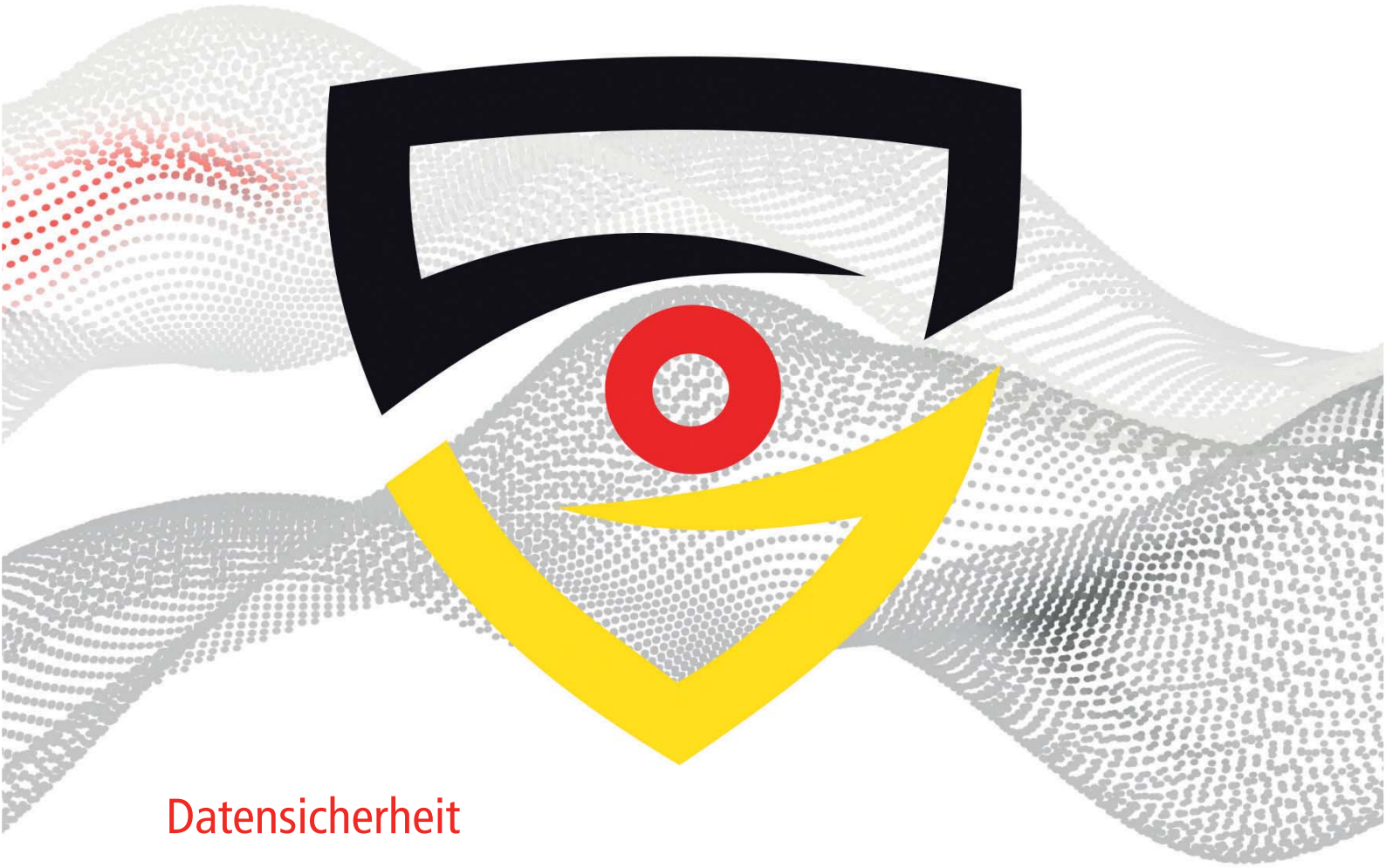
OKTOBER 2018

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

MADE IN GERMANY



Datensicherheit

Endpoint Security APT

Backdoor Data Leakage

Compliance Verschlüsselung

Patch Management

Powered by:

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

VOGEL IT MEDIEN

Eine Publikation von IT-BUSINESS Security Insider

Wir lieben Langzeitbeziehungen.

gdata.de/partner-werden

it sa 2018
Die IT-Security Messe und Kongress
Besuchen Sie uns: Halle 9, Stand 438

Das G DATA Partnerprogramm: Sagen Sie ja, wir meinen es ernst.

Stabile Beziehungen halten ein Leben lang. Vertrauen und Kontinuität sind auch in einer **G DATA Partnerschaft** die Basis, auf der wir mit Ihnen arbeiten. Bei uns finden Sie garantiert Ihren Platz, besten Virenschutz, viele lukrative Vorteile und kompromisslose IT-Sicherheit. Bereits 2011 unterzeichneten wir eine TeleTrusT-Selbstverpflichtung. Das Ergebnis: unsere No-Backdoor-Garantie.

G DATA
TRUST IN GERMAN SICHERHEIT

„Security by Design“ – jetzt und überall!

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

Liebe Leserinnen und Leser,
ob Autos oder Küchenmaschinen: Viele Gegenstände des Alltags sind heute vernetzt, die Digitalisierung durchdringt damit nahezu alle Lebensbereiche. Die Leitkonzepte „Security by Design“ und „Security by Default“ sollten daher schon bei der Planung von Produkten ein fester Bestandteil sein. Leider sieht die Realität oftmals anders aus.

Gravierende Auswirkungen kann dies bei der Automatisierung, Digitalisierung und Vernetzung von Produktionsanlagen (Industrie 4.0) haben. Um hier ein hohes und gleichartiges IT-Sicherheitsniveau sicherzustellen, hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) mit seiner Arbeitsgruppe „Smart Grids/Industrial Security“ ein Prüfschema nach IEC 62443-4-2 „Industrielle Kommunikationsnetze – IT-Sicherheit für industrielle Automatisierungssysteme“ veröffentlicht. IT-Sicherheit im Umfeld der Automatisierungstechnik soll damit auch von Produkten, die von unterschiedlichen Prüfstellen zertifiziert wurden, vergleichbar werden. In diesem Zusammenhang sei auch auf die TeleTrusT-Handreichung „Stand der Technik“ hingewiesen. Neben der produzierenden Wirtschaft sind ebenso die Verwaltung sowie private Anwender mehr denn je auf sichere und vertrauenswürdige Informationsinfrastrukturen angewiesen. Der Staat ist hier in der Pflicht, IT-Sicherheit als gesamtgesellschaftliche Aufgabe zu begreifen. Bekannte Sicherheitslücken müssen schnellstmöglich den Herstellern gemeldet werden. Andernfalls lässt man Cyberkriminellen oder interessierten fremden Diensten die Tür offenstehen.

Die IT-Sicherheitsbranche in Deutschland stellt sich mit ihren Experten den gegenwärtigen und kommenden Herausforderungen. Den KMU kommt hier besondere Bedeutung zu, da sie in Deutschland insbesondere in der IT-Sicherheitswirtschaft eine bedeutende Stellung bei Produkten, Know-how, Wirtschaftskraft und Arbeitsplätzen einnehmen. „IT Security made in Germany“ ist Qualitätsmerkmal und ein schlagendes Verkaufsargument und strahlt dabei weit über die Landesgrenzen hinaus.

Diese Sonderpublikation informiert Sie über Lösungen, die deutsche Unternehmen im Bereich IT-Sicherheit entwickelt haben. Gemeinsam mit den TeleTrusT-Mitgliedern wünsche ich Ihnen eine informative Lektüre und hoffe, dass Sie zahlreiche Anregungen erhalten, um die IT-Sicherheit in Ihrem Unternehmen, in Ihrer Behörde und auch in Ihrem privaten Umfeld weiter zu stärken. □

Titelbild: © barani83 - stock.adobe.com (M) Carin Boehm

TeleTrusT-Initiative „IT Security made in Germany“

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

Trust Seal
www.teletrust.de/itsmig

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

Stabilität kommt von Architektur: Netzwerksicherheit mit SINA.

Wer täglich mit vertraulichen Daten arbeiten muss, braucht eine ganzheitliche Lösung für eine sichere Netzwerk-Architektur: SINA von secunet. Anders als bei einem Flickwerk aus schlecht harmonisierenden Einzelkomponenten administrieren Sie mit SINA alle Bausteine über ein zentrales Management. Mit SINA werden Sicherheit und Komfort zu einer Einheit. Dazu besitzt SINA mit die höchsten Zulassungen durch BSI, EU und NATO und ist ohne Grenzen skalierbar für Arbeitsumgebungen bis hin zu mehreren Tausend Arbeitsplätzen.

IT-Sicherheit „Made in Germany“.
www.secunet.com/sina

secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

Vertrauen hat einen Namen

Mit der Vergabe des Vertrauenszeichens „IT Security made in Germany" an deutsche Anbieter erleichtert der TeleTrusT – Bundesverband IT-Sicherheit e.V. 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 21.9.2018)

- 1984not Security GmbH
- 8ack GmbH
- abl social federation GmbH
- Accellence Technologies 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
- aumass GmbH & Co. KG
- Avira GmbH & Co. KG
- Backes SRT GmbH
- BCC Unternehmensberatung GmbH
- bc digital GmbH
- Bechtle GmbH & Co. KG
- befine Solutions AG
- Beta Systems IAM Software AG
- Biteno GmbH
- Blue Frost Security GmbH
- bowbridge Software GmbH
- Brabbler Secure Message and Data Exchange AG
- Brainloop AG
- Bundesdruckerei GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- certgate GmbH
- CGM Deutschland AG
- CHIFFRY GmbH
- Cloud Identity and Access Management (C-IAM)
- cloudTEC GmbH
- CoCoNet Computer-Communication Networks GmbH
- Cognitec Systems GmbH
- cognitix GmbH
- COMback Holding GmbH
- comcrypto GmbH
- commocial GmbH
- Condition-ALPHA Digital Broadcast Technology Consulting
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- CONTURN Analytical Intelligence Group GmbH
- Crashtest Security GmbH
- CryptoMagic GmbH
- CryptoTec AG
- CSO GmbH
- cv cryptovision GmbH
- CYPP GmbH
- dacoso data communication solutions GmbH
- dal33t GmbH
- Daniel Aßmann – Datenschutz & QM
- DATAKOM GmbH
- DATUS AG
- DERMALOG Identification Systems GmbH
- Detack GmbH
- DeviceLock Europe GmbH
- dhpg IT-Services GmbH Wirtschaftsprüfungsgesellschaft
- DFN-CERT Services GmbH
- digitalDefense Information Systems GmbH
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- ditis Systeme Niederlassung der JMV GmbH & Co.
- DocRAID – professional data privacy protection
- DoctorBox GmbH
- DriveLock SE
- e-ito Technology Services GmbH
- eBlocker GmbH
- ecsec GmbH
- Elaborated Networks GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- exceet Secure Solutions AG
- Fiducia & GAD IT AG
- floragunn GmbH
- FSP GmbH
- FZI Forschungszentrum Informatik
- G DATA Software AG
- GBIT Consulting UG
- GBS Europa GmbH
- genua GmbH
- Giegerich & Partner GmbH
- Glück & Kanja Consulting AG
- grouptime GmbH
- GZIS GmbH
- HiScout GmbH
- HOB GmbH & Co. KG
- Hornetsecurity 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/ □

- Huf Secure Mobile GmbH
- ifAsec GmbH
- if(is) – Institut für Internet-Sicherheit
- Infineon Technologies AG
- INFODAS GmbH
- Inlab Networks GmbH
- innovaphone AG
- isits AG International School of IT Security
- ITConcepts Professional GmbH
- IT-Sitter GmbH Deutschland
- ISL Internet Sicherheitslösungen GmbH
- itWatch GmbH
- keepbit SOLUTION GmbH
- KeyIdentity GmbH
- Keyp GmbH
- KikuSema GmbH
- KIWI.KI GmbH
- KORAMIS GmbH
- LANCOM Systems GmbH
- limes datentechnik gmbh
- Link11 GmbH
- Linogate GmbH
- maincubes one GmbH
- MaskTech GmbH
- MATESO GmbH
- MB Connect Line GmbH Fernwartungssysteme
- Mentana Claimsoft GmbH
- metafinanz Informationssysteme GmbH
- M&H IT-Security GmbH
- MTG AG
- NETZWERK Software GmbH
- NCP engineering GmbH
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- Nexis GmbH
- nicos AG
- Nimbus Technologieberatung GmbH
- OctoGate IT Security Systems GmbH
- OTARIS Interactive Services GmbH
- P-ACS UG
- PfalzKom, Gesellschaft für Telekommunikation mbH
- PHOENIX CONTACT Cyber Security AG
- Pix Software GmbH
- PPI Cyber GmbH
- PRESENSE Technologies GmbH
- procilon IT-Solutions GmbH
- PROSTEP AG
- Protforce GmbH
- PSW GROUP GmbH & Co. KG
- Pyramid Computer GmbH
- QGroup GmbH
- QiTEC GmbH
- QuoScient GmbH
- ReddFort Software GmbH
- RED Medical Systems GmbH
- retarus GmbH
- Rhebo GmbH
- Rohde & Schwarz Cybersecurity GmbH
- r-tec IT Security GmbH
- sayTEC AG
- SAMA PARTNERS Business Solutions GmbH
- SC-Networks GmbH
- Secomba GmbH
- secrypt GmbH
- secucloud GmbH
- SECUDOS GmbH
- secunet Security Networks AG
- Securepoint GmbH
- Sengi GmbH
- SerNet GmbH
- signotec GmbH
- Softline AG
- Steen Harbach AG
- Steganos Software GmbH
- syracom consulting AG
- sys4 AG
- TDT AG
- TESIS SYSware Software Entwicklung GmbH
- THREATINT GmbH & Co. KG
- TÜV Informationstechnik GmbH
- Uniki GmbH
- Uniscon GmbH
- Utimaco IS GmbH
- valvisio consulting GmbH
- VegaSystems GmbH & Co. KG
- virtual solution AG
- WhosApp GmbH
- WMC Wüpper Management Consulting GmbH
- Würzburger Versorgungs- und Verkehrs GmbH
- ZenGuard GmbH
- Zertificon Solutions GmbH

Sicherer Datenaustausch im virtuellen Datenraum

Daten gehören zu den wertvollsten Ressourcen eines Unternehmens – deren reger Austausch mit Geschäftspartnern, Kunden und Kollegen zum Arbeitsalltag. Virtuelle Datenräume stellen heute eine hochsichere und einfach zu bedienende Lösung für den standort- und unternehmensübergreifenden Datenaustausch dar.

NETFILES

Virtueller Datenraum – Höchstmaß an Sicherheit

Sicherheit, Zuverlässigkeit und Kontrolle – Stichworte, die beim Austausch von vertraulichen Unternehmensdaten oberste Priorität haben. Täglich müssen zahlreiche Dokumente wie z.B. Vertrags-, Finanz- und Projektunterlagen, Konstruktionszeichnungen oder Grafiken unternehmensübergreifend ausgetauscht werden – per E-Mail, über FTP oder die Cloud. Häufige Folgen: Probleme beim E-Mail-Versand mit Anhängen, kompliziert zu bedienende Software, Kontrollverlust über den aktuellen Stand einer Dokumentversion, Datendiebstahl oder gar Wirtschaftsspionage schädigen das Geschäft.

Virtuelle Datenräume schließen diese essentielle Sicherheitslücke. Unternehmen können mit dieser Lösung ihre sensiblen Daten und umfangreichen Projektunterlagen mit einem Höchstmaß an Sicherheit und Effizienz online austauschen und bereitstellen. Dabei kontrollieren und steuern sie, wer ihre Daten erhält und wie sie genutzt werden dürfen: Ob nur zur Ansicht, zum Download oder zur Bearbeitung.

Made in Germany – zertifizierter Anbieter

Bedienkomfort, Kosteneffizienz und Kontrolle der Datensicherheit sind bei der Qualität einer Datenraum-Lösung ebenso wichtige Kriterien wie Seriosität und Standort des Anbieters. netfiles bündelt alle Vorteile: In Deutschland ansässig, unterliegt das Unternehmen den strengen Auflagen des Bundesdatenschutzgesetzes (BDSG) und der europäischen Datenschutzgrundverordnung (DSGVO). Seine IT-Sicherheitsverfahren wurden vom TÜV Süd nach ISO/IEC 27001 zertifiziert.

Im netfiles Datenraum werden sämtliche Dokumente mit dem Advanced Encryption Standard (AES) 256-Bit stark verschlüsselt und vor unbefugtem Zugriff geschützt. Die Server des Anbieters befinden sich ausschließlich in hochsicheren Rechenzentren in Deutschland.

Interessierte Unternehmen können den netfiles Datenraum kostenlos und unverbindlich 14 Tage lang testen:
www.netfiles.de/kostenlos-testen ■

NETFILES

Ihr virtueller Datenraum

Sicherer Austausch vertraulicher Daten

Sicherer Datenaustausch

Mit netfiles können Daten einfach und sicher innerhalb eines Unternehmens oder mit Kunden und Lieferanten ausgetauscht und sichere Datenräume für beispielsweise M&A Projekte, Due Diligence Prüfungen, Asset-Transaktionen, Gremienkommunikation, Immobilien und Vertragsmanagement eingerichtet werden. Detaillierte Zugriffsrechte regeln Lese- und Schreibrechte im Datenraum und gewährleisten höchsten Schutz bei der Bereitstellung und Verteilung von Dokumenten und eine effektive Zusammenarbeit.

Made in Germany

Höchste Sicherheit für Ihre Daten – Die netfiles GmbH ist ein deutsches Unternehmen mit Sitz, Entwicklung und Hosting in Deutschland.

Kostenlos testen
www.netfiles.de

netfiles GmbH
+49 8677 915 96-10 · vertrieb@netfiles.de

Wo steht Deutschland bei Industrie 4.0?

Die Digitalisierung der Industrie steht weltweit bei vielen Ländern auf der Agenda. Wer Erfolg als Industriestandort haben will, muss die Voraussetzungen für die Digitalisierung verbessern. Das gilt auch für Deutschland. Öffentliche Stellen, Wirtschaftsverbände und Marktforscher haben dazu Position bezogen.

Von Oliver Schonschek

© fotohansel/stock.adobe.com

„Deutschland ist in vielen technologischen Zukunftsfeldern international sehr gut aufgestellt", so der Bundeswirtschaftsminister anlässlich der Hannover Messe. „Der Begriff Industrie 4.0 ist längst eine anerkannte Marke für die Digitalisierung der deutschen Fertigungsindustrie. Wir wollen bei Zukunftstechnologien führend sein, zum Beispiel bei der Digitalisierung und Automatisierung, beim autonomen Fahren, bei Künstlicher Intelligenz, der Batteriezellfertigung oder natürlich auch in Schlüsselbereichen wie IT-Sicherheit, Bio- oder Quantentechnologie."

Doch wie steht es um die Digitalisierung der deutschen Wirtschaft? Der Wirtschaftsindex DIGITAL erreicht 2018 wie im Vorjahr einen Wert von 54 Punkten (von maximal 100 Punkten). Der Index ist ein Teil des Monitoring-Report Wirtschaft DIGITAL, der jährlich im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) erstellt wird. Er bildet ab, wie es um die Digitalisierung der deutschen Unternehmen steht.

Aktuell sticht laut Bundeswirtschaftsministerium hervor, dass sich die Digitalisierungsschwerpunkte der deutschen Wirtschaft verlagert haben: Während zuletzt der Dienstleistungssektor deutliche Fortschritte machte, ist es jetzt die Industrie. Der Digitalisierungsgrad der deutschen Industrie ist seit 2016 von 39 auf aktuell 45 Punkte angestiegen.

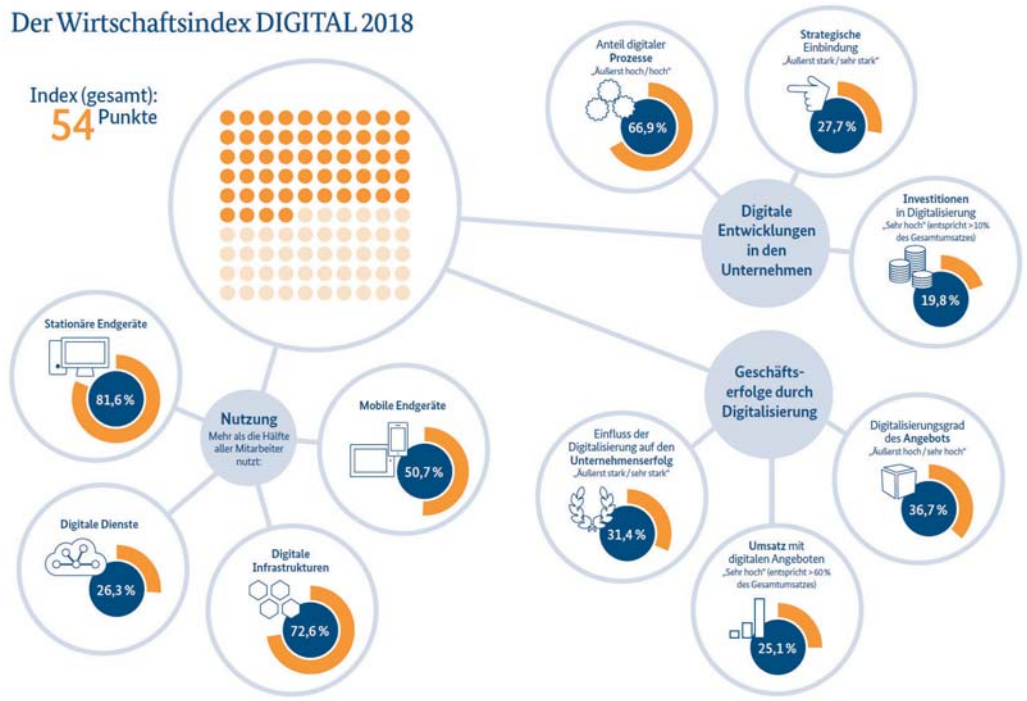


Bild: BMWi

Der Wirtschaftsindex DIGITAL drückt in einer Zahl den Digitalisierungsgrad der deutschen Wirtschaft aus. Er basiert auf der Befragung hochrangiger Entscheider aus 1.061 Unternehmen. In den Wirtschaftsindex fließen drei Themen ein: die Nutzung digitaler Geräte, der Stand der unternehmensinternen Digitalisierung sowie die Auswirkung der Digitalisierung auf die Firmen.

Vergleicht man jedoch den Index für die deutsche Wirtschaft insgesamt (54 Punkte) mit dem für die deutsche Industrie (45 Punkte), wird deutlich: Die deutsche Industrie hat Nachholbedarf bei der Digitalisierung. Auf dem Weg hin zu Industrie 4.0 gibt es noch einiges zu tun. Dabei gibt es Branchenunterschiede: Vorreiter in Sachen Industrie 4.0 ist laut Ernst & Young (EY) vor allem der Automobilbau. Hier setzt bereits jedes zweite Unternehmen (50 Prozent) auf die vernetzte Produktion. Auch die Konsumgüterindustrie hat die Vorteile erkannt. 46 Prozent der Unternehmen aus dieser Branche haben entsprechende Anwendungen im Einsatz. Es folgen die Elektrotechnik (37 Prozent) und der Maschinenbau (34 Prozent).

In einer Selbsteinschätzung, welche Nation beim Thema Industrie 4.0 führend ist, wird Deutschland unter den Top drei gesehen, mit 22 Prozent nur knapp hinter den USA (26 Prozent) und Japan (25 Prozent), wie der Digitalverband Bitkom berichtet. Doch wie sieht es wirklich aus?

Umfragen geben Hinweise auf Hemmnisse für Industrie 4.0

Zahlreiche Studien haben in den letzten Monaten untersucht, wo es Hindernisse für Industrie 4.0 in Deutschland gibt, darunter Ernst & Young mit der Umfrage „Industrie 4.0: Status Quo und Perspektiven". Demnach sehen 59 Prozent in den hohen Investitionskosten das größte Hemmnis, Industrie 4.0 im Betrieb einzuführen. Auch der Fachkräftemangel (57 Prozent) wird wie auch in den Vorjahren als großes Hindernis gesehen. Es folgen Sicherheitsbedenken (48 Prozent) und mangelnde Standards (46 Prozent).

Der Deutsche Industrie- und Handelskammertag (DIHK) nennt weitere Gründe: Die vielerorts unzureichenden Breitbandangebote erschweren eine Teilhabe der Unternehmen an produktivitätsrelevanten Trends beziehungsweise machen diese ganz unmöglich. Der Erfolg von Industrie 4.0 beziehungsweise darüber hinaus einer sogenannten Smart-Service-Welt wird insbesondere davon abhängen, ob die ⇨

dafür erforderlichen leistungsfähigen digitalen Infrastrukturen überall dort verfügbar sind, wo die Anwendungen sie erfordern. Ansonsten entstehen existenzgefährdende Wettbewerbsnachteile, so der DIHK.

Es herrscht internationaler Wettbewerb bei Industrie 4.0

Die Bemühungen, Industrie 4.0 einzuführen, lohnen sich; die von Ernst & Young befragten Betriebe sehen zahlreiche Vorteile: 72 Prozent schreiben Industrie 4.0 etwa ein großes Potenzial bei der Erhöhung der Produktionsflexibilität zu, gefolgt von schnelleren Reaktionszeiten (52 Prozent) und einer Erhöhung der Gesamtanlageneffektivität (47 Prozent). Im Durchschnitt rechnen die Unternehmen, die Potenzial zur Kostenreduktion sehen, mit Einsparungen von mehr als fünf Prozent durch Industrie 4.0. Knapp jedes fünfte Unternehmen (17 Prozent) rechnet mit Ersparnissen von mindestens zehn Prozent.

Diese Vorteile von Industrie 4.0 sehen allerdings auch andere Industrieländer, sodass Deutschland unter Wettbewerbsdruck gerät: In 68 Prozent der Industrie-Unternehmen weltweit hat die Digitalisierung der Produktion höchste Priorität, wie die aktuelle Industrie-4.0-Studie von McKinsey & Company zeigt. Deutschland liegt mit 69 Prozent im globalen Durchschnitt, doch Unternehmen in China (87 Prozent) und Indien (94 Prozent) widmen dem Thema noch größere Aufmerksamkeit.

28 Prozent der deutschen Unternehmen meinen, dass sie in ihrer Branche Vorreiter bei Industrie 4.0 seien, 64 Prozent sehen sich gleichauf mit der Konkurrenz. Diese Selbsteinschätzung kann jedoch täuschen, so die Berater von McKinsey: Erst in 21 Prozent der deutschen Firmen werden die wichtigsten Industrie-4.0-Anwendungen wie digitales Performancemanagement, KI-basierte Nachfrageprognose oder 3D-Druck schon umfassend angewendet. In China und Indien sind es mehr als 30 Prozent.

Empfehlungen für eine bessere Positionierung von Industrie 4.0

Die Berater von McKinsey nennen in ihrer Studie mehrere Fallstricke bei Industrie 4.0 in Deutschland, aus denen sich folgende Empfehlungen ableiten lassen:

- Mehr Aufmerksamkeit des Topmanagements: Die Geschäftsleitung muss für die Industrie-4.0-Strategie verantwortlich sein.
- Strategische Vision: Sie ist Voraussetzung für einen erfolgreichen Einsatz von Industrie 4.0.
- Industrie 4.0 ist mehr als Technologie: Es ist besonders wichtig, Industrie-4.0-Anwendungen schon früh auf ihre Wirtschaftlichkeit zu prüfen.
- Offenheit für Partnerschaften: Jedes Unternehmen sollte definieren, welche Anwendungen entscheidend sind, und nicht versuchen, alles allein zu machen – dies ist bei der Komplexität und der Entwicklungsgeschwindigkeit nicht zu leisten.
- Kulturwandel: Entscheider sollten agile Prozesse und Strukturen in ihrem Unternehmen einführen und die Mitarbeiter für die Veränderungen begeistern. □

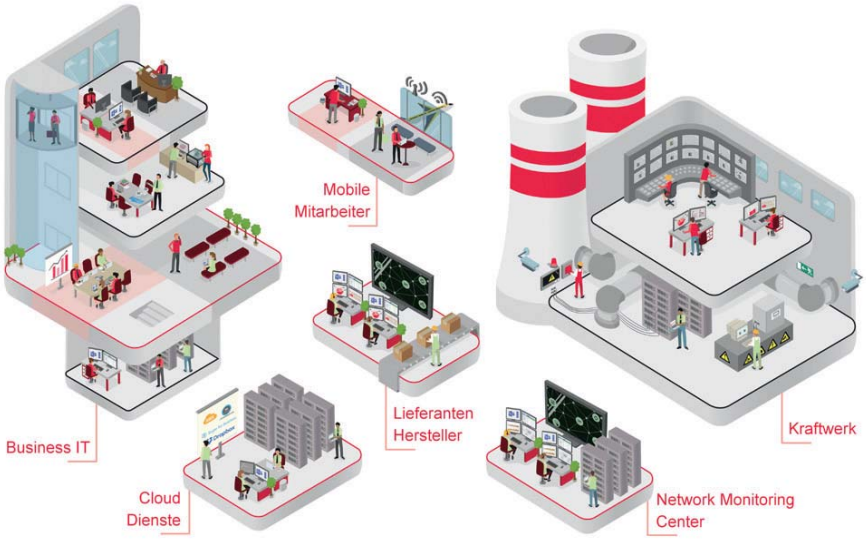
Zahlen zu Industrie 4.0 in Deutschland

- 40 Milliarden Euro beträgt die Summe der bis 2020 geplanten jährlichen Investitionen der deutschen Industrie in Industrie-4.0-Anwendungen.
- 20 Prozent der Unternehmen in der Automobilindustrie nutzen bereits jetzt selbststeuernde Anlagen.
- 153 Milliarden Euro beträgt das zusätzliche volkswirtschaftliche Wachstum in Deutschland durch Industrie 4.0 bis 2020.
- 83 Prozent der Unternehmen sehen einen hohen Digitalisierungsgrad ihrer Wertschöpfungsketten im Jahr 2020.

Quelle: BMWi

Kritische Infrastrukturen sicher vernetzen

Digitalisierung bedeutet vor allem Vernetzung und Automatisierung. Um den reibungslosen Betrieb kritischer Anlagen und Systeme zu gewährleisten, steht nun statt der physischen Infrastruktur zunehmend die digitale Orchestrierung von Anlagen, Mitarbeitern, externen Fachkräften, Lieferanten, Partnern und Kunden im Fokus.



Die stetige Modernisierung von Anlagen und Geräten sowie der damit verbundene Einsatz neuer Technologien im Bereich der Automatisierungsprozesse steigert die Abhängigkeit von Informations- und Kommunikationstechnik. Mit Blick auf die IT-Sicherheit stellen sich in dieser Situation sowohl bekannte als auch neuartige Herausforderungen. Auf beides gibt es bereits Antworten. Eine resistente IT-Infrastruktur ist mehr denn je eine notwendige Basis für betriebskritische Prozesse. Die IT-Sicherheit muss mit dem steten Bedarf an Vernetzung Schritt halten und Insellösungen, heterogene Systemumgebungen, verschieden klassifizierte Netze mit zum Teil besonderem Schutzbedarf sowie entsprechende Endgeräte und Anwender sicher zusammenbringen.

Eine Lösung zur sicheren Vernetzung und Separierung kritischer Netzwerke ist die secunet security infrastructure (ssi), die branchenübergreifend in klassischen IT- und auch Industrienetzwerken eingesetzt werden kann. Um ein einheitliches Sicherheitsökosystem zu etablieren, umfasst ssi verschiedene Komponenten – so zum Beispiel vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Verschlüsselungs- und Netzseparierungstechniken. Ziel dabei ist, kritische Netze über Standorte hinweg zu isolieren und über sichere Gateways und Quarantänesysteme mit der „Außenwelt“ – d. h. mit Herstellern, Dienstleistern, Projektpartnern – zu verbinden. Gleichzeitig können die etablierten Perimeter und Schutzvorrichtungen im Netzwerk intelligent und automatisiert in Echtzeit überwacht werden. So behalten Betreiber kritischer Infrastrukturen jederzeit den Überblick und die Kontrolle über ihre Systeme. ■

IT SECURITY „MADE IN GERMANY“
NOSPAMPROXY

Würzburger Versorgungs- und Verkehrs-GmbH (WVV) erweitert mit NoSpamProxy sein Dienstleistungsportfolio um E-Mail-Sicherheit als Service

Energie, Mobilität, Parkraum, Binnenhäfen und Badespaß – dafür steht die Würzburger Versorgungs- und Verkehrs-GmbH (WVV). Nun nutzt das Versorgungsunternehmen seine IT-Kompetenz und erweitert unter der Marke WVV iT solutions sein Portfolio um Mail-Security als Service.

Sicherer Datenaustausch in der Energiewirtschaft als Treiber

Neue Regularien der Bundesnetzagentur zum sicheren Datenaustausch zwischen Marktpartnern der Energiewirtschaft erforderten bei der WVV die Einführung von E-Mail-Verschlüsselung. Die EDI@Energy-Richtlinie verlangt unter anderem die Signatur und Verschlüsselung von E-Mails nach dem S/MIME-Standard mit digitalen Zertifikaten eines Vertrauensdienstean-bieters. Den Unternehmen der Energiebranche drohen erhebliche Konsequenzen bei Nichteinhaltung der Richtlinie, wie etwa das Recht des Empfängers auf Verweigerung der Annahme der unsignierten elektronischen Nachricht.

Um die neuen Auflagen erfüllen zu können, wurde nach einer ganzheitlichen Lösung gesucht, die nicht nur die Anforderungen der EDI@Energy-Richtlinie erfüllt, sondern auch die der DSGVO und der allgemeinen IT-Sicherheit. Die IT-Experten der WVV entschieden sich für das E-Mail-Security-Gateway NoSpamProxy von Net at Work als Verschlüsselungs- und E-Mail-Security-Lösung. Nach einem Workshop und einem Test im Echtbetrieb wurde NoSpamProxy in wenigen Tagen unternehmensweit genutzt. Dabei bietet das Gateway alle erforderlichen Funktionen zum einfachen Betrieb und zur Administration des E-Mail-Verkehrs. Anwender können ohne besondere Schulung und Verschlüsselungs-Chinesisch entsprechend der festgelegten Policies E-Mails automatisch verschlüsselt versenden und empfangen.

Für die Beantragung und Verwaltung von Zertifikaten wurde D-Trust, der Vertrauensdiensteanbieter der Bundesdruckerei, direkt angebunden. Ein besonderer Vorteil von NoSpamProxy ist die nahtlose Integration der Zertifikateverwaltung mit dem D-Trust Certificate Service Manager (CSM), der den Aufwand für die Zertifikatsverwaltung deutlich reduziert und hochverfügbare sowie optimal organisierte Zertifikatsbestände ermöglicht. Die Anbindung an NoSpamProxy gewährleistet den automatisierten Abruf von Zertifikaten für jeden Mitarbeiter.

Vom Kunden zum Partner

Die Lösung hat das Team der WVV so überzeugt, dass man nach dem erfolgreichen Einsatz intern beschloss, auch externen Kunden einen modernen Mail-Security-Service auf der Basis von NoSpamProxy anbieten zu wollen. Im besten Sinne eines Versorgungsunternehmens bietet die WVV privaten und gewerblichen Kunden unter der Marke WVV iT solutions digitale Zertifikate für die interne und externe Sicherheit an. Dieser Service wird nun um E-Mail-Sicherheit als Service ergänzt: Kunden können zukünftig den Betrieb ihrer E-Mail-Sicherheit komplett an WVV iT solutions auslagern.

> ”Wir sind von NoSpamProxy so begeistert, dass wir darauf aufbauend auch unseren Kunden einen vollständigen Service für E-Mail-Sicherheit mit Spam- und Malware-Schutz, sicherer E-Mail-Verschlüsselung und der Möglichkeit zur sicheren Übertragung großer Datenmengen anbieten. Durch den intensiven Einsatz intern als Referenz-Lösung, können wir sicherstellen, dass unsere Kunden unsere Erfahrungen und Best Practices übernehmen können. Einzigartig dabei ist, dass nur Komponenten ‚Made in Germany' zum Einsatz kommen.

Andreas Reumann, Gruppenleiter IT der Würzburger Versorgungs- und Verkehrs-GmbH

noSpamproxy® Protection zum Schutz vor Spam, Phishing und Malware, das Modul Encryption zur einfachen Verschlüsselung von E-Mails, das Modul Large-Files-Transfer zur sicheren Übertragung großer Dateien sowie das Modul Disclaimer für zentrale Marketingbotschaften in ausgehenden Mails. Zusammen gewährleisten sie den vollständigen Schutz Ihrer E-Mail-Kommunikation. Zentral auf Microsoft Server on Premise oder in Azure, einfach, sicher, wirtschaftlich. Mehr Informationen erhalten Sie online unter www.nospamproxy.de

Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn
GERMANY
T +49 5251 304-600
info@netatwork.de

VPN-Gateway als Mittler zwischen IT und Operativer Technologie

Informationstechnologie (IT) und Operative Technologie (OT) wachsen zusammen, unter anderem im Industrial Internet of Things (IIoT). In puncto Sicherheit haben aber viele Produktionsumgebungen noch Nachholbedarf. Abhilfe kann ein zentraler Verwaltungspunkt schaffen, indem er eine Brücke schlägt zwischen Produktions- und Informationswelt. Ein wichtiges Mittel hierfür wären geschützte Netzverbindungen von IT und OT durch Verschlüsselung und Zusatzfunktionen zur Vereinfachung des Managements sicherheitsrelevanter Komponenten beider Welten.

Von Jürgen Hönig, NCP engineering

Etwas despektierlich heißt es ja „Kommunikation ist, wenn man sich trotzdem versteht“. Aktuell sprechen durch das Internet der Dinge, oder im professionellen Bereich das Industrial Internet der Dinge (englisch IIoT), immer mehr einzelne Punkte miteinander. Die Verständigung wird dadurch aber immer schwieriger.

Dies hat unter anderem mit der Technik selbst zu tun. Im industriellen Bereich sind seit vielen Jahren proprietäre Bussysteme und Protokolle üblich, die mit der IIoT-Welt, die typischerweise auf TCP/IP setzt, nicht kompatibel sind. Außerdem ist die Anzahl unterschiedlicher IIoT-Geräte enorm. Waren früher – wenn überhaupt – eine Handvoll Geräte in Produktionshallen in der Lage über ein Netzwerk miteinander zu kommunizieren, sind es heute Hunderte oder gar Tausende.

Intensive Datenkommunikation bedeutet viele offene Kommunikationskanäle und damit erhöhte Sicherheitsanforderungen. Durch die Vielzahl an Verbindungen zwischen IIoT-Geräten entstehen neue Angriffsvektoren. Mussten früher maximal die eingehenden Remote-Control-Verbindungen für Fernwartungszwecke geschützt werden, enthalten nun auch interne Datenströme schützenswerte Informationen. Im Prinzip muss in einer voll vernetzten IIoT-Umgebung jede Verbindung abgesichert werden, die den Perimeter der Produktionshalle verlässt. Und selbst Verbindungen zwischen Komponenten innerhalb der Produktion sollten betrachtet werden. Im Ergebnis ist es die größte Herausforderung, eine sehr große Zahl unterschiedlichster Verbindungen möglichst sicher, aber auch sehr zuverlässig, hochverfügbar und möglichst automatisiert zu schützen.


Bild: NCP

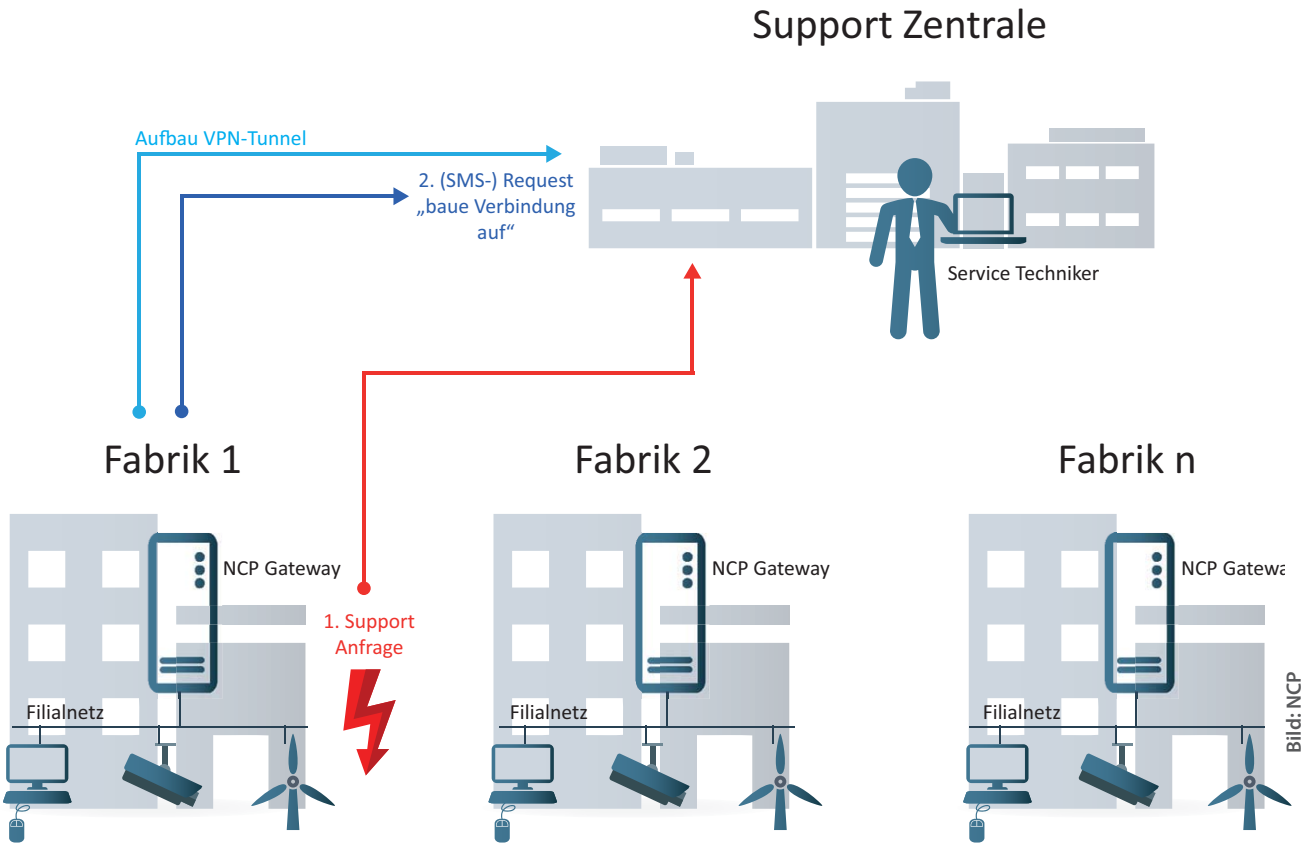
Produktionsumgebung treibt Cloud-Nutzung voran

Berücksichtigt werden muss dabei auch das Thema Cloud. Viele Firmen, die bislang keine Cloud-Dienste nutzten, haben bei IIoT-Anwendungen deutlich weniger Bedenken gegenüber der Cloud. Viele Maschinenhersteller sind mittlerweile ebenfalls dazu übergegangen, ihre Fernwartungsdienste über die Cloud anzubieten. Hierdurch werden direkte Verbindungen zwischen Hersteller-LAN und Maschine durch Verbindungen mit der Cloud als Endpunkt ersetzt. Auch diese Datenströme müssen gesichert werden, was bei der Menge an IIoT-Elementen hohe Skalierbarkeit und eine einfache, möglichst automatisierte Verwaltung bedeutet.

Wie lassen sich diese Sicherheitsanforderungen der Produktionsumgebung in ein übergreifendes Sicherheitskonzept eingliedern? Traditionell handelte es sich bei IT und OT um technisch und organisatorisch getrennte Welten ohne Berührungspunkte. Heute werden abteilungsübergreifend alte und neue Produkte, Technologien und damit auch deren Protokolle verzahnt. In der IT spielt Sicherheit eine der Hauptrollen, während in der Produktion vor allem effiziente und durchgängige Prozesse im Vordergrund stehen. Diese Ziele gilt es in einem übergreifenden Konzept zu vereinen.

Mit der Sicherheitslösung als Dreh- und Angelpunkt

Dieser Herausforderung könnte beispielsweise durch die Nutzung der umfangreichen Managementmöglichkeiten einer Endpoint-Sicherheitslösung als zentralem Dreh- und Angelpunkt begegnet werden. Die Schutzziele Vertraulichkeit und Integrität lassen sich für ⇨



Zentral verwaltete Fernwartung

Datenverbindungen ideal durch ein Virtual Private Network (VPN) umsetzen. Wenn die VPN-Lösung IT- und OT-Anforderungen gerecht werden kann, haben die Anwender einen Ansatzpunkt, um ihre Sicherheitslösung in beide Welten auszubringen und trotzdem von nur einer Stelle aus zu kontrollieren.

Dies ermöglicht jedoch nicht jede VPN-Lösung. Zwar nutzen VPNs etablierte Techniken und sind von vielen Herstellern verfügbar, allerdings mit Unterschieden zwischen klassischen VPN-Umgebungen und einem Einsatz im Industrieumfeld. So verwenden Industriekomponenten im Normalbetrieb selten eine Benutzerschnittstelle. Wenn diese Netzverbindungen gesichert werden sollen, muss die Authentifizierung und Autorisierung ohne Interaktion ablaufen. Ebenfalls eine große Rolle spielt die Skalierbarkeit. Schon einige Dutzend SPS und die dazu gehörenden Sensoren und Aktoren führen zu einem weit verzweigten Netz mit einer großen Zahl von Verbindungen. Nicht jede davon ist zwingend schützenswert, aber die reine Anzahl sorgt schnell für Unübersichtlichkeit. Es kommt beim effektiven Schutz darauf an, auch große Verbindungsmengen mit möglichst geringem Aufwand zu verwalten und den Überblick zu behalten.

Unterstützung bei der einheitlichen Verwaltung erhalten die IT- und OT-Abteilungen von Geschäftsleitung und Controlling. Eine Konsolidierung ist nicht nur aus Sicht der Sicherheit sinnvoll, auch die Kosten lassen sich mit einer homogenen Lösung besser kontrollieren. Das lokale Netz kann auf externe Teilnehmer wie Partner, Kunden oder Dienstleister ausgedehnt werden. Eine Brücke zwischen den Welten ist daher nicht nur technisch, sondern auch ökonomisch sinnvoll.

VPN-Gateways für OT und IT

Für den Nürnberger VPN-Hersteller NCP sind diese Anforderungen mittlerweile Tagesgeschäft. Aus seinen VPN-Gateways, die traditionell im Bereich IT eingesetzt wurden, ist eine universelle Plattform geworden, die in beiden Welten zuhause ist. Die neuen Anforderungen aus der OT wie automatische Authentifizierung und hohe Skalierbarkeit spiegeln sich in Erweiterungen der Standard-VPN-Server und speziellen Gateways für IIoT-Umgebungen wider.

Ein typischer Anwendungsfall zeigt, wie gut sich eine durchdachte VPN-Lösung in die OT-Welt einfügen lässt. Produktionsumgebungen sind oft in sich geschlossene Inseln, die mit identischen IP-Adressbereichen agieren. Solange keine Interaktion mit anderen Inseln notwendig ist, stellt dies auch kein Problem dar. Doch für VPN-Verbindungen zwischen den Inseln und weiteren Hosts im Netz sind 50 Subnetze nach dem Muster 192.168.1.xxx zunächst ein großes Hindernis. Bei einem Kunden von NCP wurden mehrere Tausend IP-Kameras in fünf Bereiche aufgeteilt, jeweils mit identischen Netzparametern. Normalerweise wäre kein Zugang zu den Kameras möglich, ohne in vier Netzsegmenten alle Parameter zu ändern. Durch die Network Address Translation isoliert der NCP Enterprise Management Server die verwendeten IP-Adressen der Inselsysteme vom Rest des Netzwerks. So sind Dutzende, Hunderte oder Tausende Inselnetze mit den gleichen IP-Parametern möglich, ohne dass es zu Konflikten kommt.

Flexibler Verbindungsaufbau und automatische Authentifizierung

Ebenfalls sehr wichtig ist die Art des Verbindungsaufbaus. IIoT-Geräte arbeiten häufig an weit abgelegenen Standorten, benötigen aber keine durchgehend aktive Netzverbindung. Moderne IIoT-Gateways wie die von NCP können selbstständig eine Verbindung initiieren, sich über ihre einzigartige ID beim VPN-Gateway ausweisen und erhalten dann Zugriff auf das interne LAN. Der gesamte Vorgang ist vollkommen automatisiert. Auch Authentifizierungsmethoden über Smartcards oder Zertifikate sollte das IIoT-Gateway unterstützen – ebenso ID-Nummern der Hardware wie die Prozessor-ID oder eine Seriennummer des Motherboards. Es ist ausreichend, wenn das Linux-basierte Betriebssystem des Gateways das Merkmal über eine Systemfunktion und ein Shellscript auslesen kann.

In Unternehmen mit maßgeblichem Produktionsanteil verändern sich derzeit die Aufgaben und Zuständigkeiten teilweise sehr stark. Wie viele Sicherheitsanbieter feststellen, wird die OT offener und engagierter bei der Absicherung ihrer Systeme und sucht aktiv die Verbindung mit dem Gegenpart in der IT. Auf der anderen Seite erkennen auch die IT-Administratoren, dass ihr Wirkungsbereich nicht an der Schwelle zur Werkshalle aufhört.

Intern sind die Firmen inzwischen gut aufgestellt und haben ihre Hausaufgaben gemacht – alle Voraussetzungen für ein umfassendes Sicherheitskonzept sind damit vorhanden. Es mangelt nur noch an Tools, um die zahlreichen „Fäden“ ohne großen Aufwand zusammenzuführen und sicherzustellen, dass in der Masse der Verbindungen nichts übersehen wird. Eine zentrale VPN-Lösung, die sowohl den technischen als auch den organisatorischen Anforderungen von IT und OT genügt, kann das passende Tool für diese Aufgabe sein. □

Der Autor

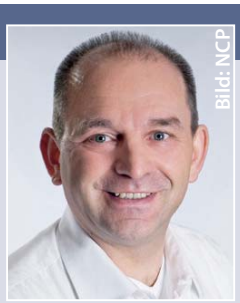


Bild: NCP

Jürgen Hönig ist Leiter Marketing bei der NCP engineering GmbH.

IT-Sicherheit für Unternehmen ganzheitlich gedacht

Unternehmen stehen im Fadenkreuz von Cyberkriminellen. Alleine in den Jahren 2016 und 2017 verzeichnete die deutsche Industrie einen Schaden von 43,4 Milliarden Euro – das zeigt eine Studie des Branchenverbands Bitkom. Firmen müssen dann nicht nur die oft fatalen Folgen von Sabotage, Datendiebstahl oder Spionage bewältigen, sie müssen auch ihre eigene IT-Sicherheit überdenken.

Von Kathrin Beckert-Plewka, G DATA Software

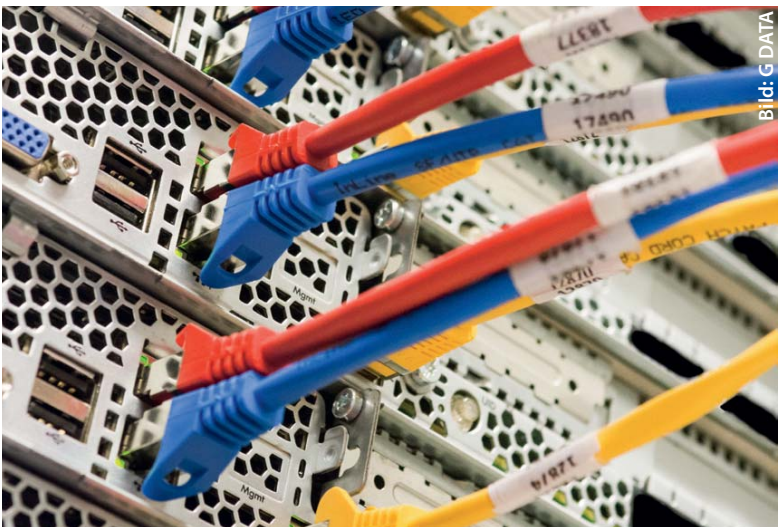
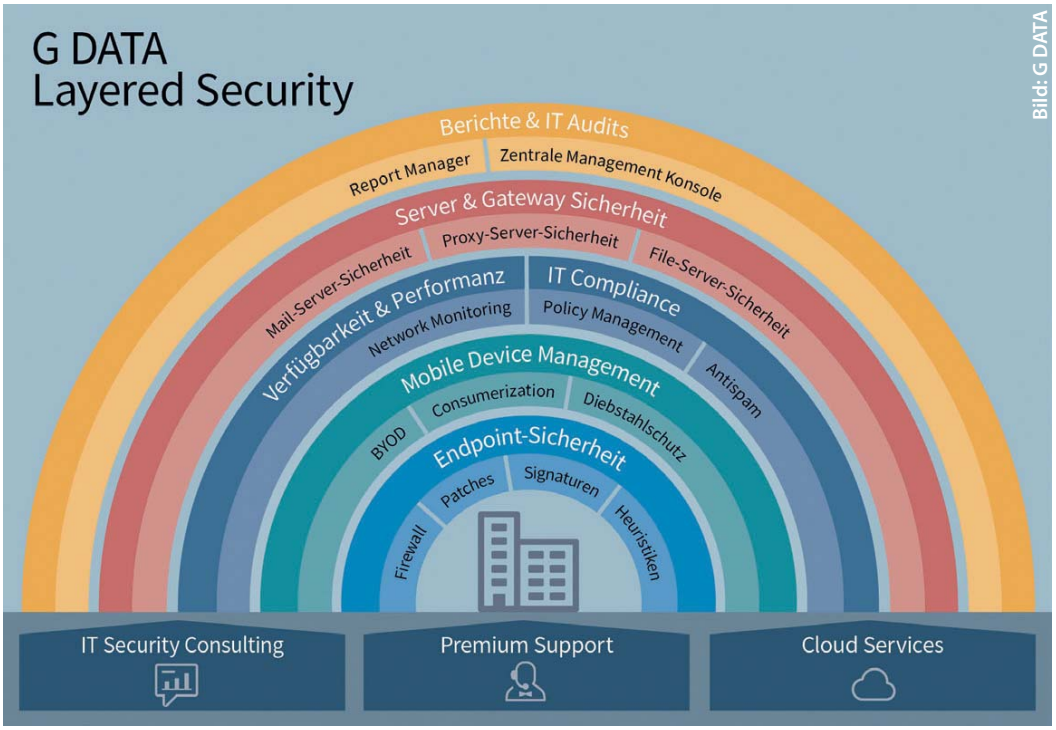


Bild: G DATA

Dabei stehen IT-Verantwortliche vor der schwierigen Aufgabe, die IT-Systeme bedarfsgerecht und lückenlos abzusichern und dabei die Produktivität nicht zu beeinflussen.
Entscheidend ist ein durchdachtes und passgenaues IT-Sicherheitskonzept, das alle individuellen Risiken, Herausforderungen und Bedürfnisse des Unternehmens berücksichtigt, zum Beispiel die Absicherung heterogener Netzwerkstrukturen oder die Definition besonders schützenswerter Bereiche. Ein zuverlässiger und umfassender Schutz vor Cyberangriffen ist unverzichtbar. Dabei stellen die Mobilität der Daten und der Einsatz unterschiedlicher Geräte und Systeme IT-Verantwortliche oft vor eine große Herausforderung.

Die Lösung: mehrschichtige IT-Sicherheit

Um das Konzept umzusetzen, ist der Einsatz einer modularen und mehrschichtigen Sicherheitslösung sinnvoll, die sich nahtlos in die bestehenden Systeme einbinden lässt. Beim „Layered Security"-Konzept, wie es beispielsweise G DATA bei seinem Business-Portfolio einsetzt, wird der Schutz Schicht für Schicht aufgebaut. Sinnvoll ist, wenn die Sicherheitslösung klassische Security-Maßnahmen mit NextGen-Schutztechnologien vereint, so ist ein Schutz auch vor noch unbekannten Schadpro-



Schicht für Schicht wird beim „Layered Security"-Modell die IT-Sicherheit für ein Unternehmen aufgebaut. Vorteil: Die IT-Systeme sind durch den Einsatz von nur einer Lösung abgesichert.

grammen und Angriffsmustern sichergestellt. Lösungen der neuesten Generation stellen außerdem sicher, dass nicht nur einzelne Systeme und Client-PCs sicher vor Online-Gefahren sind, sondern auch alle Server, Notebooks, Tablets und Smartphones mit ihren unterschiedlichen Betriebssystemen mit in die IT-Security-Architektur eingebunden sind.

Umfassender Funktionsumfang statt einzelner Insellösungen

Mehrschichtige Sicherheit wird oft durch den Einsatz von mehreren kooperierenden Modulen sichergestellt. Das „Layered Security"-Modell bietet nicht nur Sicherheit für Server und Endpoints, darüber hinaus garantiert das System die Verfügbarkeit und Performanz der IT-Systeme, sodass die Produktivität, aber auch die Sicherheit der Daten und die Vertraulichkeit garantiert sind. Daher ist es wichtig, auf eine integrative Sicherheitslösung zu setzen, die alle notwendigen Komponenten vereint und die zentrale Verwaltung über eine einheitliche Schnittstelle ermöglicht.

Die Vorteile für Unternehmen liegen auf der Hand: „Layered Security" schützt die IT-Infrastruktur umfassend vor allen Cybergefahren und ermöglicht durch die zentrale Verwaltung aller eingebundenen Geräte eine einfache Steuerung ohne großen Ressourcenaufwand. Die Installation einer integrierten Lösung von einem einzelnen Anbieter ist – im Gegensatz zum Einsatz von Einzelkomponenten – zudem oft mit einem finanziellen Vorteil verbunden. □

Die Autorin


Bild: G DATA

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

Netzwerksegmentierung – der heilige Gral unternehmerischer IT-Security

Bereits im 13. Jahrhundert entstanden in Europa die ersten Einrichtungen, die auf ein Konzept zur Verteidigung setzten, das uns auch heute helfen könnte, unsere heutigen IT-Sicherheitsprobleme nachhaltiger zu lösen. Die Rede ist hier von den Mauern und Gräben, die eine Burg oder Stadt schützen, indem sie Angreifer abschirmen und Schützenswertes vor diesen abschotten.

Von Markus Schräder, CryptoMagic

Vergleicht man die Verteidigungsstrategien der heutigen IT-Sicherheit mit einer Stadt, die sich gegen mittelalterliche Armeen erwehren muss, so kann man durch die oft fehlende Isolation (übertragen: Mauern) den Eindruck einer Stadtwache haben, die versucht, im Akutfall innerhalb der eigenen Stadt sich jeden feindlichen Soldaten einzeln vorzunehmen, aber ein ums andere Mal überrannt wird ohne hieraus zu lernen.

Isolation 1.0

In den ersten Firewalls stand die Idee der Abschottung im Mittelpunkt. Der Grundsatz lautete: Was nicht erreicht werden kann, das kann auch nicht angegriffen werden. Die Angriffsfläche wurde beispielsweise signifikant durch die Nutzung von Paketfiltern verringert, indem über eindeutige Kriterien (z.B. Port und IP) erwünschte von nicht erwünschter Kommunikation getrennt wurde. Dass auch heute noch dieser isolatorische Ansatz, der in den Anfängen der 1990er Jahre Einzug hielt, in so gut wie allen IT-Sicherheitskonzepten auch heute noch enthalten ist, zeigt, wie sehr sich dieser bewährt hat und auch heute noch aktuell ist.


© Maksim Pasko/stock.adobe.com

Isolation 2.0

Es haben sich über die Jahre weitere Varianten isolatorischer Ansätze etabliert. Beispielsweise schotten Virtual Private Networks (VPNs) generalisiert den Datenverkehr ab, sodass hiermit auch über nicht vertrauenswürdige Netze durch den Einsatz von Verschlüsselung selbst sensible Daten transportiert werden können. Ähnliches leistet spezialisiert HTTPS für Webseiten oder SSH für Konsolenverbindungen. Die Virtualisierung von Betriebssystemen und Containern ermöglicht die gleichzeitige aber isolierte Nutzung einer Serverhardware einschließlich Betriebssystem. Auf Clientseite wird seit Langem über Sandboxing ein isolatorischer Ansatz verfolgt, beispielsweise indem ein Browser über die Scriptsprache Javascript auch potenziell bösartige Software in einer kontrollierten und isolierten Umgebung ohne Gefahr ausführen kann. In vielen Firmennetzwerken wird zudem die Isolation in Form einer demilitarisierten Zone (DMZ) an Firewalls genutzt oder VLANs, die hardwareseitige Isolation zwischen Port-Gruppen auch über mehrere Switches hinweg.

Isolation 4.0

Auch wenn das Prinzip einer DMZ allgemein bekannt ist, so wird dieses kaum systematisch im internen Netzwerk angewandt, sondern meist nur bei Servern, die am Übergang der Firewall zu nicht vertrauenswürdigen Netzwerken lokalisiert sind. Andere weitergehende Formen der Netzwerktrennung sind nur selten zu finden, wie beispielsweise die Port-Security, die es unterbindet, dass unbekannte Geräte durch ⇨

- einfaches Anstecken an einem Switchport ins Netzwerk eingebracht werden können. Die Frage stellt sich, warum hier nicht mehr passiert.

Der nächste logische Schritt ist es, die Kommunikation zwischen den Netzwerkgeräten im internen Netzwerk grundsätzlich nur verschlüsselt und authentisiert zuzulassen. Dieser Schritt wird in vielen Firmennetzwerken nicht gegangen, da er mit einem enormen Aufwand verbunden ist. Der Aufwand besteht darin, dass gewünschte Kommunikation in einem derart isolierten Netzwerk zwischen den Geräten gezielt nur zugelassen werden kann, wenn Technologien wie Virtual Private Network (VPN) genutzt werden, die es ermöglichen, verschlüsselte und getrennte Verbindungen über ein bestehendes Netzwerk herzustellen.

Wenn dies über die Technologie VPN umgesetzt wird, so muss pro Verbindung jedem Teilnehmer eine IP-Adresse zugeordnet werden und zudem zur verschlüsselten Kommunikation kryptografisches Material verteilt und regelmäßig aktualisiert werden. Zudem ist pro Verbindung ein Satz an Filterregeln zu pflegen, da ansonsten alle Dienste der Teilnehmer gegenseitig erreichbar sind. Da die für Filterregeln notwendigen Protokolldetails oft nicht bekannt sind und der Aufwand, diese für jede Verbindung nachzuvollziehen und zu pflegen, wirtschaftlich nicht vertretbar ist, erscheint diese Herangehensweise als unrealistisch. Um diesen Aufwand zu reduzieren und handhabbar zu gestalten, ist eine Technologie notwendig, die dies praktikabler ermöglicht, indem unabhängig von den Protokolldetails der jeweiligen Verbindung die Isolation stattfindet. Dies ist gegeben, wenn nicht wie im VPN die Parameter des verwendeten Protokolls, Ports und der IP-Adresse ausschlaggebend sind, sondern wenn anhand anderer Parameter die Isolation hergestellt werden kann. Die hierfür bestmöglichen Parameter sind: Welche Anwendung welchen Benutzers kommuniziert mit welcher anderen Anwendung welchen Servers? Wenn zudem zur Kommunikation bereits vergebene IP-Adressen trotzdem getrennt genutzt werden können, so führt erst dies zu einer wesentlich einfacheren und handhabbaren Verwaltung. Der Einsatz einer solchen Technologie im Gegensatz zum VPN verbessert die Kosten-Nutzen-Rechnung in grundlegenden Aspekten wesentlich.

Durch die Sicherstellung, dass eine bestimmte Software auf einem Client nur mit einer anderen bestimmten Software auf einem Server kommunizieren kann, wird die Angriffsfläche, die von bösartiger Software angegriffen werden kann, auf die vermittelnde Software reduziert. Wenn bei dieser Trennung zudem unterschieden wird, welche Komponente in einer Software genau am Zugriff beteiligt ist, sprechen wir von einem gänzlich neuen Sicherheitsniveau.

Isolierte Verbindungen zwischen Software ergeben einen Stabilitätsgewinn, da andere Verbindungen oder der allgemeine Netzwerkverkehr keinen störenden Einfluss nehmen können. Wenn die Protokolldetails von Kommunikationsbeziehungen nicht mehr relevant sind, kann jegliche aufwändige und fehleranfällige Bestimmung dieser entfallen. Dies kann Aufwand und Kosten sparen und bringt neben einem Sicherheitsgewinn große Vereinfachungen im Betrieb mit sich.

Detektion als Alternative

Als Alternative zur Isolation und Abschottung ist der Ansatz der Detektion weit verbreitet, meist sogar als primäre Verteidigungslinie gegenüber Angriffen auf IT-Systeme. Dieser Ansatz basiert auf der Erkennung von bösartigen oder gefährlichen Mustern anstatt auf der Isolation von Software und Systemen. Diese Muster werden von erfolgreichen Angriffen abgeleitet und beim Feststellen von Lücken nach und nach verbessert.

Der größte Nachteil dieses Ansatzes ist, dass sich hier mindestens bis zum Bekanntwerden

eines erfolgreichen Angriffes unvermeidlich Schutzlücken ergeben und zudem neuartige sowie ausreichend veränderte Angriffe prinzipiell nicht erkannt werden können. Spätestens wenn die menschliche Intelligenz diese Muster auf Lücken gezielt durchforstet, findet sich fast immer eine Umgehungsmöglichkeit. Dies möchte ich an zwei konkreten Beispielen erläutern:

Stellen Sie sich einen Virenscanner vor, der ein unbekanntes Programm erschöpfend bewerten soll, so dass eine belastbare Aussage getroffen werden kann. Da dies oft nur mit Erfahrungswerten oder dem Vorliegen des Schädlings selbst möglich ist, geschieht es auch heute immer wieder, dass Crypto-Trojaner durch die Systeme schlüpfen. Fast schon trivial kann dies von einem Angreifer erreicht werden, indem er einfach seine Software im Vorfeld gegen Virenscanner testet und diese entsprechend so lange verändert, bis der Virenscanner nicht mehr anschlägt – dies ist sogar bei der viel gelobten Verhaltenserkennung ein funktionierender Ansatz.

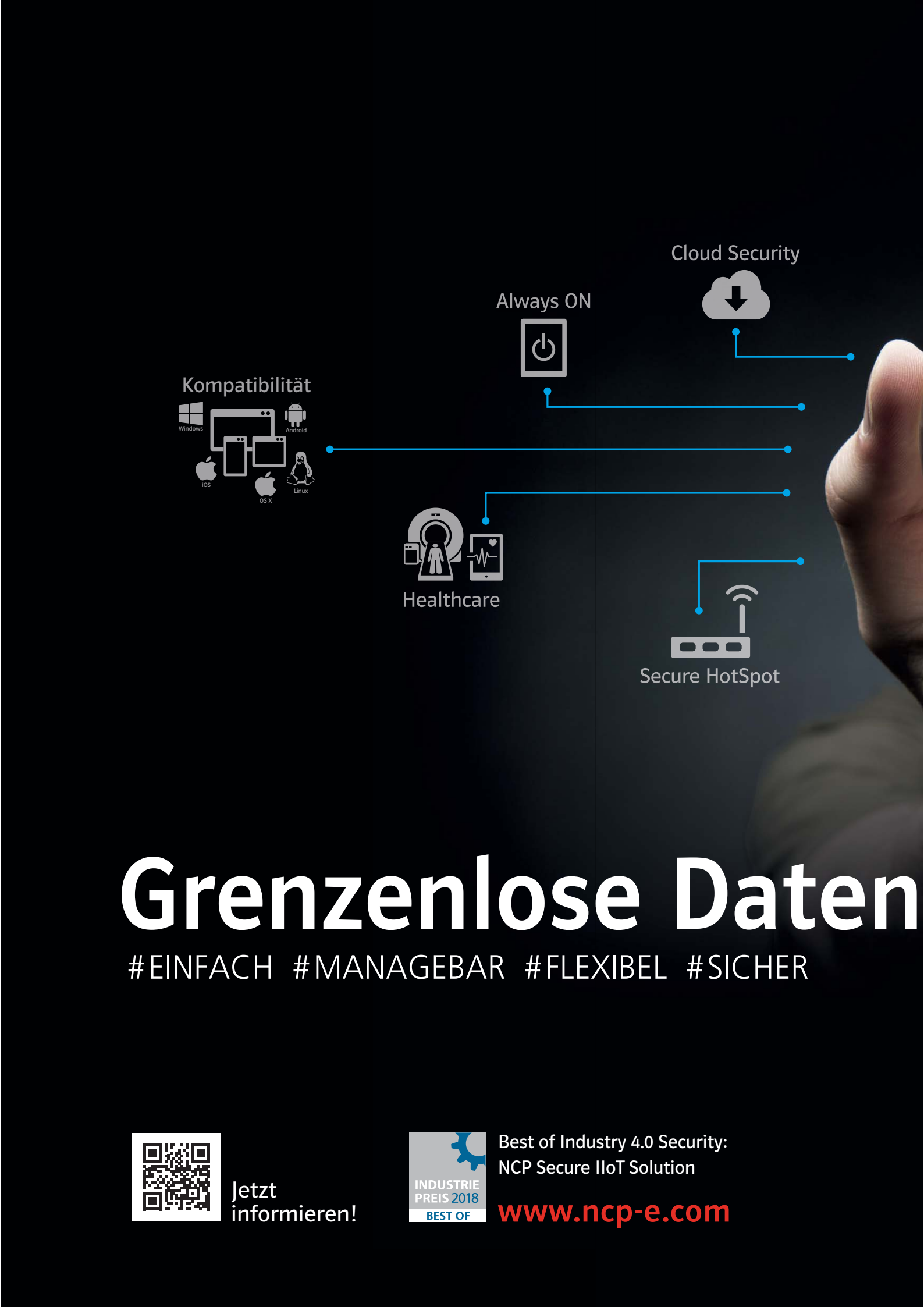
Ein zweites Beispiel sind Firewalls, hier spezifisch Web Application Firewalls, deren Aufgabe es ist, Webserver zu schützen. Diese haben lange Zeit 0-Bytes im Datenstrom unbehandelt übertragen, so dass trotz des Einsatzes eines solchen Systems lange Zeit hierüber geschützte Webserver erfolgreich angegriffen werden konnten. Erst nachdem diese Problematik breite Bekanntheit erlangte, wurden 0-Bytes als Gefahr erkannt und entsprechend behandelt. Da über verschiedene Umwege, beispielsweise über Encodings, von findigen Angreifern immer wieder 0-Bytes eingeschleust werden konnten, waren diese Angriffe in Variationen über lange Zeit trotz des Einsatzes derartiger Firewalls erfolgreich durchführbar.

Insbesondere Next-Generation-Firewalls oder Intrustion-Detection/Prevention-Systeme verwenden immer weniger nachvollziehbare und unüberschaubare komplexe Muster sowie heuristische Modelle, um jeden neuen wie alten Angriff weiterhin einzeln erkennen und abzuwehren zu können. Auf diesem Weg wird bis heute versucht, die Angriffsszenarien der Zukunft beherrschen zu können. Während dieses Vorgehen von mäßigem Erfolg geprägt ist, solange Angriffe nach einem bekannten Schema ablaufen, sind neuartige Angriffe in der Regel auf diesem Weg nicht aufzuhalten. Die Suche nach den Ursachen bei diffusen Fehlern, die unvermeidbare Nebenwirkungen beim fehlerhaften Greifen dieser Muster darstellen, ist meist langwierig und für alle Beteiligten frustrierend.

Es ist somit nicht verwunderlich, dass aus den beschriebenen Gründen ein gezielter und aufwändiger Angriff gegen diesen Ansatz im Normalfall erfolgreich sein kann – und oft nur am Aufwand scheitert. Trotz verbesserter Verfahren und dem Einsatz von künstlicher Intelligenz, die für niemanden mehr nachvollziehbar ist, waren 70 Prozent der deutschen Unternehmen in den Jahren 2016 und 2017 von erfolgreichen Angriffen betroffen. Diese Zahlen sind einer Umfrage des Bundesamtes für Sicherheit in der Informationstechnik von Anfang 2018 entnommen. In der gesamten letzten Dekade konnte kein Rückgang erfolgreicher Cyber-Angriffe erreicht werden, und es ist davon auszugehen – hier sei eine Extrapolation in die Zukunft erlaubt –, dass dies mit der Detektion als primäre Verteidigungslinie so bleiben wird. □

Der Autor

Markus Schräder blickt auf über 15 Jahre IT-Security-Erfahrung zurück. Er ist heute Geschäftsführer von CryptoMagic und war zuvor für verschiedene öffentliche und private Einrichtungen als Freelancer tätig.



Grenzenlose Daten

#EINFACH #MANAGEBAR #FLEXIBEL #SICHER

Jetzt informieren!

INDUSTRIE PREIS 2018 BEST OF

Best of Industry 4.0 Security:
NCP Secure IIoT Solution

www.ncp-e.com

NCP

SECURE COMMUNICATIONS

schnelle &
Zero Touch Konfiguration einfache Rollouts

kommunikation

Zertifikats zentrales
management Management

Industrie 4.0 Sicherheit softwarebasiert

plattformfähig cloudfähig

Secur IT y

made in Germany

Webapplikationen: Sicherheit auf allen Ebenen

Ob SAP, SharePoint, Outlook Web Access oder CRM-Anwendungen wie Microsoft Dynamics: Webanwendungen sind aus dem Geschäftsleben nicht mehr wegzudenken. Die Protokolle HTTP und HTTPS lassen sich mit herkömmlichen Firewalls jedoch nicht umfassend schützen. Und Web Application Firewalls waren bisher oft zu komplex, um sie einfach und sicher bedienen zu können. Neue Ansätze erleichtern die Handhabung erheblich – und bieten gleichzeitig mehr Sicherheit.

Von Walter Schumann, Rohde & Schwarz Cybersecurity

Bild: Rohde & Schwarz Cybersecurity

Für Hacker und organisierte Kriminelle sind Webanwendungen und Webdienste leicht zu überwinden. Denn das Web, speziell das Protokoll HTTP und auch das etwas sicherere HTTPS, wurde nicht für die heute üblichen komplexen Anwendungen konzipiert. Deshalb lassen sich Schwachstellen kaum vermeiden. Demnach steigt der Anteil an Datenlecks durch Angriffe auf Webanwendungen laufend.

Die Folgen dieser Angriffe sind gravierend: Wichtige Firmeninformationen können verloren oder zerstört und Kundendaten gestohlen werden. Fallen Kundendaten in die Hände von Hackern, führt das nicht nur zu einem enormen Imageschaden. Seit dem 25. Mai 2018 kann es teuer werden: Die EU-Datenschutz-Grundverordnung (EU-DSGVO) sieht empfindliche Strafen vor, wenn personenbezogene Daten nicht richtig geschützt werden. Die Finanzbranche hat auf die steigende Bedrohungslage bereits reagiert: Der „Payment Card Industry Data Security“ (PCI DSS) – ein Standard im internationalen Zahlungsverkehr – fordert den Schutz der Daten von Karteninhabern.

Die Sicherheit von Webanwendungen geht daher längst nicht nur die Betreiber von Online-Shops und Banking-Portalen etwas an. Große Unternehmen nutzen laut dem Open Web Application Security Project, kurz OWASP, aktiv bis zu 100 Applikationen. Und auch im Mittelstand und in kleinen Unternehmen gehören sie zum Standard. Hinzu kommen Webdienste, die als Backend für Mobilgeräte dienen und die Kommunikation zwischen Maschinen ermöglichen.

Verdächtige Inhalte stoppen

Wer Angriffe auf Webanwendungen abwehren will, braucht eine spezielle Web Application Firewall. Denn nur Web Application Firewalls können Daten überprüfen, die im HTTP- bzw. HTTPS-Protokoll auf der Anwendungsebene verkehren. Bei unpräzisen Untersuchungsmethoden liegt die Anzahl der Alarmmeldungen aufgrund von sogenannten False-Positives schnell bei mehreren Hundert am Tag. Bedrohungen werden erkannt, wo gar keine sind. Damit verursacht eine Web Application Firewall eher Mehrarbeit, als dass sie einen entscheidenden Vorteil bringt.

Um dies zu umgehen, wird die Firewall nicht selten wieder deaktiviert. Mit bestimmten technischen Konfigurationsmethoden lässt sich das Erkennen von bösartigem Datenverkehr zwar optimieren – allerdings nur durch Mitarbeiter, die über entsprechendes Spezialwissen verfügen. Kleine und mittelgroße Unternehmen kommen hier schnell an ihre Grenzen.

Mit neuen Konfigurationsmethoden lassen sich False-Positives erheblich reduzieren, ohne dass ⇨

So funktioniert eine Web Application Firewall

Eine Web Application Firewall wird als Reverse Proxy installiert. Sie kann deshalb den gesamten Datenaustausch zwischen Clients und Webserver analysieren. Verdächtige Inhalte werden von ihr gestoppt. Da die meisten Webanwendungen heute verschlüsselt sind, ist die Web Application Firewall ebenfalls in der Lage, SSL-verschlüsselten Datenverkehr zu überprüfen.

Eine Web Application Firewall bietet Schutz vor SQL-Injections, Cross-Site Scripting (XSS) und vielen weiteren Webangriffen. Entscheidend für die Qualität und Wirksamkeit des Schutzes ist die Art und Weise, wie sie bösartige Eindringlinge erkennt. Verschiedene Methoden sind dazu möglich. Verbreitet ist das sogenannte White- oder Blacklisting. Dabei werden wiederkehrende Muster von bösartigen Angriffen aufgelistet, sodass diese geblockt werden können. Solche Listen führen jedoch häufig zu False-Positives. Mit neuen Analyse-Ansätzen lassen sich diese deutlich reduzieren.

↪ Mitarbeiter komplexe Einstellungen treffen müssen. Die wichtigsten neuen Methoden sind:

Verhaltensbasierte Technologien und Workflow-Konzept

Statt Datensätze nur aufzulisten, werden Internetbedrohungen anhand ihrer Aktivitäten und spezifischen Verhaltensweisen identifiziert. Durch diese automatische Präzisierung der Daten sind aufwändige Voreinstellungen durch den IT-Administrator nicht mehr nötig. Auch Mitarbeiter ohne Spezialwissen können die Web Application Firewall installieren, und diese erfüllt in der Folge einen hohen Sicherheitsstandard. Gleichzeitig erhalten erfahrene Administratoren neue Möglichkeiten, die richtige Sicherheitsstufe einzustellen.

Scoring-Modell

Mit Scoring-Modellen lassen sich Denial of Service-Angriffe (DDoS) verhindern. Diese versuchen, einen Webserver durch eine massive Zusendung von Anfragen zum Absturz zu bringen. Nimmt man als Schwellenwert etwa die Anzahl der Anfragen, die eine einzelne IP innerhalb eines festgelegten Zeitraums übermitteln darf, werden Anfragen gestoppt, die über diese Anzahl hinausgehen. Das Scoring-Modell hat sich in Tests als äußerst effektiv erwiesen und konnte über 85 Prozent der neuen Angriffe ohne vorherige Aktualisierung oder Lernphase abwehren.

Der Autor


Bild: Rohde & Schwarz

Walter Schumann ist Senior Vice President Sales & Marketing von Rohde & Schwarz Cybersecurity. Das IT-Sicherheitsunternehmen schützt Unternehmen und öffentliche Institutionen weltweit vor Cyberangriffen.

Advanced Threat Detection

Angriffsarten werden immer ausgefeilter. Um sie aufzuspüren, werden besonders starke Sicherheitsmechanismen benötigt. Advanced-Threat-Detection-Lösungen sind speziell auf solche schwierigen Fälle ausgerichtet. Sie nutzen zum Beispiel sogenannte Sandboxing-Technologien, mit denen sich zu schützende Bereiche komplett isolieren lassen.

Einfache und sichere Authentifizierung

Auch die Authentifizierung spielt für die Sicherheit einer Webanwendung eine entscheidende Rolle. Nicht-autorisierten Personen wird der Zugriff auf die Anwendung verwehrt. Dafür muss eine Web Application Firewall in der Lage sein, den Anmeldeprozess und die Authentifizierung einer Webanwendung zu überwachen, ohne allerdings den Zugriff auf sie zu erschweren.

Dies gelingt, wenn hinter einer Anmeldung mittels Single-Sign-on weitere starke Authentifizierungen gruppiert werden. Der User kann mit einer einmaligen Authentifizierung an seinem Arbeitsplatz auf alle Rechner und Dienste zugreifen. Wenn diese Authentifizierung erfolgreich war, führt die Web Application Firewall weitere Authentifizierungen bei der Nutzung der jeweiligen Anwendung durch – ohne dass es der User merkt. Diese Technologien machen es möglich, dass das Verhältnis von Usability und Sicherheit bei Web Application Firewalls stimmt.

Fazit: Das Sicherheitsniveau mit Web Application Firewalls erhöhen

Eine Web Application Firewall in Kombination mit einer Netzwerk-Firewall steigert das Sicherheitsniveau von Unternehmen erheblich. Damit sind sie auf dem neuesten Stand, wenn es um die Anforderungen an eine moderne und belastbare IT-Infrastruktur geht. □

Warum E-Mail-Verschlüsselung trotz EFAIL & Co. sinnvoll ist

Flächendeckende E-Mail-Verschlüsselung gehört zum IT-Grundschutz und zu den grundlegenden Anforderungen der DSGVO. Dennoch werden Sicherheitslücken wie EFAIL immer wieder als Grund dafür angeführt, keine Verschlüsselung einzuführen. In diesem Artikel beleuchten wir das Für und Wider der E-Mail-Verschlüsselung und erläutern neue Schutzmechanismen des kommenden S/MIME-4.0-Standards.

Von Stefan Cink, Net at Work

Immer wieder werden Bedenken zur Wirksamkeit von E-Mail-Verschlüsselung geäußert. Zuletzt wurde im Mai dieses Jahres unter dem Begriff EFAIL eine Sicherheitslücke beschrieben, mit der unter bestimmten Umständen der Inhalt einer verschlüsselten E-Mail zugänglich gemacht werden kann. Dazu muss der Angreifer zunächst in den Besitz der verschlüsselten E-Mail gelangen. Diese wird dann – vereinfacht gesagt – mit einem Schadcode modifiziert erneut an den Empfänger gesendet. Durch das automatische Nachladen vermeintlicher Bilder wird der entschlüsselte Inhalt der E-Mail ganz oder teilweise an den Angreifer übermittelt.

Betroffen hiervon sind E-Mails im HTML-Format auf E-Mail-Clients mit entsprechenden S/MIME- oder PGP-Plugins, die automatisch Inhalte nachladen und diese Manipulation – durchaus dem geltenden Standard folgend – nicht erkennen oder sie ignorieren. Auch Gateway-basierte Lösungen können betroffen sein, wenn sie nicht dediziert auf diese Angriffsform hin optimiert wurden. Aber rechtfertigt die gelegentliche Identifikation von Sicherheitslücken in der E-Mail-Verschlüsselung, etwaige ⇨

- Projekte zur Einführung der Verschlüsselung zu verschieben? Sicher nicht.

Jede Verschlüsselung ist besser als keine

Die Alternative wäre, nicht zu verschlüsseln und darauf zu hoffen, dass die Nutzer keine vertraulichen Informationen oder personenbezogenen Daten per E-Mail versenden. Eine Vorstellung, die mit Blick auf die geschäftlichen Gepflogenheiten und das typische Nutzerverhalten geradezu als naiv einzustufen ist.

Hinzu kommt, dass schon heute die notwendigen Aufwände und technischen Fähigkeiten für Attacken auf verschlüsselte E-Mails hoch sind. Im Beispiel von EFAIL muss der Angreifer zunächst die richtige, verschlüsselte E-Mail abfangen. Das kann zwar durch Lauschangriffe auf das Netzwerk oder durch Kompromittieren des E-Mail-Accounts, E-Mail-Servers, Backups oder Clients erfolgen. Jedoch benötigt man bei einer gut gepflegten IT-Sicherheitsinfrastruktur für all diese Wege als Angreifer bereits einiges Geschick und die notwendigen Mittel.

Zudem schließen gewissenhafte Hersteller von E-Mail-Verschlüsselungslösungen Lücken wie EFAIL rasch durch entsprechende Patches und neue Methoden. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit Blick auf EFAIL & Co. klargestellt, dass OpenPGP und S/MIME „nach Einschätzung des BSI [...] weiterhin sicher eingesetzt werden können, wenn sie korrekt implementiert und sicher konfiguriert werden." Wie von den BSI-Experten erwartet, werden die Standards OpenPGP und S/MIME im Rahmen der anstehenden Überarbeitungen angepasst.

S/MIME-4.0-Standard bringt mit Authenticated Encryption noch mehr Sicherheit

Ein Beispiel für eine neuere Methode ist die Nutzung von Authenticated Encryption, deren Verwendung die kommende Version 4.0 des S/MIME-Standards ermöglicht. Dabei wird mit AES-GCM eine neue Klasse von Betriebsmodi für Block Cipher genutzt, die neben Vertraulichkeit auch Authentizität und Integrität sicherstellt. Die Injektion von Code in verschlüsselte E-Mails – wie sie auch bei EFAIL und verwandten Angriffsmustern praktiziert wird – wird damit sicher unterbunden.

Schon heute unterstützen die ersten Hersteller den neuen Standard in wesentlichen Teilen. Da Unternehmen und andere Organisationen jedoch nicht warten können, bis sich der neue Standard flächendeckend durchgesetzt hat, verfügen gute E-Mail-Security-Suiten über einen

Wie funktioniert EFAIL im Detail?

Grundlage für dieses Angriffsmuster ist eine Schwachstelle in den PGP- und S/MIME-Standards bzw. in deren Umsetzung. Die Angreifer machen sich dabei zunutze, dass auch bei verschlüsselten E-Mails die ersten Zeichen einer E-Mail bekannt sind. E-Mails starten in der Regel mit dem Text „Content-type: multipart/signed". Mit diesem Wissen lässt sich nun ein Angriff über den Betriebsmodus CBC für Block Cipher durchführen, der im Rahmen der aktuellen S/MIME- und PGP-Standards genutzt wird.

Dazu muss zunächst die verschlüsselte E-Mail vollständig mitgeschnitten werden. Da die Übersetzung der ersten Blöcke der verschlüsselten E-Mail bekannt ist, können nun Blöcke erzeugt werden, die nach der Entschlüsselung den HTML-Code <img ignore="" src=angreifer.url/ ergeben. Diese Blöcke werden dem eigentlichen, verschlüsselten E-Mail-Text vorangestellt. Sendet man nun diese modifizierte E-Mail an den Empfänger, entschlüsselt das Empfängersystem zunächst den kompletten Inhalt der E-Mail und sendet das Ergebnis per URL-Abfrage an den Angreifer.

dedizierten Schutzmechanismus, der wirksam vor Angriffsmustern wie EFAIL schützt und auch mit älteren E-Mail-Security-Standards funktioniert.

Trend zu zentralen Gateway-Lösungen

Das Beispiel EFAIL zeigt wieder einmal, dass die Zukunft der sicheren E-Mail-Kommunikation in zentral administrierbaren, integrierten Secure-Mail-Lösungen liegt. Zentrale Gateways zeigen hier klare Vorteile: Während bei clientbasierten Lösungen sichergestellt werden muss, dass der bereitgestellte Fix auf allen Clients mit ihren potenziell unterschiedlichsten Softwareständen richtig installiert und ausgeführt wird, reicht bei zentral administrierten Secure-E-Mail-Gateways das Update an einer Stelle aus.
Darüber hinaus erlauben moderne Gateway-Lösungen die effiziente Kombination aller verfügbaren Sicherheitsmechanismen. Beispielsweise kann eine intensive Auswertung der Senderreputation im Spam- und Malwareschutz bereits im Vorfeld die Chancen für eine erfolgreiche Kompromittierung zum Zweck des Mitschneidens verschlüsselter E-Mails drastisch einschränken. Mit SPF, DKIM & DMARC wird Spoofing sicher abgewehrt, so dass der Angreifer mit einer dem Empfänger unbekannten Domain senden muss, was wiederum in der Reputationsprüfung berücksichtigt werden kann. Wird für den Versand von E-Mails auch die DANE-Information mit einbezogen, kann sichergestellt werden, dass sich kein Angreifer zwischen Sender und Empfänger einklinken kann, indem eine TLS-verschlüsselte Verbindung aufgebaut wird.

Resilienz als wesentliche Neuerung

Jede Kommunikationsbeziehung – auch per E-Mail – hat immer zwei Akteure, und ihr Schutz ist immer nur so gut wie das schwächste Glied in der Kette. Daher sind besonders innovative E-Mail-Security-Produkte zunehmend resilient ausgelegt, d.h. sie funktionieren auch dann gut, wenn der Kommunikationspartner schwach ausgeprägte Kenntnisse hat, nur über unzureichende Infrastruktur verfügt oder sonstige widrige Umstände herrschen. Ein Beispiel im Bereich der Verschlüsselung ist die Möglichkeit zur verschlüsselten Übertragung auch dann, wenn der Kommunikationspartner keine eigene Verschlüsselungsinfrastruktur hat. Ein weiteres Beispiel für Robustheit gegen Fehler der Kommunikationspartner ist Advanced Key Management: Hat der Empfänger einer E-Mail beispielsweise unterschiedliche Zertifikate im Einsatz, sorgt das sendende Produkt für den Absender unbemerkt dafür, dass die richtige Kombination genutzt wird. Letztlich ist auch die Unterbindung von EFAIL-Attacken, selbst wenn der Kommunikationspartner nur über eine schwache E-Mail-Security verfügt, eine Resilienz-Funktion.
Durch die Weiterentwicklung der Technik wird die E-Mail-Verschlüsselung von einem bereits hohen Niveau aus immer sicherer. Der größte Unsicherheitsfaktor liegt heute darin, dass Unternehmen und Organisationen zum Teil noch immer keine E-Mail-Verschlüsselung nutzen – und dabei wäre das so leicht abzustellen. □

Der Autor


Bild: Net at Work

Stefan Cink ist E-Mail-Security-Experte bei Net at Work und Produktmanager 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.

Retarus E-Mail Security: Lassen Sie sich nicht aufhalten von Ransomware, Phishing und CxO Fraud

Neben der Flut aus Spam- und Viren-Mails sehen sich Unternehmen zunehmend auch mit komplexen Bedrohungen wie Social Engineering oder ausgefeilten Phishing-Angriffen konfrontiert. Traditionelle Sicherheitsmechanismen bieten vor solchen individualisierten Attacken oft keinen ausreichenden Schutz mehr.

retarus:

Zudem kursiert Malware binnen kürzester Zeit in stets neuen Varianten, die von gängigen Virenschutzlösungen häufig nicht gleich erkannt und somit nicht sofort herausgefiltert werden. Einmal unentdeckt ins Postfach eines Users gelangt, breitet sich Malware ungehindert in der gesamten IT-Infrastruktur aus. Die innovativen Funktionen von Retarus E-Mail Security schützen Sie auch vor Angriffen, gegen die traditionelle Virenfilter oft machtlos sind.

Deferred Delivery Scan

Ein zeitlich nachgelagerter Re-scan überprüft ausgewählte Dateianhänge, noch bevor diese zugestellt werden. Gerade bei neuer Malware können zum Zeitpunkt der erneuten Überprüfung bereits Signaturen vorliegen, die beim ersten Scannen noch nicht verfügbar waren.

Sandboxing

Unbekannte, verdächtige Dateien im E-Mail-Anhang werden vor der Zustellung durch die Sandbox-Mechanismen in einer sicheren Testumgebung überprüft. Hierfür setzt Retarus auf Technologie des führenden Anbieters Palo Alto Networks.

External Sender Visibility Enhancement

Diese Funktion markiert im Empfängerfeld eingehende Nachrichten deutlich, die im Absender eine nur scheinbar zum Unternehmen gehörige Absenderdomäne verwenden.

CxO Fraud Detection

Noch einen Schritt weiter als External Sender Visibility Enhancement geht die CxO Fraud Detection: Sie nutzt neben einer fortschritt-

lichen Analyse des E-Mail-Headers auch spezielle Algorithmen gegen From- oder Domain-Spoofing, die gefälschte Absenderadressen noch zuverlässiger als Betrugsversuch entlarven. Unternehmen können sich so besser vor finanziellem Schaden durch Social Engineering und CEO Fraud schützen.

Time-of-Click Protection

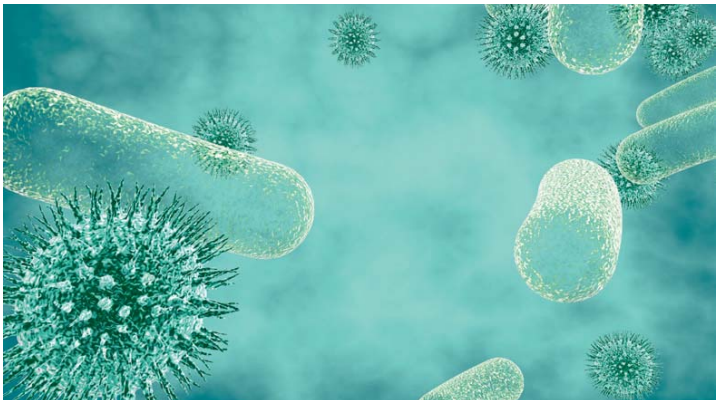
Um Phishing-Angriffe und somit den Verlust sensibler Daten rechtzeitig zu unterbinden, überprüft Retarus alle Links in eingegangenen E-Mails bei jedem Anklicken erneut auf mögliche Schadwirkungen. Sollten zwischenzeitlich neue Erkenntnisse über die Zielseite vorliegen, wird diese blockiert und eine Sicherheitswarnung angezeigt.

Forensic SIEM Integration

Forensic SIEM Integration bietet die Möglichkeit, forensische Daten (sog. Events) in Echtzeit bereitzustellen und per API an bestehende SIEM-Tools weiterzuleiten. Auf diese Weise kann der Datenstrom unkompliziert mit zusätzlichen Details zur E-Mail-Sicherheit angereichert werden.

Patient Zero Detection

Falls trotz vorgeschalteter Schutzmaßnahmen Malware via E-Mail in die Unternehmensinfrastruktur gelangt, kommt die von Retarus entwickelte und zum Patent angemeldete Technologie Patient Zero Detection zum Einsatz. Diese erzeugt schon beim Eingang einer E-Mail einen digitalen Fingerabdruck aller Attachments sowie enthaltenen URLs. Sobald Retarus E-Mail Security später in einem identischen Anhang Schadcode entdeckt oder eine URL als Phishing-Versuch identifiziert, werden alle bisherigen Empfänger der gleichen E-Mail-Anhänge und Links sowie deren Administratoren unverzüglich informiert. Über den Patient Zero Detection Reacting Process lassen sich Alertings automatisiert verarbeiten. Administratoren werden in der Regel alarmiert, bevor infizierte E-Mails geöffnet werden. So lassen sich diese unmittelbar löschen.



Die innovativen Funktionen von Retarus E-Mail Security schützen Sie vor Angriffen, gegen die traditionelle Virenfilter oft machtlos sind.

Die Retarus Cloud Services können Sie individuell an den Sicherheitsbedarf Ihres Unternehmens anpassen. Bereits die Essential Protection von Retarus E-Mail Security greift auf umfassende Schutzmechanismen mit bis zu vier verschiedenen Virenscannern zurück. Mit der Retarus Advanced Threat Protection sichern Sie Ihr Unternehmen zusätzlich gegen hochentwickelte Bedrohungen ab, während die Postdelivery Protection Sie vor Malware warnt, die selbst ausgefeilte vorgelagerte Schutzmechanismen umgehen kann.
Weitere Informationen finden Sie unter www.retarus.de/ATP ■

Retarus auf der it-sa!

Besuchen Sie uns vom 9. bis 11. Oktober 2018 in Nürnberg in Halle 10.1 / Stand 710.

Multi-Faktor-Authentifizierung: Basis für das Identitäts-management der Zukunft

Aktuell wird viel über das digitale Identitätsmanagement der Zukunft diskutiert. Mehrere Initiativen aus den unterschiedlichsten Branchen arbeiten mit Hochdruck an deutschen Identitäts- und Datenplattformen, um eine Alternative zu US-amerikanischen Angeboten von Playern wie Google oder Facebook zu schaffen.

Von Dr. Amir Alsbih, KeyIdentity

Die nationalen Initiativen zielen darauf ab, Internetnutzern hierzulande den Zugriff auf Online-Portale, Anwendungen und Transaktionen so einfach und sicher wie möglich zu machen – und zwar auf Basis der deutschen Sicherheits- und Datenschutzstandards und ohne das Risiko, dass die wertvollen Nutzerdaten im Ausland kompromittiert werden.

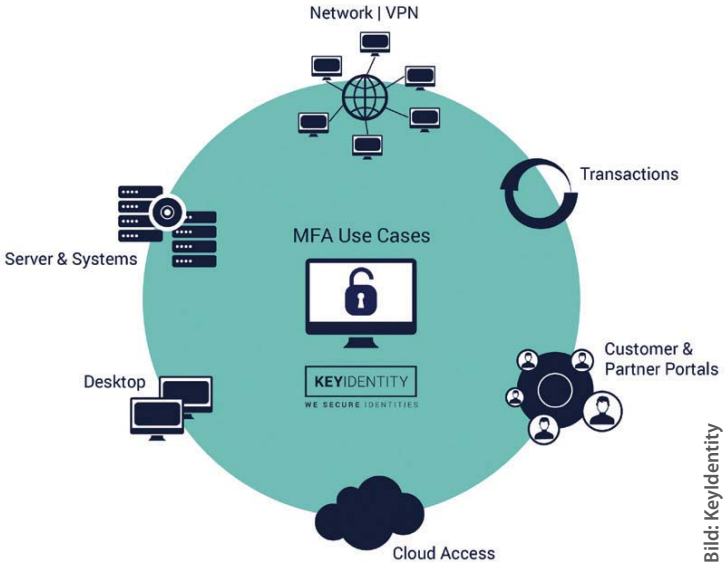


Bild: KeyIdentity

Eine wirklich lückenlose Authentifizierung digitaler Logins und Transaktionen kann nur die Multi-Faktor-Authentifizierung (MFA) gewährleisten.

Wenn digitales Identitätsmanagement, dann richtig!

Dies ist zweifelsohne ein wichtiger Schritt. Jedoch braucht es im Zeitalter der fortschreitenden Digitalisierung einen viel umfassenderen Sicherheitsansatz: Denn beim digitalen Identitätsmanagement der Zukunft werden nicht nur die Daten aus einer einzelnen Anwendung erfasst. Damit ein Nutzer wirklich alle seine Daten sicher vorhalten und verwenden kann, dürfen zahlreiche andere Zugänge wie etwa Kunden- und Mitarbeiterportale oder Supplier-Logins nicht außen vor gelassen werden. So lassen sich auf lange Sicht beispielsweise die Adressdaten der Deutschen Post mit Kontodaten aus dem Onlinebanking oder E-Commerce verknüpfen. Loggt sich ein Nutzer in eines dieser Portale ein, muss er seine Adresse und Kontodaten nicht noch einmal eingeben. Diese wären dann vorausgefüllt.

Passwörter allein zu unsicher

Dieses Beispiel macht eines deutlich: Durch das Erfassen und Verknüpfen von Nutzerdaten aus verschiedenen Einsatzbereichen entsteht ein riesiger Datenpool, der die aktuellen Kapazitäten von Anbietern wie Facebook oder Google bei Weitem übersteigt. Die Daten sind hochsensibel und müssen daher besonders gut und umfassend geschützt werden. Ein herkömmliches Passwort reicht für diese hohe Anforderung nicht mehr aus. Dies belegen nicht nur tägliche Fälle von Hackerangriffen, sondern auch Studien: So sind gestohlene oder schwache Passwörter mittlerweile in 81 Prozent aller Fälle die Ursache für einen Hack – Tendenz steigend (Quelle: Verizon Data Breach Investigations Report 2017). Die Ursache dafür liegt in ihrer Konzeption selbst: Einfache Passwörter sind leichter zu „knacken" (Stichwort: Targeted Password Guessing) und damit zu missbrauchen. Komplexere Passwörter können sich Nutzer nur schwer merken. Sie werden deshalb häufig notiert oder nach Schemata wie „Passwort1", „Passwort2" etc. gebildet, wodurch sie ebenfalls einfacher potenziellem Missbrauch ausgesetzt sind.

Aus den Fehlern anderer lernen

Welche gravierenden Folgen der Diebstahl eines Passworts zu einer der umfangreichen Identitätsmanagement-Plattformen hat, kann sich wohl jeder ausmalen. Bereits heute berichten Nutzer von schwerwiegenden Problemen, wenn etwa ihr Google- oder Facebook-Zugang gehackt wurde. Die verknüpften Zugänge zu Plattformen wie eBay, Amazon oder Twitter lassen schwerwiegende Kompromittierungen zu, die oftmals auch noch sehr spät bemerkt werden. Deutsche Unternehmen sollten aus diesen Fehlern lernen und die nationalen Identitätsmanagement-Plattformen deutlich besser vor Missbrauch schützen. Nur dann gewinnen sie auch das Vertrauen der Nutzer.

Identitätsschutz der Zukunft nur mit Multi-Faktor-Authentifizierung

Eine wirklich lückenlose Authentifizierung digitaler Logins und Transaktionen kann nur die Multi-Faktor-Authentifizierung (MFA) gewährleisten. Bereits ihre Grundidee ist wesentlich sicherer: Statt nur einen einzigen Faktor abzufragen, werden zwei oder mehr voneinander unabhängige Berechtigungsnachweise wie Codes, Smartphone-Bestätigungen oder biometrische Nachweise verlangt. Ein Hacker, der das Passwort eines Nutzers kennt, scheitert letztlich an der Verifizierung des zweiten Faktors. Dank MFA-Technologie lassen sich digitale Identitäten zuverlässig verifizieren. Daneben schützt sie auch Transaktionen, in dem sie sicherstellt, dass diese rechtmäßig sind. Das ist gerade im Onlinebanking insbesondere vor dem Hintergrund von PSD2 und unter Berücksichtigung der Zunahme bargeldloser Bezahlungen immens wichtig. Ein weiterer Vorteil der MFA-Technologie ist das sogenannte Vier-Augen-Prinzip. Damit lassen sich besonders kritische Vorgänge im Geschäftsumfeld wie hohe Geldtransfers oder Freigabeprozesse im Bereich kritischer Infrastrukturen doppelt absichern. □

Der Autor


Bild: KeyIdentity

Dr. Amir Alsbih ist CEO von KeyIdentity, einem führenden Anbieter von Identity- und Access-Management-Lösungen. Der Doktor der Ingenieurswissenschaften im Fach Informatik hat über 15 Jahre Berufserfahrung in der IT-Security-Branche und war unter anderem IT-Sicherheitschef bei der Haufe Gruppe. Zudem dozierte er an der Albert-Ludwigs-Universität Freiburg in den Bereichen der angewandten Informationssicherheit sowie der IT-Forensik.

Als G DATA Partner von einer starken Gemeinschaft profitieren

Vertrauen zwischen einem IT-Sicherheitshersteller und seinen Kunden ist ein hohes und zu schützendes Gut. Gerade angesichts der zunehmenden Digitalisierung ist es wichtig, dass dieses Vertrauen gestärkt wird. Das neue G DATA Partnerprogramm legt den Fokus auf die Partnerentwicklung. Jeder Partner des Bochumer IT-Sicherheits-Herstellers erhält eine umfassende Unterstützung durch das erfahrene G DATA Vertriebsteam und volle Ausrichtung auf Wachstum. So entstehen lukrative Langzeitbeziehungen auf Augenhöhe.

TRUST IN GERMAN SICHERHEIT

Reseller profitieren als G DATA Partner von einer stabilen Partnerschaft. Ein vertrauensvoller Umgang miteinander und eine Kommunikation auf Augenhöhe ist eine Selbstverständlichkeit. Gemeinsam mit G DATA kann der Channel das durch immer höhere Sicherheitsanforderungen an Unternehmen entstehende Marktpotenzial ausschöpfen und seinen Netzwerkkunden zuverlässigen Schutz ihrer Ressourcen bieten. Dazu hat G DATA nicht nur seinen Vertrieb ausgebaut und neu strukturiert, sondern auch die Partnerbetreuung intensiviert. Das Ziel ist klar: G DATA will Langzeitbeziehungen zu seinen Partnern etablieren und sie weiterentwickeln.

Das neue G DATA Partnerprogramm

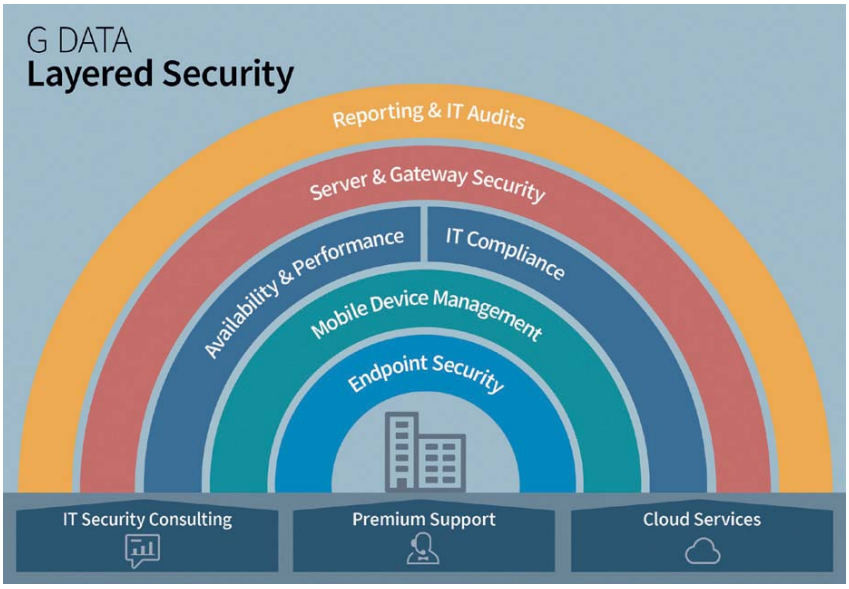
Das neue G DATA Partnerprogramm setzt genau hier an. Ein besonderer Fokus liegt auf der Partnerentwicklung. Die G DATA Partner Sales Manager sind direkte Ansprechpartner und werden die G DATA Partner als Vertriebsprofis bei allen Fragen rund um Technik, Bestellungen, Angebote und Marktsituation unterstützen. Die neue G DATA Academy bietet Partnern ein umfassendes Angebot an Produkt- und Vertriebsschulungen zu allen relevanten IT-Themen bequem als Webinar. So können Partner und ihre Mitarbeiter perfekt vorbereitet ins Rennen gehen.

Kein Neugeschäft ohne Neukunden – G DATA generiert Leads für seine Partner. Auf Messen, Roadshows und mit gezielten Aktionen finden die G DATA Vertriebsprofis Interessenten und leiten die Kontaktdaten direkt an den Partner weiter. G DATA Partner erhalten so eine passgenaue Unterstützung, um lukrative Neugeschäfte abzuschließen – inklusive Projektschutz.

G DATA bietet seinen Partnern über das Partnerportal größtmögliche Unterstützung im Tagesgeschäft. Bestellungen, Lizenzerweiterungen und -verlängerungen können jederzeit einfach und bequem über das Portal getätigt werden.

Über 30 Jahre Erfahrung in der IT-Sicherheit

Seit über 30 Jahren sorgt G DATA für Sicherheit in der digitalen Welt. Als mittelständisches Unternehmen versteht der Bochumer IT-Security-Hersteller die Bedürfnisse des Mittelstandes sehr genau und entwickelt passgenaue Sicherheitslösungen für dessen speziellen Anforderungen. Als in Deutschland ansässiger Anbieter sorgt G DATA für sichere Netzwerke – ohne Kompromisse. Unternehmen profitieren dabei von der einzigartigen, mehrschichtigen Sicherheitsarchitektur, die IT-Infrastrukturen an allen relevanten Punkten vor Angriffen schützt. „Trust in German Sicherheit“ ist dabei sowohl Leitmotiv als auch Versprechen. Vertrauen, Verlässlichkeit und ein umfassender Service und Support sind selbstverständliche Attribute, die G DATA Kunden schätzen.



G DATA bietet seinen Partnern mit dem Layered-Security-Ansatz ein umfassendes und perfekt verzahntes Sicherheitskonzept für Unternehmensnetzwerke jeder Größe.

No-Backdoor-Garantie

Bereits 2011 unterzeichnete G DATA im Rahmen der TeleTrust-Selbstverpflichtung eine „No-Backdoor“-Garantie. 2011 hat der Bundesverband IT-Sicherheit e. V. TeleTrust mit der Arbeitsgruppe „IT Security made in Germany“ (ITSMIG) eine Initiative gegründet, die Kriterien für ein Qualitätssiegel für sichere und vertrauenswürdige IT-Security-Lösungen festlegt.
Als ITSMIG-Mitglied erfüllt G DATA alle fünf Kriterien, um das Vertrauenszeichen führen zu dürfen *(siehe Artikel "Vertrauen hat einen Namen" auf Seite 6)*.

Kundendaten bleiben in Deutschland

Angesichts der großen Verunsicherung von Unternehmen und Privatanwendern stellt sich die Vertrauensfrage heute mehr denn je. Eine G DATA Umfrage unter 200 deutschen Mittelständlern hat gezeigt: 9 von 10 Unternehmer halten es für wichtig, dass IT-Security-Hersteller ihre Informationen, und damit einhergehend Kunden- und Telemetriedaten, ausschließlich in Deutschland verarbeiten. Mit der Kampagne „Meine Daten bleiben in Deutschland“ klärt G DATA auf. Dem deutschen IT-Sicherheitsanbieter ist die Privatsphäre seiner Kunden genauso wichtig, wie die Absicherung von Systemen. Von den höheren Sicherheitsanforderungen und -bedürfnissen der Unternehmen und dem entstehenden Marktpotential können Fachhändler und Systemhäuser als G DATA Partner profitieren. ■

Weitere Informationen zum G DATA Partnerprogramm finden Sie unter:
www.gdata.de/partner-werden

G DATA auf der it-sa: Halle 9, Stand 438

Was zeichnet Managed Security Services aus Deutschland aus?

Fachkräftemangel, wachsende Komplexität und neuartige Bedrohungen machen Cyber Security zu einer großen Herausforderung. Managed Security Services sind deshalb gefragt. Anbieter aus Deutschland sollten sich positionieren, die Datenschutz-Grundverordnung (DSGVO/GDPR) hilft dabei.

Von Oliver Schonschek

Digitale Transformation hat die Sicherheitslage weiter verschärft, so die IDC-Studie „IT-Security-Trends in Deutschland 2018". Doch die Unternehmen in Deutschland können oder wollen offenbar auf diese Situation nicht angemessen reagieren, meint IDC. Ein Anzeichen dafür sehen die Marktforscher darin, dass mehr als zwei Drittel der befragten Unternehmen berichten, in den letzten 24 Monaten erfolgreich attackiert worden zu sein.

Gleichzeitig besteht einiges an Nachholbedarf bei der Cyber Security in Deutschland: Laut der IDC-Umfrage verfügen nur 58 Prozent der Unternehmen über ein zentrales Konzept für Informationssicherheit, das alle Systeme und Geräte umfasst. Zwar haben insgesamt 80 Prozent damit begonnen, ihre IT-Security-Abläufe zu automatisieren, dies allerdings nur punktuell und damit unzureichend.

Gesetzliche Vorgaben, Regelwerke und Compliance-Anforderungen und der damit verbundene Datenschutz sowie die Absicherung der IT-Systeme, die in kritischen Infrastrukturen (KRITIS) betrieben werden, zwingen zu neuen Investitionen in Security, so IDC. Durch den vorherrschenden Mangel an Fachkräften für Sicherheit, Datenschutz und Compliance sind Dienstleister und Managed Security Services (MSS) dabei sehr gefragt. Das weltweite Angebot an MSS ist der hohen Nachfrage entsprechend groß. Die Suche nach der passenden Lösung und den besten Anbietern ist für die meisten Unternehmen schwierig.

IDC berichtet, dass nicht selten über 50 bis 80 unterschiedliche Security-Lösungen in einem Unternehmen im Einsatz sind, entweder als On-Premises Software-Lösung, Appliance, Security-as-a-Service oder Managed Security Service. Das spricht nicht unbedingt für eine strategische Entscheidung im Security-Bereich vieler Unternehmen.

Compliance erhöht Anforderungen und bietet Vorteile für Anbieter aus der EU

Eine strategische Entscheidung für Security-Lösungen sollte Compliance-Anforderungen berücksichtigen. Wenn Unternehmen zu Managed Security Services greifen, liegt in vielen Fällen aus Datenschutzsicht eine Auftragsverarbeitung (Artikel 28 DSGVO) vor. Anwenderunternehmen müssen bei der Wahl eines

Die DSGVO stellt hohe Anforderungen an MSS-Anbieter in Deutschland und der EU.

Security-Services daran denken, dass hierbei Datenschutzvorgaben zu beachten sind. Grundsätzlich muss der Managed Security Services Provider über ein angemessenes Datenschutzniveau verfügen.

Man kann auch sagen: Die Nutzung eines Security-Services darf nicht zum Datenrisiko werden. Tatsächlich kann dies aber der Fall sein, ohne dass sich die betroffenen Nutzer darüber im Klaren sind.

Unter „personenbezogenen Daten" versteht man nach DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung identifiziert werden kann.

Es steht außer Frage, dass solche Daten und Kennungen in den Protokolldaten enthalten sein können, die Security-Services sammeln, auswerten und speichern. Eine unzureichende Prüfung des Datenschutzes bei der Wahl eines MSS-Providers kann deshalb der Datensicherheit schaden, die man eigentlich mit dem Security-Service steigern möchte.

Anbieter von MSS aus Deutschland und der EU sollten deshalb auf die Compliance-Vorteile von MSS „Made in Germany" oder „Made in EU" verweisen. Diese Vorteile zeigen sich, wenn man die möglichen Folgen von Security-Services für den Datenschutz betrachtet.

Mögliche Datenschutzfolgen von Security-Services beachten

Beim Einsatz neuer Technologien, wozu auch neue Security-Lösungen zählen können, sieht die DSGVO Datenschutz-Folgenabschätzungen (Artikel 35 DSGVO) vor. Eine Datenschutz-Folgenabschätzung kann insbesondere dann erforderlich sein, wenn es zu einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen oder zu einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche kommt.

Dies betrifft auch Security-Lösungen und Security-Services, wie eine Veröffentlichung mehrerer Aufsichtsbehörden für den Datenschutz in Deutschland zeigt. Deren sogenannte Positivliste zur Datenschutz-Folgenabschätzung ⇨

- ist eine gemeinsam abgestimmte Liste der Verfahren, bei denen zwingend aus Sicht der jeweiligen Aufsichtsbehörde eine Datenschutz-Folgenabschätzung (DSFA) erfolgen muss.
  Beispiele für den Bedarf einer DSFA, die in der Positivliste genannt werden und Security betreffen können, sind:
  - Fraud-Prevention-Systeme
  - Einsatz von Data-Loss-Prevention-Systemen, die systematische Profile der Mitarbeiter erzeugen
  - Geolokalisierung von Beschäftigten
  - Einsatz von RFID/NFC durch Apps oder Karten

  Bei der Bewertung der Datenschutzfolgen solcher Lösungen und Services spielt es auch eine entscheidende Rolle, ob die zu schützenden Nutzerdaten (personenbezogene und personenbeziehbare Daten) womöglich in einen Drittstaat übermittelt werden sollen, also außerhalb der EU genutzt und gespeichert werden.
  In diesem Fall ist die Nutzung des Security-Services nur zulässig, sofern der Provider geeignete Garantien für den Datenschutz vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen, wie es die DSGVO formuliert.

Gemeint ist, dass der Datenschutz nachweislich bei dem Anbieter im Drittstaat das gleich hohe Datenschutzniveau erreichen muss, wie wenn die Services in der EU durchgeführt würden. Die Personen, deren Daten verarbeitet werden, müssen alle Betroffenenrechte nach DSGVO ausüben können, also etwa die Rechte auf Löschung der Daten (Recht auf Vergessenwerden), auf Auskunft, auf Einschränkung der Verarbeitung und auf Datenübertragbarkeit.

Tipp: Deutsche Anbieter sollten Standortvorteil nutzen

Anbieter von Managed Security Services aus Deutschland können und sollten auf ihr Datenschutzniveau verweisen und auf das Ausbleiben der Datenübermittlung in einen Drittstatt. Anbieter für MSS aus Deutschland bzw. der EU unterliegen direkt der DSGVO und müssen alle Betroffenenrechte umsetzen.
Diese Verpflichtungen aus der DSGVO sollten die Anbieter für Managed Security Services in Deutschland nicht als Belastung, sondern als Standortvorteil sehen. Die Compliance mit der DSGVO ist Unternehmen aus Deutschland sehr wichtig. Managed Security Services auf Basis der DSGVO sind deshalb ein Wettbewerbsvorteil auf dem Security-Markt. □

Die Verpflichtungen aus der DSGVO sollten die Anbieter für MSS in Deutschland nicht als Belastung, sondern als Standortvorteil sehen.

Wie IT-Sicherheitslösungen bei der DSGVO-Compliance helfen

Die Datenschutz-Grundverordnung (DSGVO/GDPR) und das neue Bundesdatenschutzgesetz (BDSG-neu) stellen hohe Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten. Diese lassen sich nur erfüllen, wenn wirksame, aktuelle IT-Security-Lösungen zum Einsatz kommen. Hier können Lösungen und Anbieter aus Deutschland punkten.

Von Oliver Schonschek

Wer Cloud-Anwendungen nutzt oder dies plant, für den ist Datenschutz das wichtigste Kriterium, wenn es um die Auswahl eines Cloud-Dienstleisters geht, so der Cloud-Monitor 2018 von Bitkom und KPMG. Fast alle Unternehmen (97 Prozent) gaben an, dass für sie die Konformität mit der Datenschutz-Grundverordnung bei Cloud-Lösungen unverzichtbar ist.

Folglich gilt: Wer Cloud-Services als Dienstleister anbieten möchte, muss den Datenschutz in der Cloud auf hohem Niveau gewährleisten. Der Cloud-Datenschutz setzt zwingend zuverlässige Maßnahmen für die Sicherheit der Verarbeitung voraus. Das betont auch der Verband der Internetwirtschaft eco.

Demnach muss die Sicherheit der Verarbeitung (nach Art. 32 DSGVO) grundlegend über das bisher nach altem Datenschutzrecht geforderte Sicherheitsniveau hinausgehen. Cloud-Anbieter und andere Auftragsverarbeiter müssen den hohen Sicherheitsanforderungen genügen, um überhaupt als Auftragsverarbeiter in Betracht zu kommen, wie der Verband eco erläutert. Die Frage nach der Sicherheit der Verarbeitung ist ein zentrales Kriterium für die Zulässigkeit der Verarbeitung an sich.

Im Datenschutz reicht Manpower nicht aus

Die technisch-organisatorischen Maßnahmen aus der Datenschutz-Grundverordnung gehören zu den dringenden Herausforderungen für Unternehmen, denen nur mit angemessenen Ressourcen entsprochen werden kann, so der TeleTrusT – Bundesverband IT-Sicherheit.

Cloud-Anbieter und andere Unternehmen können den Datenschutz ohne geeignete Werkzeuge nicht stemmen. Zum einen mangelt es an Datenschutzexperten. So geben sechs von zehn Unternehmen (61 %) in Deutschland an, dass die Rekrutierung von Datenschutzexperten sehr schwierig ist. Ähnlich viele Unternehmen (57 %) sagen: Der Markt für Personal im Bereich Datenschutz ist nahezu leergefegt, wie eine Befragung unter mehr als 500 Unternehmen im Auftrag des Digitalverbands Bitkom ergab. Dieser Mangel an Datenschutzfachkräften betrifft Anwenderunternehmen und IT-Dienstleister. ⇨

- Beide benötigen deshalb Security- und Datenschutz-Lösungen, die Aufgaben zuverlässig übernehmen.

Ein weiterer Punkt, der den Bedarf an geeigneten Datenschutz- und Sicherheitswerkzeugen zeigt, sind die Vorgaben der DSGVO in Artikel 32 (Sicherheit der Verarbeitung): Dort wird gefordert, dass Unternehmen und Dienstleister geeignete technische und organisatorische Maßnahmen treffen, um ein angemessenes Datenschutzniveau zu gewährleisten.

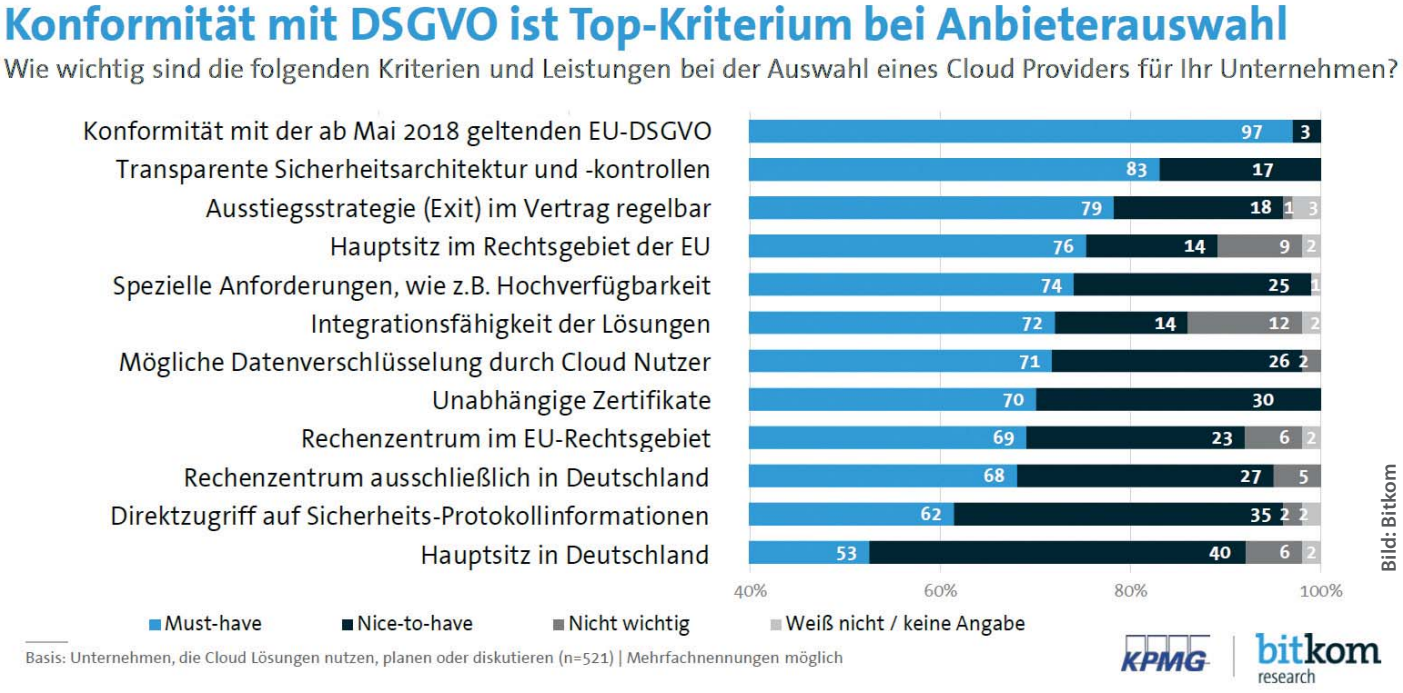
Kriterien für die Eignung hierbei sind die „Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen". Insbesondere sind also aktuelle Sicherheitsmaßnahmen auszuwählen, die dem Stand der Technik entsprechen, was für viele Unternehmen jedoch erst einmal keine leichte Aufgabe darstellt.

Zusätzlich wird ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gefordert.

Die eingesetzten Sicherheitsmaßnahmen zur Umsetzung der DSGVO müssen ihre Wirksamkeit unter Beweis stellen können, also den versprochenen Schutz für die Daten auch zuverlässig leisten.

Suche nach geeigneten Lösungen auf dem IT-Sicherheitsmarkt

Ob man Cloud-Dienste anbietet oder seinen Kunden Datenschutz-Services offerieren möchte: Für die Suche nach IT-Sicherheitslösungen, die den Vorgaben der DSGVO entsprechen, braucht man Hilfestellungen, denn der Security-Markt ist umfangreich, dynamisch



Wer Cloud-Dienste anbieten will, muss für DSGVO-Compliance sorgen, wie der Cloud-Monitor 2018 von KPMG und Bitkom zeigt. Entscheidend ist dabei insbesondere die IT-Sicherheit.

Bild: TeleTrusT

Was ist eigentlich der von der DSGVO geforderte Stand der Technik? TeleTrusT klärt mit seiner umfangreichen und aktualisierten „Handreichung zum Stand der Technik" auf: https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/

und komplex. Der TeleTrusT – Bundesverband IT-Sicherheit zum Beispiel bietet Unterstützung, wenn es um Fragen zum Stand der Technik und zur Zuverlässigkeit von Security-Lösungen geht.

So erklärt TeleTrusT: Die Datenschutz-Grundverordnung fordert für die IT-Sicherheit den Stand der Technik, doch sie lässt unbeantwortet, was im Detail darunter zu verstehen ist. Deshalb hat TeleTrusT seine Handreichung zum Stand der Technik (https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/) entsprechend überarbeitet und erweitert. Die Handreichung versteht sich als Ausgangspunkt bei der Ermittlung von gesetzlichen IT-Sicherheitsmaßnahmen.

Darüber hinaus kann das TeleTrusT-Zeichen „IT Security made in Germany" Orientierung bieten bei der Anbieter- und Lösungssuche. So gehört zu den Kriterien für die Erlangung dieses Zeichens insbesondere:

- Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.
- Die angebotenen Produkte dürfen keine versteckten Zugänge („Backdoors") enthalten.
- Der Anbieter muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen und damit seit 25. Mai 2018 der Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz.

Fazit: DSGVO-Compliance beginnt mit geeigneten Security-Lösungen

IT-Dienstleister, die Cloud-Services anbieten, müssen auch für ihren Erfolg in Kundenprojekten die Einhaltung der DSGVO sicherstellen. Dazu gehört eine wirksame IT-Sicherheit, die dem Stand der Technik entspricht. Bei der Anbietersuche helfen zum Beispiel Angebote von Branchenverbänden wie TeleTrusT. Sie ersetzen nicht die eigene Bewertung angebotener Security-Lösungen, aber sie helfen bei der Orientierung auf dem dynamischen Security-Markt und bei den hohen Anforderungen der DSGVO.

Wer als Dienstleister die DSGVO-Compliance erfüllt und die Sicherheit nachweisen kann, findet im Cloud-Markt sehr gute Geschäftschancen: Das Interesse an der Cloud ist ungebrochen hoch, wie der Cloud-Monitor 2018 belegt, der Bedarf an Cloud-Sicherheit ebenso. □

Schutzengel für persönliche Daten: Datenschutzbeauftragte

In vielen Unternehmen tun sie bereits seit Jahren ihren Dienst: Datenschutzbeauftragte. Bisher agierten sie meist im Hintergrund. Mit der verbindlichen Einführung der DSGVO im Mai 2018 rücken sie und ihr Tätigkeitsfeld allerdings stärker ins Blickfeld.

Von Petra Adamik

Mittlerweile sollte die Position des Datenschutzbeauftragten (DSB) in jedem Unternehmen besetzt sein. So sieht es die DSGVO vor. Dennoch erntet man vielfach Schulterzucken, fragt man Unternehmen nach ihrem Verantwortlichen für den Datenschutz. Gerade kleine und mittelständische Betriebe weisen hier noch erhebliche Defizite auf. Datenschutz ist vielfach immer noch das Stiefkind unter den Prozessen. Oft fehlen in diesem Segment sowohl Budgets als auch die Zeit, sich mit dem Thema zu beschäftigen und einen geeigneten Kandidaten zu bestellen. Dennoch gilt: Auch KMU sind zu Datenschutz verpflichtet. Wird er vernachlässigt oder ignoriert, gehen Betriebe ein erhebliches Risiko ein. Es drohen hohe Bußgelder und Strafen, die schnell zur wirtschaftlichen Belastung werden können.

Mit einem Datenschutzbeauftragten sind Unternehmen auf der sicheren Seite. Er hat die Aufgabe, im Unternehmen die gesetzlichen Anforderungen an den Datenschutz zu überwachen und deren Einhaltung sicherzustellen. Der DSB muss das Niveau des Datenschutzes kontrollieren, ein Konzept für ein Datenschutz-Management ausarbeiten und dafür sorgen, dass es im Betriebsablauf verankert und umgesetzt wird. Das erfordert ein detailliertes Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis. Der DSB muss dafür sorgen, dass die Datenverarbeitungsprogramme

in einem Unternehmen fachgerecht eingesetzt und verwendet werden. Deshalb muss er über umfassende IT-Kenntnisse verfügen. Nur dann ist er in der Lage zu erkennen, ob bei den IT-Prozessen die datenschutzrechtlichen Vorgaben eingehalten werden. Juristische und betriebliche Kenntnisse sind ebenfalls essenziell, um die Aufgaben entsprechend der DSGVO zu erfüllen. Darüber hinaus muss der DSB sich permanent über die aktuellen gesetzlichen Bestimmungen und etwaige Änderungen informieren. Den DSB kann ein Unternehmen aus den Reihen der eigenen Mitarbeiter ernennen. Alternativ bietet sich aber auch die Bestellung eines externen Beauftragten an. In Deutschland haben sich mittlerweile flächendeckend Beratungsunternehmen auf diese Dienstleistung spezialisiert und arbeiten mit zertifizierten Datenschutzberatern zusammen, um die Datenschutzanforderungen in den Unternehmen umzusetzen.

Soziale Kompetenz und Durchsetzungskraft sind gefordert

Aber nicht nur fachlich muss der Datenschutzbeauftragte auf der Höhe sein. Auch soziale Kompetenzen sind gefragt. Dazu gehört Integrität ebenso wie Verschwiegenheit und Kommunikationstalent. Solche persönlichen Fähigkeiten sind wichtig, um die Informations- und Beratungsaufgaben sowie die Funktion als Ansprechpartner für alle Beteiligten im Unternehmen wahrzunehmen. Wichtig ist auch ein gewisses Maß an Durchsetzungsfähigkeit, denn der DSB muss in der Lage sein, seine Stellung gegenüber der Geschäftsleitung zu wahren und notfalls auch durchzusetzen. Das gilt besonders bei der unterschiedlichen Einschätzung hinsichtlich der datenschutzrechtlichen Anforderungen an die jeweiligen Verarbeitungsvorgänge.

Die Aufgaben von Datenschutzbeauftragten sind in der Datenschutzgrundverordnung klar geregelt. Ein DSB muss ein Unternehmen über ⇨

Interner versus externer Datenschutzbeauftragter

Grundsätzlich kann ein betrieblicher Datenschutzbeauftragter (DSB) sowohl intern in Person eines Mitarbeiters als auch extern in Person eines Dienstleisters bestellt werden. Ausschlaggebendes Kriterium für die Wahl sollte stets die notwendige berufliche Qualifikation sein. Das gilt insbesondere im Hinblick auf das Fachwissen im Bereich des Datenschutzrechts und der Datenschutzpraxis.

Interner Datenschutzbeauftragter

Der interne betriebliche DSB ist ein Angestellter des Unternehmens. Er sollte alle notwendigen Anforderungen eines DSB erfüllen können, um diese Position auszufüllen. Nach der Berufung zum internen DSB steht der Mitarbeiter unter Kündigungsschutz und hat Rechte auf weitere Ansprüche, wie beispielsweise eine eigene Ausstattung oder Fortbildungen. Wird ein betrieblicher DSB bestellt, der nicht die geforderten Fähigkeiten besitzt, wird dies gesetzlich so behandelt, als sei im Unternehmen kein DSB.

Externer Datenschutzbeauftragter

Im Gegensatz zum internen DSB ist der externe DSB ein zertifizierter Datenschutzexperte, der einem Unternehmen als Dienstleister zur Verfügung steht. Die Expertise eines externen betrieblichen Datenschutzbeauftragten garantiert dabei ein Höchstmaß an Schutz. Die Kosten für die Dienstleistung werden vertraglich geregelt. Innerhalb der vereinbarten Vertragslaufzeit kümmert sich der externe Datenschutzbeauftragte um alle Aspekte des Datenschutzes und sorgt für die Einhaltung der Regeln.

Quelle: Datenschutzexperte.de

Die sozialen Kompetenzen eines DSB müssen vielfältig sein, auch muss er sich gegenüber der Geschäftsleitung durchsetzen können.

- die Einhaltung der DSGVO und anderer Vorschriften zum Datenschutz unterrichten (Art. 39ff DSGVO). Allerdings bedeutet dies nicht, dass er auch selbst für die Umsetzung der Vorschriften verantwortlich ist. Die Aufgaben eines Datenschutzbeauftragten werden in Artikel 38 und Artikel 39 DSGVO geregelt. Typische Aufgaben sind unter anderem:
  - Überprüfung des allgemeinen IT-Sicherheitskonzepts
  - Überprüfen, ob die Mitarbeiter ausreichend über das Datengeheimnis sowie die Regeln zum Datenschutz informiert sind und diese auch umsetzen
  - Kontrolle der technischen und der organisatorischen Maßnahmen zum Datenschutz
  - Überprüfung von Verzeichnissen, in denen Verarbeitungstätigkeiten protokolliert werden
  - Erstellung jährlicher Tätigkeitsberichte
  - Unterstützung bei der Ausarbeitung eines Daten-Löschkonzepts
  - Kooperation mit den Aufsichtsbehörden

Um alle Aufgaben im Umfeld des Datenschutzes erfüllen zu können, muss ein Datenschutzbeauftragter sämtliche Datenschutzregelungen und deren Auslegung kennen. Gefordert ist auch das Wissen um alle bereichsspezifischen Spezialnormen sowie über Vereinbarungen mit den Arbeitnehmervertretungen.

Bei der Haftung gibt es Unterschiede zwischen externen und internen DSB. So haftet ein externer Datenschutzbeauftragter in vollem Umfang für die Erfüllung sämtlicher Aufgaben und vertraglich vereinbarter Pflichten. Ist intern ein Arbeitnehmer mit den Aufgaben eines DSB betraut, gelten dagegen die Grundsätze der beschränkten innerbetrieblichen Arbeitnehmerhaftung. In diesem Fall haftet der Arbeitnehmer lediglich bei Vorsatz und grober Fahrlässigkeit in vollem Umfang. Bei leichter Fahrlässigkeit scheidet eine Haftung des internen Datenschutzbeauftragten aus. □

Ein Blick auf die Bußgeldvorschriften

Die Einzelheiten rund um Verstöße und die damit in Verbindung stehenden Bußgelder sind in der DSGVO und im Bundesdatenschutzgesetz – BDSG (neu) – festgehalten. Einzelheiten in Bezug auf konkrete Sanktionen sind zum Beispiel den §42 und §43 BDSG (neu) zu entnehmen. Während ersterer die sogenannten Strafvorschriften regelt, bestimmt §43 die Bußgeldvorschriften. Diese besagen, dass ein Verstoß gegen den Datenschutz mit einer Freiheitsstrafe von bis zu drei Jahren geahndet werden kann. Die Bußgeldvorschriften des BDSG (neu) benennen Verstöße, die mit bis zu 50.000 Euro geahndet werden können. Die DSGVO benennt in Artikel 83 Verstöße, die mit Geldbußen von bis zu 20.000.000 Euro oder im Fall eines Unternehmens von bis zu 4 Prozent des gesamten Jahresumsatzes des letzten Geschäftsjahres bestraft werden können.

Strategien – Technologien – Best Practices – Networking

ENTERPRISE MOBILITY SUMMIT 2018

18./19. Oktober • Villa Kennedy • Frankfurt a. M.

MOBILE DRIVES BUSINESS

Mobility-Strategie

User Integration

Management

Security

Jetzt anmelden! www.em-summit.de

Eine Veranstaltung der VOGEL IT AKADEMIE

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: Wilfried Platten/pl (-106) – Chefredakteur, 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: Dagmar Schauer (-202)

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

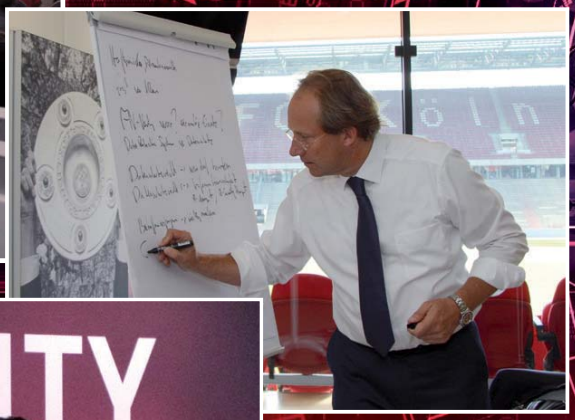
Vogel IT-Medien, Augsburg, ist eine 100prozentige Tochtergesellschaft der **Vogel Communications Group**, Würzburg, einem der führenden deutschen Fachinformationsanbieter mit 100+ Fachzeitschriften, 100+ Webportalen, 100+ Business-Events sowie zahlreichen mobilen Angeboten und internationalen Aktivitäten. 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.

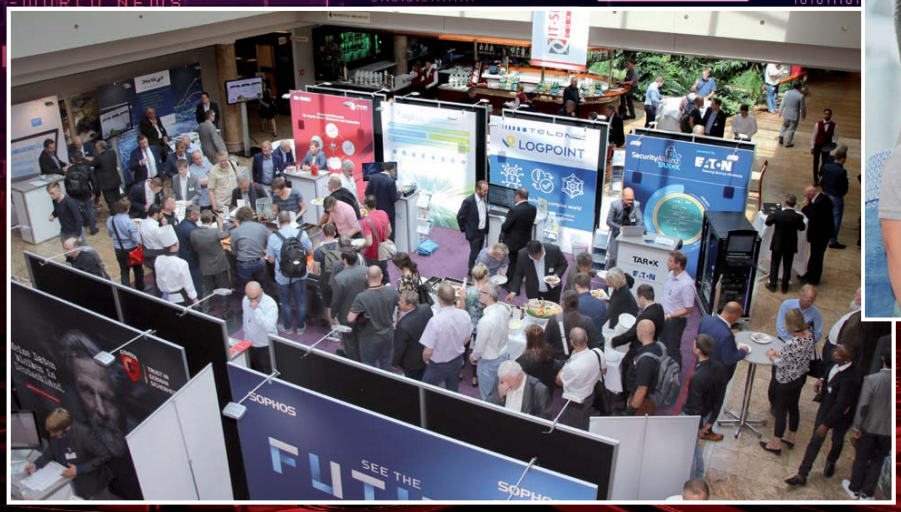
Die wichtigsten Angebote des Verlages sind **IT-BUSINESS, eGovernment Computing, IP-Insider.de, Security-Insider.de, Storage-Insider.de, CloudComputing-Insider.de, DataCenter-Insider.de, Dev-Insider.de** und **BigData-Insider.de.**

Inserenten

G DATA Software AG	Bochum	https://www.gdata.de/	2, 38, 39
NCP engineering GmbH	Nürnberg	https://www.ncp-e.com/de/	26, 27, 52
Net at Work GmbH	Paderborn	https://www.netatwork.de	14, 15
netfiles GmbH	Burghausen	https://www.netfiles.de/	8, 9
retarus GmbH	München	https://www.retarus.com/de/	34, 35
secunet Security Networks AG	Essen	https://www.secunet.com/	5, 13
Vogel IT-Akademie	Augsburg	http://www.akademie.vogel-it.com/	49, 51

Save the Date





Eine Veranstaltung der VOGEL IT AKADEMIE

IT-SECURITY
MANAGEMENT & TECHNOLOGY
CONFERENCE 2019

Geplante Termine und Orte:

Juni 2019	Raum Frankfurt
25.06.2019	Köln
04.07.2019	Garching
09.07.2019	Hamburg

» Jetzt vormerken unter **www.itsecurity-conference.de**

NCP
SECURE COMMUNICATIONS

IT Security für Industrie 4.0

Wir haben, worüber andere nur reden!

Fertige Lösungen für die sichere Kommunikation im Bereich Industrie 4.0. Wir helfen Ihnen Ihre Produktions- und Produkt-IT mit Ihrer klassischen Unternehmens-IT zu verbinden. Weltweit einmalig.

Secure Communications für Ihr Unternehmen.

Secur IT y
made in Germany

INDUSTRIE PREIS 2018 BEST OF

Best of Industry 4.0 Security:
NCP Secure IIoT Solution

www.ncp-e.com