwarten, dass KI vermehrt auf lokalen oder gar mobilen Geräten direkt ausgeführt wird, statt die Verarbeitung in einer Cloud durchzuführen. Wann immer diese Möglichkeit besteht, sollte hiervon Gebrauch gemacht werden.

Mit dem Ende des Privacy Shields kann bei Cloud-basierten KI-Diensten deutlicher Handlungsbedarf bestehen. Zum Beispiel forderte die Berliner Beauftragte für Datenschutz und Informationsfreiheit sämtliche ihrer Aufsicht unterliegenden Verantwortlichen auf, die Entscheidung des Europäischen Gerichtshofs (EuGH) zur Ungültigkeit von Privacy Shield zu beachten. Verantwortliche, die – insbesondere bei der Nutzung von Cloud-Diensten – personenbezogene Daten in die USA übermitteln, seien nun angehalten, umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln.
Doch gibt es denn Alternativen zu KI-Diensten aus US-Clouds oder aus anderen Drittstaaten, die in der Security eingesetzt werden können? Die Antwort: Ja, die gibt es, wie die folgenden Beispiele zeigen.

KI-basierte Security made in Germany

Wer im Sinne der digitalen Souveränität von Deutschland und der EU zu hiesigen KI-Lösungen im Bereich Security greifen möchte oder keine Rechtsgrundlage findet, die der Datenschutz-Grundverordnung (DSGVO) genügt, um KI-Cloud-Dienste aus Drittstaaten zu nutzen, der muss auf Künstliche Intelligenz in der Cybersicherheit nicht verzichten, ganz im Gegenteil.
Sowohl auf Seiten der Forschung als auch in bereits auf dem Markt verfügbaren Security-

KI-Lösungen für Cybersecurity-Aufgaben gibt es auch aus Deutschland, wie DeepRay in den G DATA-Businesslösungen gegen trickreich verschleierte Schaddateien.

Lösungen werden KI-Lösungen entwickelt und betrieben, die aus Deutschland oder der EU stammen. So forscht das Deutsche Forschungszentrum für Künstliche Intelligenz an mehreren Projekten, die mit KI in der Security in Verbindung stehen.

Ebenso führt der KI-Bundesverband mehrere Mitglieder und Startups auf, die Künstliche Intelligenz in der Security zum Einsatz bringen. Nicht zuletzt setzen Security-Anbieter aus Deutschland und der EU auch eigene KI-Lösungen ein, um Security-Funktionen zu optimieren und Security-Analysten zu entlasten, darunter

- Link11 mit KI-unterstütztem Schutz für Netzwerke und Websites gegen DDoS-Attacken,
- Avira mit der Protection Cloud zur Erkennung und Abwehr moderner Malware,
- G DATA mit der DeepRay-Technologie gegen intelligente Cyberattacken,
- DriveLock mit Application Whitelisting basierend auf künstlicher Intelligenz als Cloud-basierte KI und auch On-Premises-KI auf Agentenebene,
- genua mit Threat Defender für intelligenten Netzwerkschutz.

KI und Security leben jedoch vom internationalen Austausch

Auch bei KI-Lösungen für die Security aus Deutschland und der EU stehen aber immer internationale Standards und Verfahren im Mittelpunkt. Es geht nicht um Abkapselung, sondern um Kontrolle und Transparenz bei KI-Algorithmen und der Datenverarbeitung.

Beim Thema Cybersicherheit ist eine stärkere internationale Zusammenarbeit geboten. Denn die Exportnation Deutschland ist auf weltweit anerkannte Standards und Regeln angewiesen, erklärt auch der BDI (Bundesverband der Deutschen Industrie e.V.). Dabei ist Zusammenarbeit und Souveränität bei Cybersicherheit und KI kein Widerspruch. Letztlich kann die internationale Zusammenarbeit nur davon profitieren, wenn es viele, eigenständige Wege gibt, wie KI die Security weiter unterstützen kann. Durch Vielfalt wird weiterer Fortschritt in der intelligenten Security letztlich erst möglich. □

Impressum

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

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

Abonnementbetreuung: Petra Hecht, DataM-Services GmbH, 97103 Würzburg
Tel. 0931/4170-429 (Fax -497)
eMail phecht@datam-services.de

Geschäftsführer: Werner Nieberle – Geschäftsführer/Publisher

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, IP-Insider, Security-Insider, Storage-Insider, Cloud-Insider, DataCenter-Insider, Dev-Insider, BigData-Insider** und **Blockchain-Insider**.

Inserenten

Achelos GmbH	Paderborn	https://www.achelos.de/de/	8, 9
Bank-Verlag GmbH	Köln	https://www.bank-verlag.de/	38, 39
Beta Systems IAM Software AG	Berlin	https://www.betasystems-iam.com/de/	31
Build38 GmbH	München	https://build38.com/	68, 69, 70
G DATA Software AG	Bochum	https://www.gdata.de/	2, 32, 33
keepbit IT-SOLUTIONS GmbH	Augsburg	https://www.keepbit.de/	58, 59
NCP engineering GmbH	Nürnberg	https://www.ncp-e.com/de/	12, 13, 44, 45, 76
Net at Work GmbH	Paderborn	https://www.netatwork.de	48, 49
netfiles GmbH	Burghausen	https://www.netfiles.de/	75
PSW GROUP GmbH & Co. KG	Fulda	https://www.psw-group.de/	52, 53
retarus GmbH	München	https://www.retarus.com/de/	16, 17
secunet Security Networks AG	Essen	https://www.secunet.com/	5, 21
Securepoint GmbH	Lüneburg	https://www.securepoint.de/	62, 63
SoSafe GmbH	Köln	https://sosafe.de/	22, 23
TDT AG	Essenbach	https://tdt.de/de/	26, 27
ucs datacenter GmbH	Mönchengladbach	https://www.ucs.cloud/	44, 45
Vogel IT-Akademie	Augsburg	http://www.akademie.vogel-it.com/	67

NETFILES

Virtueller Datenraum

Sicherer und Compliance-gerechter Datenaustausch mit Kunden und Geschäftspartnern

Einfach

Der netfiles Datenraum ist besonders einfach zu bedienen, bietet umfangreiche Funktionalität und steht Ihnen sofort, ohne Installation von Software oder Plugins zur Verfügung. Ein Webbrowser genügt.

Sicher

Im netfiles Datenraum sind Ihre Daten sowohl bei der Speicherung als auch Übertragung durch 256-bit Verschlüsselung sicher und Compliance-gerecht geschützt.

Bewährt

netfiles gibt es seit mehr als 15 Jahren. Profitieren auch Sie von unserer langjährigen Erfahrung und dem zuverlässigen Betrieb. Wir sind ein deutsches Unternehmen und hosten ausschließlich in Deutschland.

www.netfiles.de

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

NCP
SECURE COMMUNICATIONS

Back to the future

Jetzt mit starkem Enterprise VPN für die veränderte Arbeitswelt rüsten!

Bleiben Sie jederzeit arbeitsfähig mit produktiven Mitarbeitern im Home-Office oder unterwegs von jedem Internetzugang aus.

Bauen Sie schnell und flexibel VPN Kapazitäten für tausende Anwender auf – sicher, skalierbar und universell.

NCP SECURE COMMUNICATIONS my access

www.ncp-e.com/en/bc

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