Verlagsbeilage, Oktober 2018

‹kes›

Die Zeitschrift für Informations-Sicherheit

special

E-Mail-Security: Schutz vor Advanced Threats

S. 26

Statt Chipkarte: Das Smartphone als Sicherheits-schlüssel

S. 34

it-sa 2018

Trends, Produkte und Lösungen

DATAKONTEXT

IT-SECURITY? WAR GESTERN. WIR MACHEN SECURE IT.

Sie packen Security in DevOps-Projekte oder Industrial-IT? Analysieren Threats? Oder wissen, wie die beste Security-Strategie für Morgen aussieht? Dann werden Sie Teil unserer großen Security-Community von über 160 Kolleginnen und Kollegen – allein bei Computacenter in Deutschland.

Seit zwanzig Jahren unterstützen wir als Europas führender herstellerübergreifender IT-Dienstleister unsere Kunden bei Beratung, Planung, Umsetzung und Betrieb einer sicheren IT. Zu unseren Kunden zählen globale und lokale Unternehmen – darunter mehr als die Hälfte der DAX-30-Unternehmen – die aus allen Branchen kommen: Automotive, Chemie, Energie, Finanz, Pharma oder öffentliche Auftraggeber. Unser Security-Portfolio ist eines der breitesten auf dem deutschen Markt und umfasst u. a.:

- Cyber Defence
- Endpoint Security
- Infrastructure Security
- Industrial Security
- Identity & Access Management
- Information Security Management
- Cloud Security

Regelmäßige Weiterbildungen und Herstellerzertifizierungen sind bei uns selbstverständlich. Genauso wie Zusammenhalt und Hilfsbereitschaft unter den Kollegen. Bei uns geht es um Technologie, aber vor allem um Menschen. Nicht umsonst lautet unser Motto **„WINNING TOGETHER“: Denn der Weg nach vorne gelingt nur gemeinsam.**

Interesse? Dann nichts wie los!
Weitere Informationen gibt’s auf unserer Website www.computacenter.de/karriere

Nichts Passendes dabei? Dann freuen wir uns auch über Initiativbewerbungen!

Kostenlose Karrierehotline +49 800 4682326

Security
Services & Solutions
Leader Germany
2018
ISG Provider Lens

Herzlich willkommen zur it-sa 2018!

Digitalisierung ist kein Selbstläufer: Fortschritt und Nutzen stehen Risiken und Herausforderungen gegenüber. Wenn immer mehr Daten erhoben, wenn Unternehmensnetze immer engmaschiger verflochten und selbst Herzschrittmacher digital angesteuert werden, steht vor allem eines auf dem Spiel: Vertrauen.

Klar ist: Die Aufgaben für IT-Sicherheitsverantwortliche wachsen. Um im Wettrennen gegen Cyberkriminelle zu bestehen, ist mehr denn je Know-how gefragt. Aber auch der persönlichen Vernetzung und dem Erfahrungsaustausch kommt eine immer wichtigere Rolle zu. Vom 9. bis 11. Oktober macht die it-sa das Messezentrum Nürnberg deshalb wieder zur Dialogplattform für IT-Sicherheitsexperten.

Rund 700 Aussteller, fünf offene Foren mit etwa 350 Vorträgen und das noch einmal umfangreichere Kongressprogramm machen die it-sa 2018 zur größten it-sa, die es je gab. Neben Unternehmen aus europäischen Ländern stellen Firmen aus Asien und natürlich den USA aus. Israel, die Niederlande und die Tschechische Republik zeigen sogar mit Länderpavillons Flagge. Mit etwa 500 deutschen Ausstellern unterstreicht die it-sa gleichzeitig, dass sie die Heimat der starken deutschen IT-Sicherheitsbranche ist. Experten aus allen Wirtschaftszweigen bietet die it-sa damit sowohl IT-Security-Lösungen „made in Germany“ als auch vielfältige Perspektiven auf die internationale IT-Sicherheitslandschaft.

Unter dem Dach von Congress@it-sa finden gleichermaßen hochkarätige nationale wie internationale Veranstaltungen statt: Dazu zählen der IT-Grundschutz-Tag und die Jahrestagung der IT-Sicherheitsbeauftragten in Ländern und Kommunen. Hinzu kommt in diesem Jahr das Symposium VIS!T „Verwaltung integriert sichere Informationstechnologie“ für IT-Sicherheitsexperten aus der Verwaltung in Deutschland, Österreich, der Schweiz und Luxemburg.

Nutzen auch Sie die it-sa zum Dialog und tauschen sich mit ihren Mitstreitern aus – für eine mit Sicherheit vertrauenswürdige Digitalisierung.

Ich freue mich darauf, Sie zu begrüßen.

Ihr
Frank Venjakob, Executive Director it-sa, NürnbergMesse

it-sa 2018:

IT-Sicherheit von A bis Z

Forenprogramm

NEVIS

Win time – choose us

Die Digitalisierung wartet nicht. Wie weit sind Sie?

Gewinnen Sie Zeit und nutzen Sie smarte, agile und mobile Lösungen von NEVIS.

Besuchen Sie uns an der **it-sa 2018** und erfahren Sie, wie NEVIS Sie schneller und sicherer zu Ihren Kunden bringt.

it sa 2018

Die IT-Security Messe und Kongress

HALLE 10.0
STAND 10.316

Nürnberg, 9.–11. Oktober

www.nevis-security.de/itsa-2018

Partner

Attemptum AG

BehavioSec

FSP SOFTWARE & CONSULTING Wettbewerbsvorteile aus einer Hand.

syracom

9. bis 11. Oktober

it-sa 2018: IT-Sicherheit von A bis Z

Die it-sa findet dieses Jahr zum zehnten Mal im Messezentrum Nürnberg statt. Mit rund 700 Ausstellern aus 26 Ländern, mittlerweile fünf offenen Foren und dem noch einmal umfangreicheren Kongressprogramm deckt sie das Thema IT-Sicherheit wieder von A bis Z ab. IT-Sicherheitsexperten und Entscheider aus allen Branchen bietet die it-sa damit einen einzigartigen Marktüberblick und Know-how zum Schutz vor Wirtschaftsspionage, Datenklau oder Cyber-Erpressung.

Von Thomas Philipp Haas, NürnbergMesse GmbH

In diesem Jahr werden noch einmal deutlich mehr Aussteller als in den letzten Jahren vertreten sein: Rund 700 Unternehmen präsentieren in den Hallen 9, 10.0 und 10.1 die ganze Bandbreite moderner IT-Sicherheitslösungen. „Von A wie APT-Abwehr bis Z wie Zertifizierung reicht das Angebotsspektrum der beteiligten Firmen auf der Fachmesse. In Verbindung mit dem begleitenden Kongress ist die it-sa damit die zentrale Dialogplattform der Branche und die beste Adresse für alle, die ihr Unternehmen schützen wollen“, erklärt Frank Venjakob, Executive Director it-sa, NürnbergMesse.

Bis zum Redaktionsschluss dieses Heftes haben sich Aussteller aus 26 Ländern zur it-sa 2018 angemeldet. Darunter sind Unternehmen aus Asien sowie zahlreiche Firmen aus den USA. Mit rund 500 Anmeldungen aus Deutschland zeigt die it-sa aber auch, dass sie die Messeheimat der starken deutschen IT-Sicherheitsindustrie ist. Erneut beteiligen sich drei Nationen mit eigenen Gemeinschaftsständen: Israel, die Niederlande und die Tschechische Republik. Der israelische Gemeinschaftsstand ist in Halle 9 zu finden. Fachbesucher finden hier unter anderem spezialisierte Anbieter für Netzwerk-Monitoring in industriellen Produktionsumgebungen, Intrusion-Detection oder Denial-of-Service-Abwehr und junge Firmen, die auf das internationale IT-Sicherheitsparkett drängen. Mit insgesamt 27 israelischen Ausstellern ist die Messebeteiligung der „Start-up Nation“ höher als in den Vorjahren.

In Halle 10.1 demonstrieren tschechische Unternehmen mit einem eigenen Pavillon ihre Kompetenz. Sie informieren beispielsweise über Netzwerk-Monitoring oder Advanced-Persistent-Threat-Protection. Insgesamt nehmen neun tschechische Unternehmen an der Messe teil.

Zum ersten Mal präsentieren sich auf der it-sa auch niederländische Firmen mit einem gemeinsamen Messeauftritt. Der niederländische Pavillon ist in Halle 10.0 zu finden. Im Mittelpunkt stehen hier unter anderen die Themen Security-Awareness und Managed-Security. Es beteiligen sich dieses Jahr 15 niederländische Unternehmen an der it-sa.

„Die internationalen Gemeinschaftsstände sind eine beliebte Anlaufstelle für den Dialog über Ländergrenzen hinweg. Sie unterstreichen auch die Bedeutung der grenzüberschreitenden Zusammenarbeit und zeigen, wie dynamisch die weltweite IT-Sicherheitsindustrie wächst“, erklärt Frank Venjakob.

Alle Aussteller und aktuelle Produktinformationen:
www.it-sa.de/aussteller-produkte

Übersicht zum Rahmenprogramm und Congress@it-sa:
www.it-sa.de/rahmenprogramm

Informationen zu UP18@it-sa:
www.it-sa.de/up18

Die App zur it-sa 2018:
www.it-sa.de/app

Neue offene Foren

Ein Markenzeichen der it-sa sind die beliebten offenen Foren. Nachdem mit dem letztjährigen Umzug ihre Umbenennung einherging, ergänzt jetzt ein fünftes Forum

die bekannten Vortragsblöcke zu Management und Technik. Besonderheit im neuen Forum I10, das in Halle 10.1 zu finden ist: Hier wird nur Englisch gesprochen. „Damit bieten wir Besuchern aus dem Ausland, exportorientierten Ausstellern und internationalen Organisationen eine zusätzliche Plattform“, erklärt Frank Venjakob. Im Forum I10 tritt beispielsweise Professor Udo Helmbrecht, Executive Director der Europäischen Agentur für Netz- und Informationssicherheit ENISA, als Redner auf. Der Titel seines Vortrags am Dienstag, den 9. Oktober: „Innovative solutions to enhance cybersecurity in Europe“.

Die Foren M9 und M10 in Halle 9 und Halle 10.1 richten sich vor allem an die Managementebene. Die Vorträge vermitteln das notwendige Fachwissen, um IT-Sicherheitsfragen aus einer managementorientierten Perspektive einzuordnen. Konkrete technische Ansätze für mehr IT-Sicherheit stehen in den Foren T9 und T10 in den Hallen 9 und 10.0 im Mittelpunkt.

Paula Januszkiewicz hält Keynote

Die Special-Keynote der it-sa spricht die IT-Sicherheitsexpertin Paula Januszkiewicz. In ihrem Vortrag “Attacks of the Industry: A View into the Future of Cybersecurity” geht die gebürtige Polin der Frage nach, welche Schwachstellen und Fehlkonfigurationen in komplexen IT-Infrastrukturen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bedrohen. Die Gründerin der global operierenden IT-Sicherheitsberatung CQURE zeigt mögliche Einfallstore für Spionage oder Sabotage auf und gibt Tipps für die Optimierung der IT-Sicherheit in Unternehmen und Organisationen. Paula Januszkiewicz wurde als Microsoft Enterprise Security MVP ausgezeichnet und zählt zu den wenigen Personen weltweit, die Zugang zu einem Quellcode von Windows haben. Sie spricht am Donnerstag, dem 11. Oktober, im Forum I10.

Neue Bühne für Start-ups: UP18@it-sa

Mit einem neuen Veranstaltungsformat richtet sich die it-sa dieses Jahr erstmals gezielt an Start-ups aus der IT-Sicherheitsindustrie. UP18@it-sa bringt bereits am Vortag der Messe 18 von einer Fachjury ausgewählte junge Unternehmen mit Branchengrößen, potenziellen Investoren und Förderern zusammen. In einem Speed-Pitching präsentieren die jungen Gründer ihre Geschäftsmodelle und Produktinnovationen. Der Sieger des UP18@it-sa-Award wird im Publikumsentscheid gekürt. „Mit dem Award wollen wir Cybersecurity-Start-ups zu mehr Sichtbarkeit, Anerkennung und Markterfolg verhelfen“, erläutert Mit-Initiator Philipp S. Krüger, Managing Director des Digital Hub Cybersecurity in Darmstadt. Sandra Wiesbeck, als Vorstandsvorsitzende des Bayerischen IT-Sicherheitsclusters ebenfalls Initiatorin und Jurymitglied, verweist auf den Netzwerkgedanken: „Wir bieten innovativen Start-ups dafür die Plattform, die sie verdienen.“ Auf der it-sa präsentieren sich junge Unternehmen dann wie gewohnt auf der Sonderfläche Startups@it-sa. Zusätzlich teilen sie am Dienstag, dem 9. Oktober, in gesondert ausgewiesenen Beiträgen im Forum T10 ihr Wissen.

Zur it-sa 2017 kamen 630 Aussteller und 12780 Besucher. Dieses Jahr werden 700 Aussteller erwartet. Bild: NuernbergMesse / Thomas Geiger

Congress@it-sa

Was bedeutet der Fachkräftemangel für die Ausrichtung von IT-Sicherheitsabteilungen? Wie regelt die EU-Datenschutz-Grundverordnung die Haftung beim Einsatz neuer Technologien? Auf diese und weitere Fragen finden Entscheider und IT-Sicherheitsexperten bei Congress@it-sa Antworten. In insgesamt 19 teils mehrtägigen Vortragsreihen informieren Unternehmen und Organisationen ab dem 8. Oktober im begleitenden Kongressprogramm. Erstmals macht das internationale Symposium VIS!T „Verwaltung integriert sichere Informationstechnologie“ in Nürnberg Station, das sich an IT-Sicherheitsexperten aus der Verwaltung in Deutschland, Österreich, der Schweiz und Luxemburg richtet. Auch in diesem Jahr finden sowohl der IT-Grundschutz-Tag des Bundesamtes für Sicherheit in der Informationstechnik als auch die Jahrestagung der IT-Sicherheitsbeauftragten in Ländern und Kommunen unter dem Dach von Congress@it-sa statt. Die Verleihung des siebten Deutschen IT-Sicherheitspreises erfolgt am 9. Oktober erstmals auf der it-sa. Im Rahmen des Forenprogramms stellen die Finalisten ihre Innovationen zuvor im Forum T9 vor.

it-sa – auf einen Blick

Öffnungszeiten (Fachmesse)

Dienstag und Mittwoch	09:00 – 18:00 Uhr
Donnerstag	09:00 – 17:00 Uhr

Eintritt

Tageskarte: EUR 35
Dauerkarte: EUR 65

T9 – Technik Forum (Halle 9)

Dienstag 09. Oktober

09:45 Uhr it-sa insights: BMWi - Vorstellung der Bundesinitiative „IT-Sicherheit in der Wirtschaft" und ihre Ziele und Angebote
Ministerialrat Frank Fischer, Leiter der Bundesinitiative „IT-Sicherheit in der Wirtschaft" und des Referates Mittelstand-Digital, Bundesministerium für Wirtschaft und Energie (BMWi)

10:00 Uhr Kaspersky - Sicherheit fängt im Kopf an - mit den Online Awareness Trainings von Kaspersky Lab
Mike Ritter - Channel Sales Manager / Kaspersky Labs GmbH

10:15 Uhr Juniper - Sharing is Caring: Highlights of Cyber Threat Intelligence Exchange
Aviram Zrahia - Security Evangelist / Juniper Networks GmbH

10:30 Uhr DriveLock - Smart AppGuard – Einfach sicher!
Mario Schwalm - Senior Manager PreSales / DriveLock SE

10:45 Uhr Thales - Datenverschlüsselung in der Cloud: Datensicherheitslösungen für (Multi-)Cloud-Umgebungen
Bernd Stamp - Technical Lead DACH / Thales

11:00 Uhr Hitachi Vantara - Hitachi Smart Spaces & Video Intelligence - Data Driven Decisions
Nigel Fenton / Hitachi Vantara GmbH

11:15 Uhr Cylance - Künstliche Intelligenz gegen Hacker und Malware - Hype oder Wirklichkeit?
Jan Tietze - Senior SE für die DACH-Region / Cylance

11:30 Uhr Tech Data - Thema: siehe www.it-sa.de

11:45 Uhr Arcserve - Backup und IT-Security: Auf die richtige Datensicherung kommt es an!
Ugur Yildir - PreSales Consultant / Arcserve

12:00 Uhr F-Secure - Von echten Menschen und Maschinen – Künstliche Intelligenz
Florian Kellermann - Sales Engineer / F-Secure GmbH

12:15 Uhr Nuvias Wick Hill - Thema: siehe www.it-sa.de
Nuvias Deutschland GmbH

12:30 Uhr SpyCloud - Acting Early and First: Operationalizing Compromised Credentials for Improved Security
Chip Witt - Head of Product Strategy / SpyCloud Inc.

12:45 Uhr Nuvias Wick Hill - Thema: siehe www.it-sa.de
Nuvias Deutschland GmbH

13:00 Uhr ITConcepts - Go:Roles: IDM unabhängiges Rollenmanagement
Marcus Westen - Business Development IT Security / ITConcepts Professional GmbH
Karl-Heinz Huber - Senior Solution Architect, Product Architect / ITConcepts Professional GmbH

13:15 Uhr Forcepoint - Dynamisch Skalierbare Firewall Lösungen der nächsten Generation
Denis Erk - Principal Field Sales Account Manager / Forcepoint

13:30 Uhr it-sa insights: Der Countdown läuft – Vorstellung der 10 Nominierten für den 7. Deutschen IT-Sicherheitspreis
Horst-Görtz-Stiftung - HGS

14:15 Uhr noris network - Vermeiden Sie Ressourcen-Engpässe und Schatten-IT durch die Enterprise Cloud von noris network
Johannes Wagner - Principal Enterprise Virtualization Engineer / noris network AG

14:30 Uhr MobileIron - UEM: The security architecture for modern work
Manuel Melkonian - Channel Manager / MobileIron

14:45 Uhr Paessler - IoT ganz einfach – All ihre „Dinge" auf einen Blick mit LPWAN und Monitoring
Christian Zeh - Presales Systems Engineer / Paessler - PRTG Network Monitor

15:00 Uhr Compass - Was ist bei der Planung von IT-Sicherheitsprüfungen zu beachten?
Jan-Tilo Kirchhoff - Geschäftsführer / Compass Security Deutschland GmbH

15:15 Uhr Magelan-ESET - Erfolgsfaktor IT-Security: Die neuen ESET Business-Lösungen
Christoph Thurm - Product Manager / ESET Deutschland GmbH

15:30 Uhr Dimension Data/NTT Group - Industrial Security – Securing your production environment
David Weber - Senior Security Solutions Architect / Dimension Data Germany AG & Co. KG

15:45 Uhr Nuvias Wick Hill - Thema: siehe www.it-sa.de
Nuvias Deutschland GmbH

16:00 Uhr KeyIdentity - Moderne Identitäten durchbrechen alte Muster
Rainer Endres - Head of Product Management / KeyIdentity GmbH

16:15 Uhr TREND MICRO - DevOps - Schutz mit Deep Security. Sicher entwickeln. Schnell liefern. Überall ausführen.
Stefan Rehberg - Technical Consultant / TREND MICRO Deutschland GmbH

16:30 Uhr Exclusive Networks - Thema: siehe www.it-sa.de
N.N. / Exclusive Networks Deutschland GmbH

16:45 Uhr BeyondTrust - Die fünf tödlichen Sünden von privileged Access Management
Mirco Rohr / BeyondTrust

17:00 Uhr Live-Hacking NSIDE ATTACK LOGIC - Red Team Assessments: Durchführung professioneller Angriffssimulationen
Sascha Herzog - Technischer Geschäftsführer / NSIDE ATTACK LOGIC GmbH

Mittwoch 10. Oktober

09:20 Uhr Live-Hacking: cirosec - Schwachstellen in industriellen Steuerungsanlagen am Beispiel eines Hochregallagers
Stefan Strobel - Geschäftsführer / cirosec GmbH
Max Bauert / cirosec GmbH

09:45 Uhr Sophos - Synchronized Security: Moderne Bedrohungen im Team ausschalten
Michael Veit - Technology Evangelist / Sophos Technology GmbH

10:00 Uhr Forescout - See – Control – Orchestrate; Agentenlose Visibilität, IoT-Sicherheit und Incident Response
Markus Handte - Director Systems Engineering EMEA / ForeScout Technologies Inc.

10:15 Uhr Palo Alto - Magnifier Verhaltens Analyse - Erkennen und stoppen Sie gut getarnte Netzwerkbedrohungen
Martin Schauf - Manager Systems Engineering / Palo Alto Networks GmbH

10:30 Uhr Qualys - The Art of Vulnerability Management: Vom Scannen zum Managen von Risiken
Thomas Wendt - Regional Manager Post-Sales, DACH / Qualys GmbH

10:45 Uhr Imperva - Wie kann man sensible Geschäftsdaten in einer hybriden Umgebung absichern?
Walo Weber - Sales Engineering Manager / Imperva UK Ltd

11:00 Uhr Tenable - Quantifizierung des Zeitvorteils von Angreifern
Jens Freitag - Security Specialist / Tenable Network Security GmbH

11:15 Uhr Barracuda - Die notwendige Evolution von Next-Generation Firewalls zu Cloud-Generation Firewalls
Dr. Klaus Gheri - VP & GM Network Security / Barracuda Networks AG

11:30 Uhr Allegro Packets - Netzwerkprobleme aufspüren - Allegro Network Multimeter vereinfacht das Troubleshooting
Klaus Degner - Geschäftsführer / Allegro Packets GmbH

11:45 Uhr Samsung - Mobile Endgeräte der Bundespolizei in einer sicheren Betriebsumgebung (Android/Samsung Knox/ Airwatch)
Nima Baharian-Shiraz - Technical Account Manager / Samsung Electronics GmbH
Ralf Böhr - Regierungsoberamtsrat, Projektleiter MDM / Bundespolizei

12:00 Uhr noris network - Digitalisierung - neue Risiken und die passenden Gegenmaßnahmen
Julian Fay - Team Lead Presales / noris network AG

12:15 Uhr IBS Schreiber - LIVE Hacking SAP HANA - Welche Angriffs-Szenarien gibt es?
Dipl.-Geophys. Konstantin Gork - Auditor & Consultant IT Security / IBS Schreiber GmbH
Thomas Tiede - Geschäftsführer / IBS Schreiber GmbH

12:30 Uhr ectacom - Wie SICHER ist SICHER?
Ermin Ramic - Lead CyberSecurity Solutions Consultant / ectacom GmbH

12:45 Uhr itWatch - Abwehr modernster Angriffe durch Datenwäsche/SanITizing
Ramon Mörl - Geschäftsführer / itWatch GmbH

13:00 Uhr it-sa insights: Security lässt sich schulen: Möglichkeiten und Grenzen der IT-Weiterbildung im Bereich Security
Dr. Frank Simon - Leiter Cybersecurity / Zürich Versicherung
Dr. Jürgen Großmann - Projektleiter Geschäftsbereich SQC / Fraunhofer-Institut für offene Kommunikationssysteme
Moderator
Dr. Nabil Alsabah - Bereichsleiter IT-Sicherheit / Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

13:30 Uhr Kaspersky - Security aus der Cloud für MS Office 365 und Endgeräte
Peter Neumeier - Head of Channel Germany / Kaspersky Labs GmbH

13:45 Uhr G DATA - Tausend und eine Baustelle im Mittelstand 4.0 – Effiziente und sichere IT ist kein Märchen
Matthias Koll - Senior Sales Engineer / G DATA Software AG

14:00 Uhr LogPoint - Aktive Abwehr ist ein Muss! Mehr Sicherheit, durch mehr Sichtbarkeit!
Florian Schmidt - Security Consultant DACH / LogPoint GmbH

14:15 Uhr Thales - Encrypt Everything: Datensicherheit durch Verschlüsselung
Michael Loger - Senior Sales Engineer / Thales

14:30 Uhr Aruba - Wenn der Angreifer von innen kommt - nutzen Sie die integrierte Edge Security der Netzwerkinfrastruktur
Jochen Müdsam - Channel System Engineer / ARUBA, a Hewlett Packard Enterprise company

14:45 Uhr TÜV SÜD - TÜV Hessen: Operatives Cyber Risk Management
Christian Weber / TÜV SÜD AG

15:00 Uhr Nuvias Wick Hill - Thema: siehe www.it-sa.de
Nuvias Deutschland GmbH

15:15 Uhr F-Secure - Von echten Menschen und Maschinen – Künstliche Intelligenz
Florian Kellermann - Sales Engineer / F-Secure GmbH

15:30 Uhr it-sa insights: Verleihung der it security Awards 2018
Moderator
Ulrich Parthier - Geschäftsführer / IT-Verlag für Informationstechnik GmbH

16:00 Uhr Nuvias Wick Hill - Thema: siehe www.it-sa.de
Nuvias Deutschland GmbH

16:15 Uhr OneTrust - Entwicklung eines DSGVO-gerechten 72-Stunden-Aktionsplans für Vorfälle und Datenschutzverletzungen
Robert Sindlinger - GDPR Solutions Expert / OneTrust

16:30 Uhr Varonis - 7 bewährte Vorgehensweisen für Datensicherheit in hybriden Umgebungen
Matthias Schmauch - Enterprise Sales Representative / Varonis Systems

16:45 Uhr Watchguard - So einfach wie noch nie – Multifaktor-Authentifizierung mit AuthPoint
Michael Haas - Area Sales Director Central Europe / WatchGuard Technologies, Inc.

17:00 Uhr Live-Hacking: if(is)
Chris Wojzechowski - Wissenschaftlicher Mitarbeiter / if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule
Matteo Cagnazzo - Projektleiter Gesundheitswesen / if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule

Donnerstag 11. Oktober

09:30 Uhr Live Hacking NSIDE ATTACK LOGIC - Wie Hacker unter dem Radar bleiben: Umgehung aktueller Sicherheitstechnologien
Rafael Fedler - Security Analyst / NSIDE ATTACK LOGIC GmbH

10:00 Uhr Arcserve - Schutz genießt oberste Priorität. E-Mail-Archivierung für Backup-Lösungen ein wichtiger Beitrag
Rüdiger Frank - Distribution Account Manager D-A-CH / Arcserve

10:15 Uhr Forcepoint - Dynamisch Skalierbare Firewall Lösungen der nächsten Generation
Denis Erk - Principal Field Sales Account Manager / Forcepoint

10:30 Uhr DriveLock - Der smarte Weg Ihre Daten zu schützen
Falk Trümner - Senior PreSales Consultant / DriveLock SE

10:45 Uhr Exclusive Networks - Thema: siehe www.it-sa.de
N.N. / Exclusive Networks Deutschland GmbH

11:00 Uhr sysLogixx - Syncronisierte Sicherheit, vom Client bis in die Cloud mit Sophos Synchronized Security
Mathias Fränzl - System Engineer / sysLogixx GmbH

11:15 Uhr Vade Secure - Bis 2020 werden 50% der Office-365-Kunden auf Drittanbieter Email-Sicherheitslösungen zurückgreifen
Marcin Romanowski - Channel Manager Europe / Vade Secure

11:30 Uhr NTT Security/NTT Group - Verschlüsselung für die Cloud? Ja, aber sicher – als Service!
Frank Balow - Manager CC Identity & Key Management / NTT Security (Germany) GmbH

11:45 Uhr SANS Institute - Thema: siehe www.it-sa.de
N.N. / SANS Institute

12:00 Uhr F-Secure - Von echten Menschen und Maschinen – Künstliche Intelligenz
Florian Kellermann - Sales Engineer / F-Secure GmbH

12:15 Uhr Paessler - Wenn Skripting kein Muss, sondern ein Kann für Monitoring ist
Gabriel Fugli - Senior Account Manager / Paessler - PRTG Network Monitor

12:30 Uhr Sophos - Künstliche Intelligenz– Stärken und Schwächen einer gehypten Technologie
Michael Veit - Technology Evangelist / Sophos Technology GmbH

12:45 Uhr Skybox - Angriffsflächenvisualisierung: Oder wie wollen Sie etwas schützen, das Sie gar nicht kennen?
Carlos Heller - Technical Director / Skybox Security Inc.

13:00 Uhr NTT Data/NTT Group - The Sec between Dev and Ops – Ein Überblick über relevante Sicherheitsmaßnahmen in DevOps-Ansätzen
Maximilian Siegert - Business Development Manager, IT Security Solution Sales / NTT DATA Deutschland GmbH

13:15 Uhr KPMG - Sind Ihre Industrieanlagen sicher?
Thomas Gronenwald - Prokurist und Senior Manager Cyber Security / KPMG AG Wirtschaftsprüfungsgesellschaft

13:30 Uhr EgoSecure/Matrix42 - Wie definiert man eine „einfach schön" Lösung im Rahmen der Endpoint-Security?
Daniel Döring - Director of Professional Services & Strategic Alliances / EgoSecure GmbH

13:45 Uhr operational services - Digital Forensics and Beyond: From Kernel- to Hardware-Rootkits
Michael Denzel - IT-Security Consultant / operational services GmbH & Co.KG

14:00 Uhr Live-Hacking: Hackner Security Intelligence
Thomas Hackner - Geschäftsführer / HACKNER Security Intelligence GmbH

M9 – Management Forum (Halle 9)

Dienstag 09. Oktober

09.45 Uhr Oracle - Autonomie und Resilienz für die IT in Zeiten von Digitalisierung und Disruption
Michael Fischer, Managing Principal, ORACLE Deutschland B.V. & Co. KG

10:00 Uhr TREND MICRO - CEO-Fraud - Die Erfolgsgeschichte des kriminellen Geschäftsmodels
Udo Schneider - Security Evangelist / TREND MICRO Deutschland GmbH

10:15 Uhr NTT Security/NTT Group - Paradigmenwechsel in der Sicherheitskultur: Die IT-Security auf dem Weg zum Business Driver
Patrick Schraut - VP Consulting Europe / NTT Security (Germany) GmbH

10:30 Uhr it-sa insights: IT-Sicherheit in der bayerischen Verwaltung – 10 Monate LSI
Daniel Kleffel - Präsident / Landesamt für Sicherheit in der Informationstechnik (LSI)

10:45 Uhr Aruba - Der Faktor Mensch als Risiko für gezielte Angriffe in der IT Sicherheit – UEBA
Reinhard Lichte - Lead Solution Architect – Security / ARUBA, a Hewlett Packard Enterprise company

11:00 Uhr Kaspersky - Security-Sensibilisierung geht nicht ohne Management Awareness
Alexander von Keller - Head of Enterprise Sales DACH / Kaspersky Labs GmbH

11:15 Uhr Varonis - Next-Gen Dateisicherheit trifft auf Next-Gen Cloud Dateidienste
Christoph Spitzer - Senior Customer Success Manager DACH / Varonis Systems
Zeljko Dodlek - RSM Dach / Nasuni

11:30 Uhr Tech Data Microsoft Partner - The Modern and Secure Workplace: Der generationenübergreifende und sichere Arbeits platz
Alexander Waldhaus - European Technical Solution Manager bei Tech Data / Tech Data GmbH & Co. OHG

11:45 Uhr McAfee - Das Unternehmen für durchgängige Cyber-Sicherheit vom Endgerät bis zur Cloud
Georg Hermann - Product Specialist / McAfee Germany GmbH

12:00 Uhr TÜV SÜD - Threat Intelligence als wichtiger Teil eines funktionierenden Security Lifecycles
Stefan Vollmer - Chief Technology Officer der TÜV SÜD Sec-IT GmbH / TÜV SÜD AG

12:15 Uhr G DATA - Tausend und eine Baustelle im Mittelstand 4.0 – Effiziente und sichere IT ist kein Märchen
Matthias Koll - Senior Sales Engineer / G DATA Software AG

12:30 Uhr it-sa insights: Security Governance 2020 (in der Finanzindustrie)
Umberto Annino - Präsident / ISSS – Information Security Society Switzerland

13:00 Uhr VdS - Mittelstandslösung: Datenschutz und Informationssicherheit im Doppelpack
Dipl. Ing. Markus Edel - Abteilungsleiter Managementsysteme und Cyber-Security / VdS Schadenverhütung GmbH

13:15 Uhr Sophos - IT-Security als Managed Service – DER Umsatzbringer für die Zukunft
Michael Gutsch - Manager MSP / Sophos Technology GmbH

13:30 Uhr Tenable - Die Evolution des Schwachstellen-Managements - Willkommen im Zeitalter der Cyber Exposure
Jens Freitag - Security Specialist / Tenable Network Security GmbH

13:45 Uhr Gemalto - Von User Authentifizierung zum Access Management der Zukunft
Armin Simon - Regional Sales Director Germany / Gemalto

14:00 Uhr ectacom - Mythos Sicherheit
Daniel Leiendecker - Entwickler Manager Cyber Security / ectacom GmbH

14:15 Uhr itWatch - Fremde Daten nutzen – ganz ohne Gefahr!
Ramon Mörl - Geschäftsführer / itWatch GmbH

14:30 Uhr Exclusive Networks - Thema siehe www.it-sa.de
N.N. / Exclusive Networks Deutschland GmbH

14:45 Uhr Airlock - Vom Stolperstein zum Meilenstein - Faktoren für ein erfolgreiches, nachhaltiges cIAM Projekt
Marc Bütikofer - CTO und Director Innovation / Airlock by Ergon

15:00 Uhr KPMG - Wieder eine neue Pflichtübung? – Nicht Bestandene Security Prüfungen als Showstopper im Vergabeprozess
Wolf von Waldthausen / KPMG AG Wirtschaftsprüfungsgesellschaft

15:15 Uhr telent - Cybersecurity der Businessenabler
Nico Werner - Head of Cybersecurity / telent GmbH

15:30 Uhr it-sa insights: Vorstellung der Ergebnisse der <kes>/ Microsoft-Sicherheitsstudie
Dipl. Inform. Norbert Luckhardt - Chefredakteur Zeitschrift <kes> / DATAKONTEXT GmbH

16:00 Uhr Imperva - 5 Wege, um Sie bei Problemen mit der Datenkompatibilität zu unterstützen
Martin Kulendik - Senior Account Executive / Imperva UK Ltd

16:15 Uhr Palo Alto - IT-Sicherheit in der Public Cloud - eine Darstellung für CIOs und IT-Leiter
Jens Egger - Systems Engineering / Palo Alto Networks GmbH

16:30 Uhr DriveLock - Cyber Security für Jedermann
Martin Mangold - Head of Cloud Operations / DriveLock SE

16:45 Uhr ESET - Welcome to the Dark-Web: Was sind Ihre Daten wert?
Thorsten Urbanski - Head of Corporate Communication / ESET Deutschland GmbH

17:00 Uhr it-sa insights: Paradigmenwechsel bei IT-Sicherheit: Wie sich IT-Verantwortliche in Krankenhäusern rüsten können
Hans-Wilhelm Dünn - Präsident / Cyber-Sicherheitsrat Deutschland e.V.
Dr. Stefan Bücken - IT-Sicherheitsbeauftragter (ITSB) / Universitätsklinikum Erlangen
Helmut Schlegel - Beisitzer im Vorstand / Bundesverband der Krankenhaus IT-Leiterinnen/Leiter e.V.
Jochen Kaiser - Leiter Service-Center IT / Bezirkskliniken Schwaben
Moderator
Wolf-Dietrich Lorenz - Chefredakteur, Krankenhaus IT-Journal / Antares Computer Verlag GmbH

Mittwoch 10. Oktober

09:30 Uhr bizcon - Datenzentrierte Sicherheit
N.N. / bizcon AG

09:45 Uhr Gemalto - Von User Authentifizierung zum Access Management der Zukunft
Armin Simon - Regional Sales Director Germany / Gemalto

10:00 Uhr Skybox - Ich sehe was, was du nicht siehst: Wie Sie Ihre Angriffsfläche visualisieren und Schwachstellen priorisieren
Jörg von der Heydt - Channel Director DACH / Skybox Security Inc.

10:15 Uhr CYQUEO - Any user, any device, any location – Wird die Zscaler-Cloud die Internet-Sicherheit revolutionieren?
Stephanie Huber - Technical Account Manager / CYQUEO GmbH

10:30 Uhr KeyIdentity - Wenn das IAM funktioniert – Ein IAM, das dich und das Business versteht
Dr. Amir Alsbih - CEO / KeyIdentity GmbH

10:45 Uhr AirITSystems - Implementation eines SOC - aus der Organisations-Perspektive
Tim Cappelmann - Leiter Managed Services / AirITSystems GmbH

11:00 Uhr noris network - ISO27001 - Sie können nur gewinnen
Martin Haunfelder - Senior IT Security Consultant, Governance and Standards / noris network AG

11:15 Uhr Arcserve - Business Continuity in der Cloud
Kai Steinbach - Principal Produkt Manager / Arcserve

11:30 Uhr nuvias Wick Hill - Thema siehe www.it-sa.de
N.N. nuvias Deutschland GmbH

11:45 Uhr RSA - RSA NetWitness
N.N. / RSA Security GmbH

12:00 Uhr EfficientIP - DNS & Datenschutz – Warum Firewalls nicht ausreichen - „Schützen Sie Ihre Daten vor Daten Exfiltration"
Ralf Geisler - Territory Manager - Germany / Austria / Swiss & Eastern Europe / Efficient IP GmbH

12:15 Uhr Zertificon - Neue Bedrohungslandschaften: Wie kann die Unternehmenskommunikation nachhaltig abgesichert werden?
N.N. / Zertificon Solutions GmbH

12:30 Uhr it-sa insights: DIN - Referenzarchitektur Sichere Digitale Identitäten
Benjamin Helfritz - Senior Projektmanager Abteilung Digitale Technologien / DIN Deutsches Institut für Normung e. V.

13:00 Uhr it-sa insights: eco - Allianz zur Stärkung digitaler Infrastrukturen in Deutschland
Moderation: N.N. / eco - Verband der Internetwirtschaft e.V.

14:00 Uhr Samsung - Mobile Endgeräte der Bundespolizei in einer sicheren Betriebsumgebung (Android/Samsung Knox/ Airwatch)
Thomas Aster - Senior Manager Government / Samsung Electronics GmbH
Stefan Hollensteiner - Referatsleiter IT-Infrastruktur / Bundespolizei

14:15 Uhr ESET - Next Generation Security: Mythos & Realität - Daten, Zahlen und Fakten
Thomas Uhlemann - Security Specialist / ESET Deutschland GmbH

14:30 Uhr Cyberbit - Asset Management im Zeitalter von Industrie 4.0
Felix Blanke - Manager Pre-Sales Central Europe / Cyberbit Deutschland GmbH

14:45 Uhr Totemo - Verbreitete Irrtümer über E-Mail-Verschlüsselung
Marcel Mock - CTO / totemo ag

15:00 Uhr DeskCenter - Dynamic Asset Intelligence: Basis Ihrer digitalen Transformation
Benedikt Gasch - Direktor Produktmanagement / DeskCenter Solutions AG

15:15 Uhr Magelan-Ivanti - Security für den Arbeitsplatz der Zukunft:
Bernhard Steiner - Director Sales Engineering, Ivanti Germany GmbH / Ivanti

15:30 Uhr DriveLock - Schwachstelle Mensch im industriellen Umfeld
Andreas Fuchs - Product Director / DriveLock SE

15:45 Uhr Exclusive Networks - Thema siehe www.it-sa.de
N.N. / Exclusive Networks Deutschland GmbH

16:00 Uhr Forcepoint - Aufbau eines eigenen/autonomen Security Operation Center
Denis Erk - Principal Field Sales Account Manager / Forcepoint

16:15 Uhr c.a.p.e. IT - Die CMDB im Kontext kritischer Infrastrukturen
Rico Barth / c.a.p.e. IT GmbH

16:30 Uhr NTT Data/NTT Group - Sicherheit mit Blockchain und DLT – 2018
Benjamin Matten - Strategic Solution Architect Banking / NTT DATA Deutschland GmbH

16:45 Uhr Bitsight-Protea Networks - Cyber-Risiken einfach und kontinuierlich managen
Frank Weisel / Protea Networks GmbH

17:00 Uhr F-Secure - Von echten Menschen und Maschinen – Künstliche Intelligenz
Florian Kellermann - Sales Engineer / F-Secure GmbH

17:15 Uhr Live-Hacking: Compass - Wie kommt der Hacker an sein Ziel
Jan-Tilo Kirchhoff - Geschäftsführer / Compass Security Deutschland GmbH

Donnerstag 11. Oktober

09:30 Uhr it-sa insights: Industrial Security als Voraussetzung für Industrie 4.0 / Digitalisierung in der Industrie
Dipl.-Wirtsch.-Ing. (ET) Maximilian Korff / Siemens AG

10:00 Uhr RSA - RSA SecureID
N.N. / RSA Security GmbH

10:15 Uhr ectacom - Thema siehe www.it-sa.de
N.N. / ectacom GmbH

10:30 Uhr Aruba - Sichere Integration von IOT Devices im Unternehmensnetzwerk
Reinhard Lichte - Lead Solution Architect – Security / ARUBA, a Hewlett Packard Enterprise company

10:45 Uhr Airlock - Vom Stolperstein zum Meilenstein - Faktoren für ein erfolgreiches, nachhaltiges cIAM Projekt
Marc Bütikofer - CTO und Director Innovation / Airlock by Ergon

11:00 Uhr LogPoint - SOC as a Service, Bedrohungen ändern sich!
Pascal Cronauer - Regional Director Central EMEA / LogPoint GmbH

11:15 Uhr Bitsight-Protea Networks - Cyber-Risiken einfach und kontinuierlich managen
Frank Weisel / Protea Networks GmbH

11:30 Uhr SecureLink - Cyber Defense made easy – "Home grown" oder vom Experten?
Fabian Beutel - CISSP, Lead Consultant IT-Security / SecureLink Germany GmbH

11:45 Uhr Varonis - 3 Schritte zur Sicherstellung der Compliance im Zeitalter der DSGVO
Matthias Schmauch - Enterprise Sales Representative / Varonis Systems

12:00 Uhr Forcepoint - Minority Report - Es ist nicht mehr länger Science Fiction
Stefan Maierhofer - Area VP Central Europe / Forcepoint

12:15 Uhr Exclusive Networks - Thema siehe www.it-sa.de
N.N. / Exclusive Networks Deutschland GmbH

12:30 Uhr F-Secure - Von echten Menschen und Maschinen – Künstliche Intelligenz
Florian Kellermann - Sales Engineer / F-Secure GmbH

12:45 Uhr Kaspersky - Sicherheitsfaktor Mensch - Technologie alleine reicht nicht
Peter Neumeier - Head of Channel Germany / Kaspersky Labs GmbH

13:00 Uhr ITConcepts - go:Identity 2.0 – Die automatisierte IDM Appliance Lösung
Dirk Wahlefeld - Business Analyst IT Security / ITConcepts Professional GmbH

13:15 Uhr VdS - Mittelstandslösung: Datenschutz und Informationssicherheit im Doppelpack
Mark Semmler - GF/CEO, Mark Semmler GmbH für / VdS Schadenverhütung GmbH

13:30 Uhr Compass - Sicher wie auf Wolke 7 – Penetration Tests for Cloud Environments
Jan-Tilo Kirchhoff - Geschäftsführer / Compass Security Deutschland GmbH

13:45 Uhr Zertificon - Neue Bedrohungslandschaften: Wie kann die Unternehmenskommunikation nachhaltig abgesichert werden?
N.N. / Zertificon Solutions GmbH

14:00 Uhr nuvias Wick Hill - Thema siehe www.it-sa.de
N.N., nuvias Deutschland GmbH

14:15 Uhr Dimension Data/NTT Group - Predictive Intelligence - Extending visibility and control beyond the organisation
Sebastian Ganschow - Principal Security Solutions Architect / Dimension Data Germany AG & Co. KG

14:30 Uhr thycotic - Privileged by nature? Warum traditionelle Security-Perimeter nicht mehr ausreichen.
Henning Hanke - Enterprise Solution Specialist / Thycotic

14:45 Uhr EgoSecure/Matrix42 - Seit der EU-DSGVO ist Endpoint-Security „Chef-Sache" – Compliance und Security steigern!
Daniel Döring - Director of Professional Services & Strategic Alliances / EgoSecure GmbH

15:00 Uhr Forescout - Digitale Transformation, Organisationen müssen ihre Sicherheitsstrategie überdenken
Stephan von Guendell-Krohne - Regional Director DACH / ForeScout Technologies Inc.

T10 – Technik Forum (Halle 10)

Dienstag 09. Oktober

09:45 Uhr Live-Hacking: SySS - IoT-Hacking: Angriffe auf das Internet of Things
Sebastian Schreiber - Geschäftsführer / SySS GmbH

10:15 Uhr F5 - Erweiterter Schutz für Anwendungen im Rechenzentrum und in der Cloud
Stephan Schulz - Senior Specialist Systems Engineer – Security / F5 Networks GmbH

10:30 Uhr One Identity - Single Source for Identity and Access Management
Susanne Haase / One Identity

10:45 Uhr TÜV Rheinland i-sec - Reduce time to detect & contain cyber incidents
Wolfgang Kiener - Business Development Manager / TÜV Rheinland i-sec GmbH

11:00 Uhr Fraunhofer IESE – MYDATA Control Technologies
Manuel Rudolph - Senior Security Engineer / Fraunhofer IESE

11:15 Uhr bomgar - Privileged Access Management – Herausforderungen die kein Anbieter effektiv lösen kann, außer Bomgar
Roland Schäfer - Regional Manager / Bomgar

11:30 Uhr Avecto - Machtkampf im Netzwerk: Admin-Rechte aufheben & Bedrohungen entschärfen
Dennis Weyel - Senior Technology Consultant / Avecto Ltd.

11:45 Uhr FireEye - #Halali auf den Endpunkt: Jäger oder Gejagter
Christian Husemeyer - System Engineer DACH / FireEye Deutschland GmbH

12:00 Uhr Bitdefender - Erwarte das Unerwartete: Threat Landscape Heute und Morgen
Herbert Mayer - Sales Engineer DACH / Bitdefender GmbH

12:15 Uhr Startups@it-sa: Hanko - Thema: siehe www.it-sa.de

12:30 Uhr Startups@it-sa: Cyber Observer - Thema: siehe www.it-sa.de
N.N. / Cyber Observer

12:45 Uhr Startups@it-sa: Neuvector - Kubernetes and Docker Hack – What are they and how can they be prevented with NeuVector
Dieter Reuter - Chief Solutions Architect of NeuVector / Neuvector Inc.

13:00 Uhr Startups@it-sa: Fenror7 - The bad guys are in!!! Now what???
Yaniv Miron - Founder & CEO / Fenror7 Ltd.

13:15 Uhr Startups@it-sa: DocBee - Thema: siehe www.it-sa.de

13:30 Uhr Startups@it-sa: Boxtrap Security - www.it-sa.de

13:45 Uhr Secardeo - PKI Automatisierung - Zertifikate von beliebigen CAs auf alle Geräte verteilen und verwalten
Dr. Gunnar Jacobson - CEO / Secardeo GmbH

14:00 Uhr Symantec - Ein Blick hinter die Kulissen: Die Vorgehensweisen von APT-Angreifern in einem kompromittierten Netzwerk
Armin Buescher - Senior Staff Security Researcher, Network Protection Products / Symantec Deutschland GmbH

14:15 Uhr Rohde & Schwarz - Sicheres Arbeiten auf Multi Cloud-Plattformen - Beispiel Microsoft Office 365
Dr. Bruno Quint - Director Cloud Encryption / Rohde & Schwarz Cybersecurity GmbH

14:30 Uhr MTRIX - Multi-Faktor-Authentifizierung in einer hybriden IT-Infrastruktur – Herausforderungen und Lösungen
Malte Kahrs - Geschäftsführer / MTRIX GmbH

14:45 Uhr essendi it - Sicheres Zertifikatsmanagement in Docker-Betriebsumgebungen
Werner Zügel - Geschäftsführer / essendi it GmbH
Benjamin Steiner / essendi it GmbH

15:00 Uhr NCP - Herausforderungen in der IIoT Sicherheit
Dr. Gabriele Spenger - CTO / NCP engineering GmbH

15:15 Uhr Virtual Solution - Sicherheit vs. Benutzerfreundlichkeit – Sicheres mobiles Arbeiten geht auch einfach
Pascal Schubert - Senior Presales Consultant / Virtual Solution AG

15:30 Uhr NEVIS - Live-Hacking: Cybercrime in der Realität – ist Ihr Unternehmen "richtig" geschützt?
Konstantin Luttenberger - Pre-Sales Consultant, AdNovum Informatik AG / NEVIS Security GmbH

15:45 Uhr Extreme Networks - Cloud Network Security for AWS, Google & Azure
Kurt Semba - Principal Architect / Extreme Networks GmbH

16:00 Uhr - 16:15 Uhr
Cisco - Incident Response mit Cisco Advance Malware Protection
Rene Straube - Consulting Systems Engineer / Cisco Systems GmbH

16:15 Uhr DRACOON - Datensouveränität im Kontext der digitalen Identität
Marc Schieder - CIO / DRACOON GmbH

16:30 Uhr consistec - Service oder Security Monitoring? Überblick oder Durchblick?
Dr.-Ing. Thomas Sinnwell - CEO FuE / consistec Engineering & Consulting GmbH

16:45 Uhr achelos - Gezieltes Aufdecken von Schwächen in TLS-Implementierungen
Heinfried Cznottka - Director Business Development / achelos GmbH

17:00 Uhr it-sa insights: „Locked Shields 2018" - Einblick in die größte Cyber-Abwehr-Übung der NATO
Major Bernd Kammermeier - SgLtr Übung/Sensibilisierung, Zentrum für Cyber-Sicherheit / Bundeswehr

Mittwoch 10. Oktober

09:30 Uhr BSI - Basissicherheitszertifizierung - Das neue Zertifizierungsschema des BSI für Produkte
Dr. Helge Kreutzmann - Referent / Bundesamt für Sicherheit in der Informationstechnik (BSI)

09:45 Uhr Akamai - World Class Security – auch für KMUs: Big Enterprise Security für den Mittelstand
Stefan Mardak - Senior Enterprise Security Architect / Akamai Technologies GmbH

10:00 Uhr genua - Post-Quanten-Kryptographie - Bedrohung, aktueller Stand, Lösungen
Dr. Daniel Loebenberger - Kryptologe / genua gmbh

10:15 Uhr IBM - Advanced SIEM und Threat Hunting
Justus Reich - Security Solutions Architect & TrustedAdvisor / IBM Deutschland GmbH

10:30 Uhr Fraunhofer SIT - App-Sicherheit - Automatisierte Analyse für den Unternehmensschutz
Dr. Jens Heider - Head of Department Testlab Mobile Security / Fraunhofer SIT Sichere Informationstechnologie

10:45 Uhr Splunk - Cyberangriff gegen deutsche Medienunternehmen und Organisationen im Bereich der Chemiewaffenforschung
Matthias Maier - EMEA Director of Product Marketing / Splunk Services Germany GmbH c/o Mindspace

11:00 Uhr ECOS - BSI-zugelassener Einsatz privater Endgeräte
Gerald Richter - Geschäftsführer / ECOS Technology GmbH

11:15 Uhr bomgar - Privileged Access Management – Herausforderungen die kein Anbieter effektiv lösen kann, außer Bomgar
Roland Schäfer - Regional Manager / Bomgar

11:30 Uhr Darktrace - Applying Machine Learning for Pracitcal Cyber Security
Max Heinemeyer - Director of Threat Hunting / Darktrace Limited

11:45 Uhr Check Point - IoT & Industrial Cyber-Attacks – Mythos oder Realität
Ralf Wüstling - CISSP - Security Consultant Strategic / Check Point Software Technologies GmbH

12:00 Uhr Cisco - Incident Response mit Cisco Advance Malware Protection
Rene Straube - Consulting Systems Engineer / Cisco Systems GmbH

12:15 Uhr Datto - Datto: Business Continuity & Disaster Recovery Demo
Björn Leenen - Sales Engineer (EMEA) / Datto EMEA
Shaun Durrant - Sales Engineer (DACH) / Datto EMEA

12:30 Uhr it-sa insights: Initiativen zur praktischen Kollaboration in Sachen Informationssicherheit
Marc Lindike - Head of Information Security Assurance / Flughafen München

13:00 Uhr ServiceNow - Future of Work: Governance Risk & Compliance/Integrated Risk Management
Manoj Patel - Sr. Advisory, Security & Risk Global Practice EMEA ServiceNow / ServiceNow

13:15 Uhr Computacenter - Neue Aspekte zur Automatisierung des Schwachstellen-Management-Prozesses
Peter Camillo Schmidt - Senior Consultant Secure Information / Computacenter AG & Co. oHG

13:30 Uhr it-sa insights: Sicherheit und Vertrauen in digitale Innovationen
Vortrag und anschließende Podiumsdiskussion
Moderator
Marc Fliehe - Leiter Digitales und IT-Sicherheit / VdTÜV Verband der TÜV e.V.

14:30 Uhr ITENOS - Zutrittskontrolle und Nutzerfreundlichkeit: ein Widerspruch bei der Sicherung sensibler Unternehmensbereiche?
Ralf Flöring - Leiter Corporate Projektmanagement / ITENOS GmbH

14:45 Uhr Startups@it-sa: Securai - Agile Penetrationstests – sichere Software von Anfang an.
Christoph Haas - Geschäftsführer / Securai GmbH

15:00 Uhr Startups@it-sa: Enginsight - Nur wer seine IT-Landschaft versteht kann diese auch absichern.
Mario Jandeck - Geschäftsführer / Enginsight GmbH

15:15 Uhr Startups@it-sa: IDENTOS - Vertrauenswürdige Transaktionen auf mobilen Geräten (iOS & Android)
Robert Schneider - CEO / IDENTOS GmbH

15:30 Uhr Startups@it-sa: Threema - Instant Messaging: Das Potential richtig ausschöpfen!
Roman Flepp, Head of Marketing & Sales, Threema GmbH

15:45 Uhr Proofpoint - Vertrauen ist gut, Awareness ist besser:
Oliver Karow - Manager Sales Engineering Central Europe / Proofpoint GmbH

16:00 Uhr Bitdefender - Erwarte das Unerwartete: Threat Landscape Heute und Morgen
Herbert Mayer - Sales Engineer DACH / Bitdefender GmbH

16:15 Uhr MTRIX - Sichere Authentifizierungsverfahren – ein Überblick
Malte Kahrs - Geschäftsführer / MTRIX GmbH

16:30 Uhr Avecto - Machtkampf im Netzwerk: Admin-Rechte aufheben & Bedrohungen entschärfen
Dennis Weyel - Senior Technology Consultant / Avecto Ltd.

16:45 Uhr Computacenter - Industrial Security & Produktionsdatenanalyse
Dr. Sebastian Schmerl - Solution Manager Cyber Defense for Production and IoT / Computacenter AG & Co. oHG

17:00 Uhr Live-Hacking: SySS - So brechen digitale Angreifer in Ihre Systeme ein
Sebastian Schreiber - Geschäftsführer / SySS GmbH

Donnerstag 11. Oktober

09:30 Uhr Live-Hacking: SySS - IoT-Hacking: Angriffe auf das Internet of Things
Sebastian Schreiber - Geschäftsführer / SySS GmbH

10:00 Uhr MTRIX - Professionelle Authentifizierung – Customer Success Story
Malte Kahrs - Geschäftsführer / MTRIX GmbH

10:15 Uhr Rohde & Schwarz - Web Application Security - Ihr Schutz gegen Hackerangriffe
Harald Beutlhauser - Technical Account Manager / Rohde & Schwarz Cybersecurity GmbH

10:30 Uhr Avecto - Machtkampf im Netzwerk: Admin-Rechte aufheben & Bedrohungen entschärfen
Dennis Weyel - Senior Technology Consultant / Avecto Ltd.

10:45 Uhr TÜV Rheinland i-sec - Industrial Security: AIR GAP – Yes or No!?
Wolfgang Kiener - Business Development Manager / TÜV Rheinland i-sec GmbH
Dr. Benedikt Westermann - Chief Security Analyst / TÜV Rheinland i-sec GmbH

11:00 Uhr Spike Reply - Fahrstuhl des Grauens, wenn das BACnet zurück schlägt…
Maurice Al-Khaliedy - Cyber Security Lead Consultant / Spike Reply GmbH

11:15 Uhr TUXGUARD - IT Sicherheit aus einem anderen Blickwinkel
Uwe Hanreich - CEO / TUXGUARD GmbH

11:30 Uhr Fraunhofer IESE – MYDATA Control Technologies
Manuel Rudolph - Senior Security Engineer / Fraunhofer IESE

11:45 Uhr LogRhythm - Erkennen von gerade aktiven Cyber Attacken in Echtzeit – NextGeneration SIEM
Stefan Schweizer - Regional Sales Manager / LogRhythm Germany GmbH

12:00 Uhr Bitdefender - Erwarte das Unerwartete: Threat Landscape Heute und Morgen
Herbert Mayer - Sales Engineer DACH / Bitdefender GmbH

12:15 Uhr G+H Systems - Kontinuierliche Überprüfung der Zugriffsrechte Ihrer Mitarbeiter, DSGVO-konform mit daccord
René Leitz - Leiter Product Development daccord / G+H Systems GmbH

12:30 Uhr it-sa insights - Das Thema KRITIS zur Chefsache machen
Dipl.-Wirt.-Inf. Martin Wundram - Leiter Referat IT-Forensik / Bundesverband für den Schutz Kritischer Infrastruktur e. V.

13:00 Uhr Blancco - Datenlösch- Management zertifiziert – auditfähig-wirtschaftlich
Cornelius Bührle - Director of EMEA Sales Engineering / Blancco Central Europe GmbH

13:15 Uhr Teqcycle Solutions - Sicherheitslücke Smartphone: Warum Altgeräte Unternehmen teuer zu stehen kommen können!
Michael zum Hofe - Director Business Development / Teqcycle Solutions GmbH

13:30 Uhr Airbus - OT Security Monitoring in der digitalen Fabrik
Tobias Kiesling - Team Lead ICS Security / Airbus CyberSecurity

13:45 Uhr Thema: siehe www.it-sa.de

14:00 Uhr Live-Hacking: Kalweit ITS - Just another live:hacking
Sven Philipp Kalweit - Geschäftsführer / Kalweit ITS GmbH

M10 – Management Forum (Halle 10.1)

Dienstag 09. Oktober

09:30 Uhr AXA - Cyber-Versicherung für Unternehmen
Christina Hübner - Cyber Spezialistin / AXA Versicherung AG

09:45 Uhr Peak Solution - Die Firewall der Zukunft – Warum es ohne Identity- und Accessmanagement nicht geht
Ga-Lam Chang, Geschäftsführer, Peak Solution GmbH

10:00 Uhr Infopulse - Do's & Dont's im Compliance Management
Jan Keil - Vice President Marketing / Infopulse GmbH

10:15 Uhr Computacenter - Neue Zeiten, neue Konzepte - agile Security für DevOps
Hauke Moritz - Lead Consultant Cloud Security / Computacenter AG & Co. oHG

10:30 Uhr Verizon - Ein Rahmenwerk für effektives Risikomanagement im Unternehmen
Arno Edelmann - Manager Security Solutions DACH / Verizon Deutschland GmbH

10:45 Uhr Net at Work - Verschlüssel's einfach – aber sicher
Stefan Cink - Produktmanager NoSpamProxy / Net at Work GmbH

11:00 Uhr NEVIS - Digitale Transformation – Business-Disruptor oder kalter Kaffee?
Stephan Schweizer - Chief Product Officer, AdNovum Informatik AG / NEVIS Security GmbH

11:15 Uhr WürthPhoenix - Ohne KI/ML geht im Monitoring nichts mehr. Anomalie Detection im Zeitalter von Cloud und IoT
Dr. Claus Huber - Sales Executive / Würth Phoenix GmbH

11:30 Uhr Frama - Datenschutzkonforme E-Mail-Kommunikation – Lösungen zur Einhaltung der DSGVO und Abwehr gegen Cyberangriffe
Christian Schneider - Externer Datenschutzbeauftragter / Frama Deutschland GmbH

11:45 Uhr Datto - Ransomware 2018 - der Datto Lagebericht
Markus Rex - Business Development / Datto EMEA

12:00 Uhr it-sa insights: TeleTrusT-Auditorium IT-Sicherheit - Der Stand der Technik als Compliance-Aufgabe
RA Karsten U. Bartels LL.M. - TeleTrusT-Vorstand, Leiter TeleTrusT-AG „Recht" / HK2 Rechtsanwälte
Moderator
Prof. Dr. Norbert Pohlmann - TeleTrusT-Vorsitzender / if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule

12:15 Uhr it-sa insights: TeleTrusT-Auditorium IT-Sicherheit - Das hochsichere Deutsche Smart Meter System des BSI
Markus Bartsch - Business Development / TÜV Informationstechnik GmbH TÜV NORD GROUP
Moderator
Prof. Dr. Norbert Pohlmann - TeleTrusT-Vorsitzender / if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule

12:30 Uhr it-sa insights: TeleTrusT-Auditorium IT-Sicherheit - Blockchain – Mit Standardisierung gegen Adoptionsbarrieren?
Dr. André Kudra - Leiter TeleTrusT-AG „Blockchain" / esatus AG
Moderator
Prof. Dr. Norbert Pohlmann - TeleTrusT-Vorsitzender / if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule

12:45 Uhr it-sa insights: TeleTrusT Auditorium IT-Sicherheit - Podiumsdiskussion
Dr. André Kudra - Leiter TeleTrusT-AG „Blockchain" / esatus AG
Markus Bartsch - Business Development / TÜV Informationstechnik GmbH TÜV NORD GROUP
RA Karsten U. Bartels LL.M. - TeleTrusT-Vorstand, Leiter TeleTrusT-AG „Recht" / HK2 Rechtsanwälte
Moderator
Prof. Dr. Norbert Pohlmann - TeleTrusT-Vorsitzender / if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule

13:00 Uhr it-sa insights: Desinformation – Neue Entwicklungen aus dem Cyber-Hades
Marcus Beyer - Advisory Lead Resilient Workforce NCE / DXC Technology
Dipl.-Psych. Ivona Matas - Psychologin / known_sense

13:30 Uhr G+H Systems - Kontinuierliche Überprüfung der Zugriffsrechte Ihrer Mitarbeiter, DSGVO-konform mit daccord
Sebastian Spethmann - Account Manager / G+H Systems GmbH

13:45 Uhr IBM - Intelligenter Schutz vor intelligenten Bedrohungen
Matthias Ems - Associate Partner IBM Security Services DACH / IBM Deutschland GmbH

14:00 Uhr Secorvo - DSMS - Datenschutz mit System
Dirk Fox - Gechäftsführer / Secorvo Security Consulting GmbH

14:15 Uhr genua - Prädikat „Besonders schützenswert" - Sichere Infrastruktur für die Digitalisierung
Matthias Ochs - Geschäftsführer / genua gmbh

14:30 Uhr HiScout - Zentral. Dezentral. HiScout
Julia Kreutziger - Senior Sales Manager / HiScout GmbH
Sascha Kreutziger - Senior Pre-Sales Manager / HiScout GmbH

14:45 Uhr Tools4ever - Zugriff auf Cloud-Anwendungen erleichtern & zugleich Schatten-IT bekämpfen
Jan Pieter Giele - Geschäftsführer / Tools4ever Informatik GmbH

15:00 Uhr Akamai - Cyber-Security als Bodyguard der Digitalisierung
Bernd König - Director Product Line Security EMEA / Akamai Technologies GmbH

15:15 Uhr Radarservices - Europas Sicherheits- und Bedrohungslage in Zahlen
Harald Reisinger - Geschäftsführer / RadarServices Smart IT-Security GmbH

15:30 Uhr Datagovernance - Big Data und Data Mining
Georg Bommer - CISSP, CISM, CISA / DataGovernance Technologies Ltd

15:45 Uhr Startups@it-sa: Agile Response - Reduzieren Sie Ihren Datenverlust durch Threat Hunting
Jens Frenkel - Sales Director / Agile Response Technologies

16:00 Uhr Startups@it-sa: ITS Integration - Scanley Cybrick - DSGVO Erfüllung for fun and profit
Viktor Mraz - CEO / ITs Integration GmbH
Michael Theumert - COO / ITs Integration GmbH

16:15 Uhr Startups@it-sa: Vasgard/IAN - Compliance Automation - The Missing Link
Michael Pöhlsen - Geschäftsführer / Vasgardian GmbH

16:30 Uhr it-sa insights: Sicherheitslagebild der Elektroindustrie: Digitale und analoge Herausforderungen der Anwender
Lukas Linke - Senior Manager Cybersicherheit / ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

17:00 Uhr it-sa insights: Lasst Emotionen sprießen und Drachen steigen - Rock'n'roll Awareness!
Marcus Beyer - Advisory Lead Resilient Workforce NCE / DXC Technology

17:30 Uhr AXA - Cyber-Versicherung für Unternehmen
Christina Hübner - Cyber Spezialistin / AXA Versicherung AG

Mittwoch 10. Oktober

09:45 Uhr it-sa insights: Keynote - Traum oder Albtraum – Chancen und Risiken des digitalen Zeitalters
Dr. Hans-Georg Maaßen - Präsident / Bundesamt für Verfassungsschutz (BfV)

10:00 Uhr msg systems - Wie viel Sicherheit benötigt das Internet of Things?

10:15 Uhr Rohde & Schwarz - Sichere Datenkommunikation im Unternehmen und Social Media auf einem Smartphone?
Dr. André Egners - Senior IT-Security Architect, Product Owner / Rohde & Schwarz Cybersecurity GmbH

10:30 Uhr secunet - Red-Teaming: Fortgeschrittene Bedrohungsanalysen durch simulierte Angriffe
Kevin Ott - Berater IT-Sicherheit, Penetrationstester / secunet Security Networks AG

10:45 Uhr Extreme Networks - Stealth Networking - Infrastruktur mit Tunnelblick
Andreas Helling - Senior Network Consultant / Extreme Networks GmbH
Ralf Klockewitz - Senior Network Consultant / Extreme Networks GmbH

11:00 Uhr Segusoft- Sicherer Datenaustausch als Keimzelle der digitalen Transformation in KMUs
Arno Klein - Geschäftsführer / Segusoft GmbH

11:15 Uhr NCP - Secure Communications Now And Tomorrow
Bernd Kann - Vertriebsleiter Nord / Account Manager / NCP engineering GmbH

11:30 Uhr Ginlo by Brabbler - Digitale Kommunikation - das große Datenleck
Fabio Marti - Director Business Development / ginlo by Brabbler

11:45 Uhr retarus - Catch me if you can – Die Tricks der E-Mail Betrüger
Martin Mathlouthi - Product Line Manager / retarus GmbH

12:00 Uhr it-sa insights: davit e.V. Panel - Potentiale Künstlicher Intelligenz heben - Haftungsrisiken nach der DSGVO vermeiden
Dr. Christiane Bierekoven - Rechtsanwältin, Fachanwältin für IT-Recht, Ebner Stolz Köln / davit e.V. - Arbeitsgemeinschaft IT-Recht im DAV

12:20 Uhr it-sa insights: davit e.V. Panel - Gemeinsame Daten verarbeitung mit Dritten
RA Karsten U. Bartels LL.M. - TeleTrusT-Vorstand, Leiter TeleTrusT-AG „Recht" / HK2 Rechtsanwälte

12:40 Uhr it-sa insights: davit e.V. Panel - Schritt für Schritt zur DS-GVO-Compliance
Dr. Thomas Lapp - Rechtsanwalt und Mediator, Fachanwalt für Informationstechnologierecht / IT-Kanzlei dr-lapp.de GbR

13:00 Uhr it-sa insights: IT-Sicherheit für KRITIS: Lösungen aus Praxis und Forschung
Prof. Dr. Ulrike Lechner - Lehrstuhl für Wirtschaftsinformatik / Universität der Bundeswehr München

13:30 Uhr Tesorion - Cybersecurity all-in
Rick Hofstede, Product Manager, TESORION NEDERLAND B.V.

13:45 Uhr OTRS - STORM powered by OTRS als Mittelpunkt Ihrer Cyber Defense Operations
Jens O. Bothe - Director Global Consulting / OTRS AG

14:00 Uhr Oskar Schunck - EU-Datenschutz-Grundverordnung – Was bedeuten die Änderungen der EU-DSGVO für Ihren Versicherungsschutz?
Niels Jöhnk - Leiter Competence Center Financial Lines / Oskar Schunck GmbH & Co. KG

14:15 Uhr Startups@it-sa: Lucy - Kriminalität im 21. Jahrhundert und der Faktor Mitarbeiter
Palo Stacho - Head of Operations LUCY Security / LUCY Security AG

14:30 Uhr Startups@it-sa: Datagovernance - Big Data und Data Mining
Georg Bommer - CISSP, CISM, CISA / DataGovernance Technologies Ltd

14:45 Uhr Startups@it-sa: IT-Seal - Der Employee Security Index - Awareness messen - Awareness steigern
David Kelm - Leitung Produktmanagement / IT-Seal GmbH Social Engineering Analysis Labs

15:00 Uhr r-tec IT Security - ISMS und IT Security Betrieb sind keine Königskinder
N.N. / r-tec IT Security GmbH

15:15 Uhr Ernst & Young - Ist konventioneller IT- Schutz noch zeitgemäß?
David Utrilla Torres - Senior Manager / Advisory - Cybersecurity / Ernst & Young GmbH WPG
Lars Lehmann - Technology Consulting, Senior Manager / Manager im Bereich Security / Ernst & Young GmbH WPG

15:30 Uhr it-sa insights: Key Findings der aktuellen COMPUTERWOCHE-Security-Studie
Kai Grunwitz - Senior Vice President EMEA / NTT Security (Germany) GmbH
Rüdiger Weyrauch - SE Director Central & Eastern Europe / FireEye Deutschland GmbH
Sven Schaefer - Business Development / Rackspace Germany
Moderator
Simon Hülsbömer - Senior Project Manager, Redaktion IDG Research Services, Computerwoche/CIO / IDG Business Media GmbH

16:15 Uhr SIZ - ISO 27001 am Beispiel Finanzdienstleister
Frank Hensel - Leiter ISM-Services / SIZ GmbH

16:30 Uhr TÜV Rheinland i-sec - Managing Risk & Compliance in der digitalen Transformation
Jörg Zimmermann - Principal Consultant Cybersecurity / TÜV Rheinland i-sec GmbH

16:45 Uhr GlobalSign - Cyber Security ist ein Ökosystem – Kollaboration als Schlüssel zur erfolgreichen Digitalisierung
Sebastian Schulz - Partner Account Manager / GlobalSign

17:00 Uhr it-sa insights: Cyber-Versicherung als Instrument des Cyber-Risikomanagements
Oliver Lehmeyer - Geschäftsführer / Cyber Risk Agency GmbH

Donnerstag 11. Oktober

09:30 Uhr it-sa insights: Zentrum für Cyber-Sicherheit der Bundeswehr - Moderner Dienstleister für IT-Sicherheit
Major Bernd Kammermeier - SgLtr Übung/Sensibilisierung, Zentrum für Cyber-Sicherheit / Bundeswehr

10:00 Uhr Proofpoint - Cyber-Kriminelle zielen auf den Faktor Mensch – Geschäftsführung und Mitarbeiter im Visier
Georgeta Toth - Senior Regional Director CEEMEA / Proofpoint GmbH

10:15 Uhr DEKRA - Wie gelingt ein hohes IT-Sicherheitsniveau?
Ingo Legler / DEKRA

10:30 Uhr retarus - Catch me if you can – Die Tricks der E-Mail-Betrüger
Martin Mathlouthi - Product Line Manager / retarus GmbH

10:45 Uhr Net at Work - Verschlüssel's einfach – aber sicher
Stefan Cink - Produktmanager NoSpamProxy / Net at Work GmbH

11:00 Uhr Check Point - Wolkenverhangen - Konsolidierte Sicherheitsarchitektur für private und öffentliche Cloud-Services
Stephan Fritsche - Cloud Security, IaaS Sales Manager / Check Point Software Technologies GmbH

11:15 Uhr Computacenter - Intelligentes Sourcing für die Security von morgen
Lutz Feldgen - Lead Consultant Secure Information / Computacenter AG & Co. oHG

11:30 Uhr Splunk - Wie Sie mit Hilfe der SOAR Technologie Ihre Security Operations effektiver gestalten
Angelo Brancato - Security Specialist / Splunk Services Germany GmbH c/o Mindspace

11:45 Uhr r-tec IT Security - For your objectives – ISMS plus Branchenstandards
N.N. / r-tec IT Security GmbH

12:00 Uhr Fraunhofer SIT - IT-Risiken in Produktionsumgebungen –Vorgehensmodelle zur Analyse und Bewertung
Mechthild Stöwer - Head of Department Security Management / Fraunhofer SIT Sichere Informationstechnologie

12:15 Uhr SIZ - ISO 27001 am Beispiel Finanzdienstleister
Dr. Jörg Kandels - Leiter ISM-Services / SIZ GmbH

12:30 Uhr Radarservices - Cyberattacken und IT-Sicherheit 2025 – die Expertenbefragung zu den Zukunftstrends
Harald Reisinger - Geschäftsführer / RadarServices Smart IT-Security GmbH

12:45 Uhr Symantec - Angriffe und sich täglich verändernde Bedrohungslagen: Integrated Cyber Defense Platform
Lars Kroll - Cyber Security Strategist, CISM, CISSP, ISO27001 Lead Auditor / Symantec Deutschland GmbH

13:00 Uhr msg systems - Privileged Access Management
N.N. / msg systems ag

13:15 Uhr essendi it - 360° Blick auf Zertifikatsmanagement
Josef König - Product Manager Identity & Certificate Services / SwissSign
Sarah Zügel - Head of Business Development & Communication / essendi it GmbH

M10 – Management Forum (Halle 10.1)

13:30 Uhr Datagovernance - Big Data und Data Mining
Georg Bommer - CISSP, CISM, CISA / DataGovernance Technologies Ltd

13:45 Uhr BSI - Sichere Mobile Lösungen
Dr. Christopher Basting - Referat KT 14 / Bundesamt für Sicherheit in der Informationstechnik (BSI)

14:00 Uhr One Identity - Wie bekomme ich das Recht auf Identitäts- und Zugriffsmanagement?
Susanne Haase / One Identity

14:15 Uhr it-sa insights: Auskunft nach DS-GVO: Wie müssen Unternehmen auf Anfragen reagieren?
Dr. Thomas Lapp - Rechtsanwalt und Mediator, Fachanwalt für Informationstechnologierecht / IT-Kanzlei dr-lapp.de GbR

14:30 Uhr Peak Solution - Die Firewall der Zukunft – Warum es ohne Identity- und Accessmanagement nicht geht
Ga-Lam Chang, Geschäftsführer, Peak Solution GmbH

14:45 Uhr bayme – startups stellen sich vor
Moderation: N.N. Die bayerischen Metall- und Elektro-Arbeitgeber

15:15 Uhr Live-Hacking: if(is)
Matteo Cagnazzo - Projektleiter Gesundheitswesen / if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule
Chris Wojzechowski - Wissenschaftlicher Mitarbeiter / if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule

I 10 – Forum International (Halle 10.1)

Dienstag 09. Oktober

09:30 Uhr it-sa insights: Innovative solutions to enhance cybersecurity in Europe
Prof. Udo Helmbrecht - Executive Director / ENISA - European Union Agency for Network and Information Security

10:00 Uhr SpyCloud - Acting Early and First: Operationalizing Compromised Credentials for Improved Security
Chip Witt - Head of Product Strategy / SpyCloud Inc.

10:20 Uhr Netskope - A CISOs view of Cloud and why it will revolutionize the security stack
Neil Thacker - CISO EMEA & DPO / Netskope UK LTD

10:40 Uhr Cybereason - AI and Cybersecurity – The growing need for threat hunting
Faisal Habib - VP of Field Engineering and Services EMEA / Cybereason

11:00 Uhr Juliasoft - Hunting Software Security Vulnerabilities and Privacy Leaks with Semantic Static Analysis
Pietro Ferrara - Head of Research and Development / JuliaSoft srl

11:20 Uhr Cybersprint - Digital Risk Monitoring and how to protect your online footprint
Cynthia Schouten - Chief Information Security Officer / Cybersprint B.V.

11:40 Uhr Forescout - Transforming Security Through Visibility from Campus to Cloud
Len Rosenberg - VP Engineering / ForeScout Technologies Inc.

12:00 Uhr BeOne Development - How to develop and achieve secure human behaviour?
Wilbert Pijnenburg - Commercial Director, BSc CISA CISSP / Beone Development Group BV

12:20 Uhr Guardian360/Bitsensor - DS-GVO / GDPR: Data protection by Design and by Default, from DevOps to Production
Jan Martijn Broekhof - Managing Director / Guardian360 BV
Ruben van Vreeland - Ethical Hacker, CEO / BitSensor

12:40 Uhr Ernst & Young - Effectiveness of SIEM SOC in protecting critical information Assets
Andrea Gergen - Associate Partner GSA Cybersecurity / Ernst & Young GmbH WPG
Roshan Sherifudeen - Senior Manager – Cyber Security / Ernst & Young GmbH WPG

13:00 Uhr it-sa insights: The French Cybersecurity sector: overview and opportunities
Amélie Rives - Senior Cybersecurity Consultant / Compagnie Européenne d'Intelligence Stratégique (CEIS)

13:20 Uhr HackerOne - Keynote: Security is Everyone's Responsibility
KeynoteSpeaker
Marten Mickos - CEO / HackerOne

13:40 Uhr Kaspersky - How to reduce Cyber Risks in a Context of Balkanisation and Nationalization of Cyberspace
Veniamin Levtsov - Vice President, Corporate Business / Kaspersky Labs GmbH

14:00 Uhr Proofpoint - Seeing the Attacker's View: A People-Centric Approach to Security
Adenike Cosgrove - Cyber Security Strategist EMEA / Proofpoint GmbH

14:20 Uhr OneTrusT - How to Tackle the GDPR: A Typical Privacy & Security Roadmap
Dominic Schmidt-Reiche - Sales Manager Central & Southern EMEA / OneTrust

14:40 Uhr Spike Reply - Does AI cause a knockout in the security?
Ibrahim Köse - CTO / Spike Reply GmbH

15:00 Uhr Varonis - 3 steps to ensure compliance in the age of DSGVO
Matthias Schmauch - Enterprise Sales Representative / Varonis Systems

15:20 Uhr Airbus - Gamified approaches for raising IT-Security Awareness
Dr. Andreas Rieb - Cyber Security Specialist / Airbus CyberSecurity

15:40 Uhr TÜV SÜD - Uniscon: Ultra secure processing of data and applications with Sealed Platform
Dr. Ralf Rieken - COO of the TÜV SÜD Company Uniscon GmbH / TÜV SÜD AG

16:00 Uhr DEKRA - Social Engineering - Human Security-Weaklink
Graham Stanforth, Leiter Technical Service Management, DEKRA SE

16:20 Uhr EmpowerID - AI and Robotic Process Automation and their Impact on Identity and Access Management
Patrick Parker - CEO / EmpowerID

Mittwoch 10. Oktober

09:30 Uhr it-sa insights: Hacking People - The Current State of US Business Data Breaches
Brian Dykstra - CEO / Atlantic Data Forensics, Inc.

10:00 Uhr ThreatQuotient - Cyber Threat Intelligence – Hurricanes and Earthquakes
Jonathan Couch - Senior Vice President Strategy / ThreatQuotient Inc.

10:20 Uhr Secardeo - PKI automation: Distributing and managing certificates from any CA for all your devices
Dr. Gunnar Jacobson - CEO / Secardeo GmbH

10:40 Uhr Ernst & Young - The speed of IoT and its impact on security
Daniel Rüth / Ernst & Young GmbH WPG
Aleksander Poniewierski / Ernst & Young GmbH WPG

11:00 Uhr EmpowerID - The Serverless Revolution and its Impact on IAM
Patrick Parker - CEO / EmpowerID

11:20 Uhr CenturyLink - Keeping your traffic flowing, no matter what. DDoS solutions as the first layer of defence
Allan Guillen - Security Evangelist / CenturyLink Communications Germany GmbH

11:40 Uhr EclecticIQ - Building a threat intelligence driven cybersecurity practice
Jörg Abraham - Senior Threat Analyst at EclecticIQ Fusion Center / EclecticIQ B.V.

12:00 Uhr Extreme Networks - Secure Client Access to the Network, Are we ready for IoT yet?
Andreas Richter - WLAN Consultant DACH / Extreme Networks GmbH

12:20 Uhr Mellanox - Thoughts about the Benefits and Challenges of networked NVMe and its impact on Security Technology
Michael Frings, Senior Regional Manager Government Sector - Central Europe, Mellanox Technologies

12:40 Uhr it-sa insights: ENISA's efforts on bringing communities together to secure Industry 4.0
Florian Pennings - Senior Advisor Public Private Partnerships / ENISA - European Union Agency for Network and Information Security
Apostolos Malatras - Network and Information Security Expert / ENISA - European Union Agency for Network and Information Security

13:00 Uhr it-sa insights: Heavyweight-Meeting - The future of IT security is bright – or just another bubble?
Terry Ray - Chief Technology Officer / Imperva UK Ltd
Dr. Guy Bunker - Senior Vice President Products and Marketing / Clearswift RUAG Cyber Security
Dr. Paul Vixie - Chairman, CEO and Cofounder / Farsight Security, Inc.
Moderator
Dipl. Inform. Norbert Luckhardt - Chefredakteur Zeitschrift kes / DATAKONTEXT GmbH

14:00 Uhr Verizon - Put our cybercrime case studies to work. The Verizon Data Breach Digest
Jimmy Nilsson - Director Professional Services / Verizon Deutschland GmbH

14:20 Uhr SecureLink - Attacks aren't what they used to be. What does this mean for our defense strategy?
Eward Driehuis - Chief Research Officer (CRO) / SecureLink Germany GmbH

14:40 Uhr CyberSprint/FoxIT/EclecticIQ - International Cyber Threat Update
Cynthia Schouten - Chief Information Security Officer / Cybersprint B.V.
Jörg Abraham - Senior Threat Analyst at EclecticIQ Fusion Center / EclecticIQ B.V.
Michiel Renzenbrink - International Business Development Manager / Fox-IT Group B.V.

15:00 Uhr Virtual Solution - Security vs. Usability – Secure work on mobile devices made simple
Petros Dolaschjan - Business Development / Virtual Solution AG

15:20 Uhr FireEye - Prevent, Detect, Respond: Requirements in the current threat landscape
Rüdiger Weyrauch - SE Director Central & Eastern Europe / FireEye Deutschland GmbH

15:40 Uhr sayTEC - Challenges and Remedies in a Multifaceted Information Security Landscape
Erwin Pfuhler - Key Account Manager / sayTEC AG

16:00 Uhr Juniper - Rise of Cryptocurrency Malware
Laurence Pitt - Global Security Strategy Director / Juniper Networks GmbH

16:20 Uhr Safetica Technologies - What happens to your data when you're not looking
Ota Cermak - Global Business Development Manager / Safetica Technologies s.r.o.

Donnerstag 11. Oktober

09:30 Uhr it-sa insights: Building a European Cyber security ecosystem joining both public and private sectors efforts
Eda Aygen - Advisor to the Secretary General / European Cyber Security Organisation (ECSO)

10:00 Uhr it-sa insights: BSI C5: The Game Changer in Cloud Compliance Attestation
Immo Regener / PwC PricewaterhouseCoopers GmbH - Wirtschaftsprüfungsgesellschaft

10:20 Uhr Vortragstitel siehe: www. it-sa.de

10:40 Uhr Kaspersky - How much does it cost being Risk Averse in Digitally Transforming Enterprise?
Oleg Glebov - Senior Product Marketing Manager / Kaspersky Labs GmbH

11:00 Uhr ThreatMetrix - Responding to Rising Fraud: The Ace up Your Sleeve
Alexander Frick - Sales Director D/A/CH / ThreatMetrix

11:20 Uhr DEKRA - Social Engineering - Human Security-Weaklink
Graham Stanforth, Leiter Technical Service Management, DEKRA SE

11:40 Uhr SailPoint – Thema: siehe www.it-sa.de/foren
N.N., SailPoint Technologies

12:00 Uhr SPECIAL KEYNOTE: Attacks of the Industry: A View into the Future of Cybersecurity
KeynoteSpeaker
Paula Januszkiewicz - CEO and Founder of CQURE, Poland | Security Expert and Microsoft Regional Director / CQURE Academy

Aktuelle Programmänderungen und Ergänzungen: www.it-sa.de/rahmenprogramm

Volle Kontrolle durch umfassende Übersicht

Eines wird in der Diskussion über das Management von IT-Geräten oft vergessen: Nicht nur die Erfassung und Überwachung einzelner Komponenten ist wichtig, sondern auch ihre Vernetzung untereinander. Gerade im Hinblick auf das Internet der Dinge (IoT), das bereits jetzt Unternehmen stark beeinflusst, muss der Zusammenhang zwischen den einzelnen Geräten verstanden werden. Um das IoT zu verwalten, muss jedes Gerät und jeder Service im Auge behalten werden – vom kleinsten Sensor bis hin zu Back-End-Diensten, die Rohdaten in brauchbare Informationen umwandeln.

Von Armin Leinfelder, baramundi software AG

Bevor Geräte im Unternehmensnetzwerk verwaltet werden können, muss die IT-Landschaft vollständig erfasst werden. Eine Möglichkeit dafür ist der Einsatz eines automatisierten SNMP-Scanners (Simple Network Management Protocol) in Ergänzung zur klassischen tiefgehenden Inventarisierung der Endpoints. Erkennungsregeln definieren anhand einer entweder vom Lösungsanbieter oder vom IT-Administrator festgelegten Logik, wie der Typ eines Netzwerkgerätes erkannt wird. Ebenso bestimmen Erkennungsregeln, welche Werte für diesen Typ ausgelesen und in eine Datenbank importiert werden sollen. Die Regeln sollten anhand von Operatoren, Vergleichen und Prüfungen beliebig tief geschachtelt werden können, um einzelne Geräte genauer bestimmen und zusätzliche Werte auslesen zu können. Denn nur wenn IT-Administratoren alle relevanten Details kennen, ist eine vernünftige Verwaltung der Geräte möglich. Standardregelsätze definieren die geläufigsten Netzwerkgeräte und sollten bei Bedarf beliebig um weitere Regeln und Werte ergänzt werden können. Auch Scripting (Powershell) kann helfen, sehr spezifische Regeln zu definieren.

Nachdem der Netzwerk-Scan durchgeführt wurde, zeigen moderne Lösungen die gefundenen Geräte in der Regel in Listen an. Dort können sie in verschiedene Untergruppen kategorisiert werden. Die Darstellung sollte nicht nur Detailinformationen über einzelne Netzwerkgeräte enthalten, sondern auch die Verbindungen zwischen ihnen aufzeigen. IT-Administratoren erhalten somit einen umfassenden Überblick über die im Unternehmen vorherrschende Netzwerktopologie.

Die Darstellung der IT-Landschaft erfolgt – ähnlich wie in Business-Intelligence-Lösungen – mittels einer grafischen Aufbereitung. Insbesondere bei großen und komplexen IT-Umgebungen und mit der Zunahme des Internet of Things kann eine IT-Landkarte sehr schnell unübersichtlich werden. Such- und Filterfunktionen ermöglichen es IT-Administratoren, schnell zu einem bestimmten Endgerät zu navigieren. Über die IP- oder MAC-Adresse sowie über den Hostnamen kann der IT-Administrator beispielsweise das gewünschte Gerät dann schnell und unkompliziert finden. Gewöhnlich liefern alle Netzwerkgeräte und deren Verbindungen eine große Anzahl an Daten. Informationen wie der Hostname eines Endgerätes, die IP- oder MAC-Adresse sollten für den IT-Administrator immer abrufbar sein. Um bei Konfigurationsmaßnahmen oder Störungen (z. B. Verbindungsstörung) mehr Informationen zu den betroffenen Netzwerkverbindungen zur Hand zu haben, ist es wichtig, dass Administratoren wissen, an welchem Port eine Verbindung überhaupt angeschlossen ist. Werden alle Netzwerkverbindungen in der IT-Landkarte angezeigt, kann der IT-Administrator prüfen, ob zum Beispiel eine Fallbackverbindung existiert, falls bestimmte Verbindungen ausfallen. Neben den aktuell genutzten Routen, die über STP-Algorithmen bestimmt werden, ermöglicht eine IT-Landkarte die Markierung blockierter Verbindungen. Über eine Verlinkung zur Webmanagementkonsole des jeweiligen Netzwerkgeräts sollte der Administrator komfortabel zum jeweiligen Gerät navigieren können, um dort spezifische Änderungen vorzunehmen. Neben der Darstellung etwaiger Netzwerkgeräte und deren Verbindungen in eine für den Anwender angenehme und leicht verständliche Darstellung ist das Reporting für die IT-Dokumentation ein wichtiges

Entscheidungskriterium bei der Auswahl einer Lösung. Administratoren haben bei modernen Lösungen die Möglichkeit, ihre Berichte in gängigen Formaten wie etwa PDF, Visio und SVG zu ziehen.

Compliance-Management auf allen Ebenen

Neben der Visualisierung der IT-Geräte kann deren Verwaltung durch unterschiedliche Wege bewerkstelligt werden: sei es mit zweckbestimmten Speziallösungen oder mit einer umfassenden Unified-Endpoint-Management-Lösung (UEM), die alle notwendigen Funktionen in nur einer Lösung vereint. Gerade in Zeiten zunehmender Komplexität von IT-Umgebungen, dem Zuwachs von Gerätetypen und neuen rechtlichen Anforderungen ist eine unkomplizierte und einheitliche Lösung zu empfehlen. Solch eine Lösung unterstützt die Regelkonformität der IT auf drei Ebenen:

Wirtschaftlich: Software kennen, Kosten sparen

Zusätzlich zu den Endgeräten benötigen IT-Administratoren einen Überblick über die gesamte Software. Neben der technischen Inventur der Software als solcher ist eine regelmäßige Gegenüberstellung zu den erworbenen Softwarelizenzen notwendig. Eine Vielzahl an Unternehmen hat keinen exakten Überblick darüber, wie viele Lizenzen im Einsatz sind. Die Folge: oftmals eine teure Unter- oder Überlizenzierung. Gerade im Hinblick auf Audits ist dieses Thema wichtig, da unerwartete Kosten drohen, falls die Lizenzbilanz nicht passt.

Technisch: Schwachstellen aufdecken und beheben

Eine vollständige Software-Inventur für alle Unternehmensstandorte gehört für IT-Administratoren zu einer ganzheitlichen Sicherheitsstrategie. Um Mitarbeitern immer die aktuellste Version von Software anbieten zu können, sollte eine Management-Lösung dem Administrator detailgenau anzeigen, welche Version einer Software auf welchem Endgerät installiert ist. Falls veraltete Software zum Einsatz kommt, kann der Administrator direkt die notwendigen Maßnahmen ergreifen, um potenziellen Schwachstellen vorzubeugen und regelkonform zu handeln.

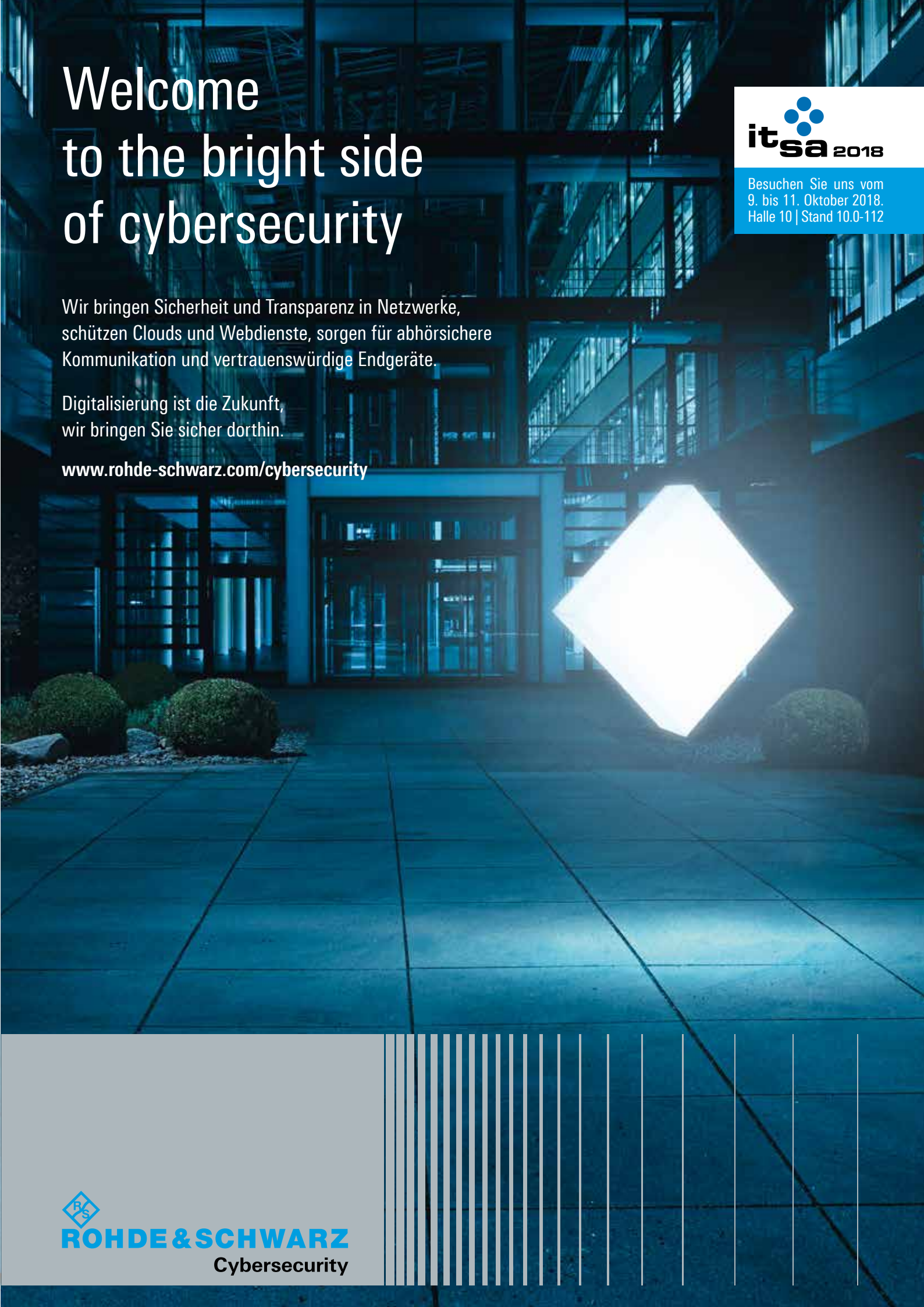
Juristisch: die DSGVO erfüllen

Neben den genannten Compliance-Aufgaben von der Inventur von Software und verschiedensten Geräten bis zum Management und Beheben von Schwachstellen spielt das Thema Datenschutz über alle Komponenten hinweg eine wichtige und grundlegende Rolle. Gerade im Hinblick auf die neue EU-Datenschutzgrundverordnung (DSGVO) haben sich auch die Anforderungen an Organisationen hinsichtlich der Rechenschaftspflicht erheblich verschärft.

Vertrauen ist gut, Kontrolle ist besser

Ein Unternehmen, das auf viele einzelne Lösungen zur Bearbeitung verschiedener Bereiche setzt, läuft Gefahr, das Management der gesamten IT unnötig komplex zu gestalten. Der Vorteil eines ganzheitlichen Managements aller Endgeräte mit nur einer Lösung liegt neben der Funktionsvielfalt und der erleichterten Einhaltung der Rechtskonformität auch in einer für den Admin unkompliziert zu realisierenden Dokumentation. Ein Zusammenführen verschiedener Berichte unterschiedlicher Quellen zu einem einzigen Report ist dann nicht mehr notwendig. Ein UEM erfüllt die Kriterien nach Funktionsvielfalt, Aktualität, Einheitlichkeit und stellt ein Hilfsmittel zur Erfüllung der Compliance-Richtlinien auf wirtschaftlicher, technischer und juristischer Ebene dar. Admins müssen sich auf die Angaben der Softwarehersteller, deren Übereinstimmung mit dem geltenden Recht und auf die gebotenen Funktionen der Lösung verlassen können. Daher ist es wichtig, dass die Verantwortlichen mit einer modernen Management-Lösung neben einem schnellen Überblick über den Status quo der Endgeräte bis ins kleinste Detail die Konformität aller Komponenten und ihre Vernetzung untereinander sicherstellen können und Administratoren trotz aller Hilfsmittel die Kontrolle über ihre IT behalten. ■

Messestand: Halle 10.0, Stand 10.0-215


Welcome
to the bright side
of cybersecurity
Wir bringen Sicherheit und Transparenz in Netzwerke, schützen Clouds und Webdienste, sorgen für abhörsichere Kommunikation und vertrauenswürdige Endgeräte.
Digitalisierung ist die Zukunft, wir bringen Sie sicher dorthin.
www.rohde-schwarz.com/cybersecurity
it sa 2018
Besuchen Sie uns vom 9. bis 11. Oktober 2018. Halle 10 | Stand 10.0-112
ROHDE&SCHWARZ
Cybersecurity

Data-Loss-Prevention

Endpoint Protector stellt Next-Generation-DLP vor

Strengere Datenschutz-Vorschriften, zunehmende Digitalisierung und engere Vernetzung machen den Schutz sensibler Inhalte vor unerwünschtem Abfluss zu einer Kernaufgabe der Unternehmen. Hersteller von Data-Loss-Prevention-(DLP)-Lösungen entwickeln angesichts der steigenden Anforderungen neue Erkennungstechnik auf der Grundlage mathematischer Verfahren. Sie ermöglicht, dass die DLP-Lösungen der nächsten Generation auf unternehmensspezifische Themen trainierbar sind und beim Schutz komplexer Inhalte effizient arbeiten.

Von Michael Bauner, Endpoint Protector GmbH

Die DSGVO führt zu einem Lernprozess in den Unternehmen und Organisationen. Sie begreifen die Auswirkungen von Datenverlust auf ihre Marktstellung und erkennen, dass sie neben den personenbezogenen Daten auch Geschäfts- und Firmengeheimnisse sowie Angaben zu kritischen Infrastrukturen vor unkontrolliertem Abfluss schützen müssen. Deren Anfälligkeit für Verlust und Diebstahl nimmt mit der Digitalisierung rapide zu, denn die Datenbestände wachsen exorbitant und immer mehr Mitarbeiter, Zulieferer und Kunden haben mit sensiblen Daten zu tun. Auch die Zahl der Kommunikationskanäle steigt.

Den Schutz vor unkontrolliertem Datenabfluss gewährleisten Lösungen für Data-Loss-Prevention. Deren mächtigstes Instrument ist die Inhaltskontrolle. In Endpoint Protector scannt das Modul „Content Aware Protection“ (CAP) Daten in Bewegung auf das Vorkommen sensibler Informationen, deren Muster in Black- und White-Regeln hinterlegt sind, und erlaubt beziehungsweise blockiert den Transfer entsprechender Dateien über E-Mail oder browserbasierte Anwendungen wie Webmailer, Cloud-Speicher, Filesharing- oder Collaboration-Tools.

In der Software sind Regeln für Gruppen von personenbezogenen Daten hinterlegt, beispielsweise für Adressdaten, Sozialversicherungs-, Kreditkarten-, Pass- und Personalausweisnummern. Diese vordefinierten Erkennungsschemata vereinfachen die Einrichtung der Richtlinien. Sie lassen sich zudem für die Umsetzung von Policies aus gesetzlichen Vorgaben und internationalen Standards wie DSGVO, HIPAA oder PCI-DSS in schnell einzurichtende Pakete zusammenfassen. Zudem können Unternehmen Dateien auf unternehmensspezifische Inhalte prüfen. Dafür lassen sich, beispielsweise zum Schutz des geistigen Eigentums oder kritischer Infrastrukturen, individuelle Wörterbücher mit Schlüsselbegriffen und regulären Ausdrücken zur Analyse von Zeichenketten anlegen.

Die Inhaltskontrolle einer DLP-Lösung prüft Daten in Bewegung auf sensible Informationen.

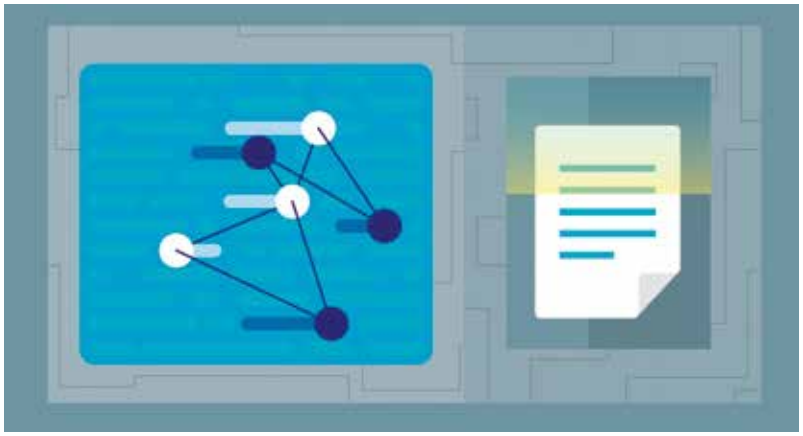
Da die Digitalisierung die Diversifizierung der Rechnerlandschaften in den Unternehmen beschleunigt, ist für den Erfolg von Data-Loss-Prevention entscheidend, dass sich die Richtlinien auf alle Rechner anwenden lassen. Es sollte keine Bereiche geben, in denen sie nicht umgesetzt werden können, weil die DLP-Lösung nicht alle Betriebssysteme abdeckt. Endpoint Protector funktioniert betriebssystem-übergreifend und gewährleistet in gemischten Umgebungen für alle Rechner den gleichen Schutzumfang.

Suche nach unstrukturierten Daten

Die Verfahren und Richtlinien für Daten in Bewegung nutzt Endpoint Protector auch für die Suche nach ruhenden Daten. Diese befinden sich nicht nur in Systemen wie ERP oder CRM, sondern in unstrukturierter oder semistrukturierter Form auch auf den Festplatten der Arbeitsplatzrechner sowie in Cloud-Speichern wie Dropbox, OneDrive, iCloud, Google Drive. Dabei handelt es sich oft um Exporte aus den zentralen Systemen sowie um eingehende Dokumente wie Bewerbungen, Teilnehmerlisten und Ähnliches. Sie alle müssen ebenfalls der DSGVO entsprechend behandelt werden, wenn das Unternehmen sich nicht strafbar machen will. Das Modul „eDiscovery" scannt die Desktop-Computer und findet über sie auch sensible Daten in den Cloud-Speichern. Die Ergebnisse werden als Report ausgegeben, sodass die Daten gelöscht oder verschlüsselt werden können.

Der Vorteil der Mustererkennung ist ihre Zuverlässigkeit. Aber Muster können übereinstimmen und trotzdem nicht zutreffen. Sind beispielsweise Produktkennungen aufgebaut wie eine Steuer- oder Kontonummer, blockiert die DLP-Lösung den Versand von Datenblatt oder Bestellformular. Um die Quote der sogenannten False-Positives zu verringern, hat Endpoint Protector der Mustererkennung eine Umfeldsuche beigestellt, die sich als individuelle Suche innerhalb der Suchergebnisse konfigurieren lässt.

DLP-Technologie vergleicht Muster anhand von Black- und White-Regeln. Die Ergebnisse sind tadellos, solange Vergleiche ein Resultat erbringen. An ihre Grenzen kommt DLP, wenn die Muster sehr komplex werden. Dann beansprucht der Abgleich so viele Ressourcen, dass die Leistungsfähigkeit des Systems darunter leiden kann.



Für komplexe Inhalte setzt Endpoint Protector eine trainierbare Erkenungstechnologie ein.

N-Gramm-Kategorisierung als DLP-Technologie

Die digitale Transformation bewirkt, dass das, was Unternehmen als ihr geistiges Eigentum ansehen und vor unkontrolliertem Abfluss schützen wollen, an Individualität zunimmt. Gemeint sind Inhalte wie Quellcode. Damit exakt bestimmt werden kann, ob ein Text Quellcode enthält und in welcher Programmiersprache er codiert wurde, würden Bibliotheken mit enormem Datenvolumen benötigt. Das ist für einen Anbieter von Enterprise-DLP wie Endpoint Protector, der seine Lösung schlank und ressourcenschonend halten will, keine Option. Die Lösung ist eine trainierbare, ressourcensparende Technologie.

Für hochkomplexe Aufgaben wie die Suche nach Code nutzt Endpoint Protector ein mathematisches Verfahren, die N-Gramm-Kategorisierung. N-Gramme sind Fragmente einer Zeichenkette. Wie häufig bestimmte Fragmente auftreten, wird vom Thema bestimmt. Anhand von Trainingstexten lassen sich daraus Profile für thematische Kategorien erstellen. Für Dateien, deren Inhalt im Hinblick auf die Zulässigkeit einer Übermittlung bewertet werden soll, wird ebenfalls ein N-Gramm-Profil erzeugt. Die Entscheidung fällt anhand der Nähe des Dateiprofils zu einem Kategorie-Profil.

Die N-Gramm-Kategorisierung will die herkömmliche Mustererkennung nicht ersetzen, denn diese funktioniert für bestimmte Bereiche ausgezeichnet. Das neue Verfahren soll Aufgaben bewältigen, die die normale Mustererkennung überfordern. Dabei kommt nicht nur der Vorteil eines erheblich geringeren Ressourcenbedarfs zum Tragen. Darüber hinaus kann ein Unternehmen künftig eigene Trainingssets und Kategorien für spezifische Themen erstellen und den Schutz vor Datenabfluss passgenau auf die Bedürfnisse ausrichten.

Fazit

Lösungen für Data-Loss-Prevention von heute sind ausgereifte Systeme, die ein breites Spektrum an Funktionalität auf der Grundlage von Mustererkennung anbieten. Unternehmen können damit den Schutz von Daten im Rahmen von internationalen Standards und gesetzlichen Vorgaben sowie von Daten gewährleisten, die immaterielle Werte repräsentieren. Da die Anforderungen an die Erkennungstechnologie stetig steigen, geht Endpoint Protector einen Schritt weiter und entwickelt Next-Generation-DLP mit dynamischen Verfahren, die für die Erkennung unternehmensspezifischer Inhalte trainiert werden können. ■

Messestand: Halle 10.0, Stand 10.0-109

IT-Container

Sichere Edge-Rechenzentren für die Industrie

Moderne Produktionsanlagen liefern laufend wertvolle Datenströme. Genutzt werden kann dieser Datenschatz aber nur mit leistungsfähigen Rechenzentren und zwar in direkter Nähe zur Produktion. Daher benötigen Unternehmen ein Konzept, um schnell und sicher neue Rechenkapazität direkt an den Datenquellen und damit auch in Fabrikhallen zu realisieren. Modular aufgebaute Edge-Datacenter bieten dafür die passende Lösung, die sich in Form eines Containers auf dem Firmengelände und ebenso in Fabrikhallen aufstellen lässt.

Von Bernd Hanstein, Rittal

Edge-Datacenter sind dezentrale IT-Systeme, die Rechenleistung direkt an den Ort der Datenerzeugung bringen. Sie stehen in unmittelbarer Nähe der Datenquellen und unterstützen damit eine schnelle Daten-Erstverarbeitung. Darüber hinaus sind sie mit Cloud-Rechenzentren verbunden, da dort eine nachgelagerte Auswertung stattfindet. Software-Anwendungen in angeschlossenen Rechenzentren nutzen schließlich die aktuellen Daten, um rechenintensive Analysen durchzuführen.

Schlüsselfertig: Im sofort einsetzbaren, schlüsselfertigen Cloud-Rechenzentrum von Rittal und iNNOVO Cloud sind von den IT Racks über die Klimatechnik bis hin zur Stromversorgung alle wichtigen Komponenten enthalten. Eine redundante Stromversorgung (A + B) garantiert eine hohe Ausfallsicherheit.

Ein Edge-Rechenzentrum ist so konzipiert, dass Unternehmen die Lösung über vorkonfigurierte, standardisierte Module an die benötigte Leistungsfähigkeit anpassen können. Module für Klimatisierung und Stromversorgung sowie IT-Racks und Sicherheitskomponenten sind bereits aufeinander abgestimmt.

Anforderungen bestimmen die Konfiguration

Je nach Anforderung und Einsatzgebiet gibt es ganz unterschiedliche Leistungsklassen von Edge-Systemen. Diese übernehmen beispielsweise als Edge-Gateway Aufgaben zur Datenkonsolidierung direkt vor Ort und initiieren anschließend den Transfer in nachgelagerte Cloud-Rechenzentren. Aber auch erste Analysen und Auswertungen nahe an der Datenquelle sind damit möglich. Kleinere Systeme übernehmen zum Beispiel die erste Aggregation von Sensordaten in einer Fertigungsstraße und tragen so dazu bei, Abläufe in der Produktion weiter zu optimieren. Es sind aber auch Edge-Datacenter verfügbar, die als leistungsstarkes Rechenzentrum die Rechenleistung an dem jeweiligen Standort erheblich steigern.

Die Auswahl der benötigten Lösung und Leistungsklasse richtet sich nach den Geschäftszielen. Davon leiten Fach- und IT-Experten die passenden Software-Anwendungen ab. Basierend auf diesem Anforderungskatalog wird die Konfiguration eines Edge-Datacenters bestimmt. Eine Reihe von Kriterien ist hierbei zu beachten: So müssen Edge-Systeme schnell und unkompliziert

einsetzbar sein, damit sich die Anforderungen aus den Fachbereichen zeitnah umsetzen lassen. Ideal ist ein Komplettsystem, das der Hersteller fertig montiert übergibt, das im Plug-and-Play-Verfahren an Energieversorgung und Netzwerktechnik angeschlossen wird und bei dem die Kälteversorgung bereits implementiert ist.

Zum Aufbau der Rechenzentren eignen sich häufig Containerlösungen. Zu den generellen Vorteilen von IT-Containern zählen die Stabilität und Sicherheit durch die Verwendung von Stahlwänden sowie die hohe Mobilität der Lösung, die es erlaubt, ein Rechenzentrum sehr flexibel auf dem Firmengelände oder innerhalb von Lager- und Produktionshallen aufzustellen. Die technische Ausführung dieser Varianten kann ganz unterschiedlich ausfallen, beispielsweise als einfacher Technikschrank oder auf Basis eines speziell gesicherten IT-Racks, das mit einer zusätzlichen Schutzhülle umgeben ist. Wer mehr Leistung benötigt, realisiert ein leistungsstarkes Edge-Datacenter auf Basis eines modularen Rechenzentrums-Containers mit wetterfester Ummantelung. Eine solche Lösung wird in direkter Nähe der Datenerzeugung innerhalb oder außerhalb von Gebäuden aufgestellt und unterstützt bei entsprechender Kühltechnologie eine Leistung von bis zu 35 kW pro IT-Rack.

Weiterhin sollte der Betrieb von Edge-Systemen automatisiert und weitgehend wartungsfrei erfolgen, um die laufenden Kosten zu verringern. Dafür ist ein umfassendes Monitoring notwendig, das die Stromversorgung, die Kühlung sowie eine Branderkennung und -löschung umfasst.

Produktionsausfall vermeiden

Für weitergehende Sicherheitsansprüche lässt sich ein Edge-Datacenter in einer Raum-in-Raum-Umgebung errichten: Eine solche Sicherheitszelle bietet höchsten Schutz bei Staub, Schmutz und Feuer. Während in Büroumgebungen die IP-22-Schutzart (IP = International Protection) ausreicht, benötigen Industrie-4.0-Installationen Schutzarten bis IP 55. Derart gesicherte Schränke helfen dabei, schädliche Staubablagerungen im Innern zu vermeiden. Außerdem verfügen sie über einen vollständigen Berührungsschutz und sind gegen Strahlwasser aus allen Richtungen geschützt. Für den Brandschutz sind ebenfalls geeignete Lösungen notwendig, wie eine im Technikschrank installierte Löschanlage. Diese sollte eine Brandfrüherkennung und ein Aktivlöschsystem verwenden, um zu verhindern, dass es zu einem größeren Feuer kommt. Somit muss ein Unternehmen weder die komplette Produktion stoppen noch die Fabrikhalle evakuieren, weil das Netzteil eines Netzwerkverteilers zu schmoren anfängt.

Welche Schutzklasse für den physischen Schutz letztlich notwendig ist, entscheiden Faktoren wie der Standort oder die benötigte Ausfallsicherheit. Darüber hinaus ist es wichtig, Gehäuse- und Rack-Türen sowie die Seitenwände der Racks zu überwachen. Elektronische

Ausgezeichneter Standort: Smarte Anwendungen und Edge-Szenarien benötigen kurze Latenzzeiten. So ist der Cloudpark Höchst für Unternehmen aus der Frankfurter Region ein ausgezeichneter Datacenter-Standort. Hier sorgen schlüsselfertige IT-Container von Rittal für den schnellen und sicheren Aufbau von IT-Ressourcen.

Hohe Mobilität: Mit den modularen, skalierbaren Datacenter-Containern von Rittal können Unternehmen ihre IT-Infrastruktur schnell, ausfallsicher und flexibel modernisieren.

Türschlösser erleichtern zudem die Auswertung, wann welche Mitarbeiter Zugriff auf die IT hatten. Bei einer Fernwartung oder in Notfällen kann es notwendig sein, das System komplett herunterzufahren und dafür auch die Stromversorgung zu unterbrechen. Hierfür werden schaltbare Power Distribution Units benötigt.

Mit Edge mehr Sicherheit erreichen

Unternehmen aus der Stahlindustrie nutzen bereits sichere Edge-Infrastrukturen mit IT-Containern. Diese Unternehmen möchten ihre Daten aus Forschung, Produktentwicklung, Fertigung oder Kundenservice unternehmensweit verwenden. Um die hohen Datenmengen verarbeiten zu können, passen die Organisationen ihre IT-Infrastruktur entsprechend an. In einem konkreten Projekt fertigt ein führender Stahlhersteller im Ruhrgebiet mehrere Hundert Stahlprodukte in stark automatisierten Fertigungsstätten. Viele Abläufe werden hier über Sensoren und Roboter gesteuert, sodass leistungsfähige IT-Systeme in unmittelbarer Nähe der Produktionsstandorte notwendig sind. Niedrige Latenzzeiten und schnelle Datenverfügbarkeit gehören damit zu den zentralen Anforderungen an die Edge-Systeme. Gleichzeitig muss die IT-Infrastruktur vor unbefugtem Zugriff und den rauen Produktionsumgebungen geschützt werden – hier bieten IT-Container mit IP-56-Schutzklasse die notwendige Sicherheit.

Das Ergebnis: Mit flexibel skalierbaren Edge-Systemen gelingt es Unternehmen in der Stahlindustrie, die IT-Infrastruktur unter Einhaltung höchster Sicherheitsstandards an den jeweiligen Stand der Digitalisierungsinitiativen anzupassen und IT-Ressourcen aus der Cloud zu integrieren. Auf Grundlage neu gewonnener Daten sowie immer mehr IT-gestützter Abläufe können schließlich neue Dienstleistungen entstehen, wie eine Wartung für Stahlerzeugnisse sowie weitere Smart Services. ■

Messestand: Halle 9, Stand 9-604

[sysob]:::®
IT-Distribution GmbH & Co.KG

Werden Sie zum MSP – gemeinsam mit sysob!

Mit der Deutschen Backup Cloud und sysob WaaS bieten wir Ihnen zwei leistungsfähige Managed-Service-Angebote, die Sie einfach und kostengünstig bei Ihren Kunden installieren können.

Bieten Sie Ihren Kunden Full Service mit minimalem Aufwand und höchsten Sicherheitsstandards – alle Daten werden in einem deutschen Rechenzentrum DSGVO-konform vorgehalten.

Als Ihr starker Partner unterstützen wir Sie mit:

» Lösungen am Puls der Zeit
» Komplettem Projektsupport
» Maßgeschneiderten Finanzierungsmodellen
» Logistikservices
» Kompetentem und persönlichem Support bei der Integration von Managed Services
» Trainings- und Weiterbildungsangeboten – inklusive Zertifizierungen

DEUTSCHE BACKUP CLOUD

SYSOB.WAAS
WLAN AS A SERVICE

Informieren Sie sich jetzt!
http://www.sysob.com/hersteller/deutsche-backup-cloud/
http://www.sysob.com/hersteller/sysob-waas/

Oder treffen Sie uns und unsere Herstellerpartner **ARTEC IT-Solutions, Clavister** und **Yubico** persönlich auf der it-sa 2018, Halle 9, Stand 446

ARTEC IT Solutions »Turning Data Into Information«
clavister CONNECT . PROTECT
yubico

sysob IT-Distribution GmbH & Co. KG
Telefon: +49 (0) 9467 / 7406-0
Email: info@sysob.com

SECURE BUSINESS.

www.sysob.com

essendi it
IT-Beratung und -Entwicklung

essendi xc

Besseres Zertifikatsmanagement

Multi-CA

ANBINDUNG INTERNER UND EXTERNER TRUSTCENTER

Einfache Zertifikatsprozesse

PROZESSAUTOMATION UND SELF-SERVICE-PORTAL

Benachrichtigungen & Alerts

FRÜHZEITIGE INFORMATION ÜBER ABLAUFENDE ZERTIFIKATE

Diese und weitere Funktionen präsentieren wir Ihnen in unserer Live-Demo auf der it-sa. Besuchen Sie uns in Halle 10.0 am Stand 10.0-520.

Digitale Bedrohung:

Kritische Infrastrukturen im Fokus

nadla / Getty Images/iStockphoto

Die Digitalisierung und Vernetzung aller Versorgungsbereiche bilden das Grundgerüst unseres modernen Lebensstandards. Bei aller Effizienz sind jedoch genau diese Systeme besonders anfällig für Manipulation und Sabotage.

Von Alexander Häußler, TÜV SÜD Management Service GmbH

Es ist nur ein Szenario unter vielen: Die Infrastruktur eines Stromanbieters wird angegriffen und die Elektrizitätsversorgung in den deutschen Großstädten über einen längeren Zeitraum unterbrochen. Sämtliche lebenswichtigen Infrastrukturen, einschließlich Gesundheitsversorgung, Transport und Kommunikation, kämen zum Erliegen oder stünden nur noch eingeschränkt zur Verfügung.

Was vor Jahren noch wie Science-Fiction anmutete, ist zur realen Gefahr geworden: Regelmäßig warnt der Verfassungsschutz vor Cyberkriminellen, die kritische Infrastrukturen auch in Deutschland im Visier haben. Die Bedrohung kann von Einzelpersonen und Gruppen, privaten Organisationen oder auch ausländischen Geheimdiensten ausgehen – Erpressung, Missbrauch vertraulicher Daten, Industriespionage bis hin zu terroristischen Anschlägen sind nur einige ihrer Motive. In jedem Fall haben die Angriffe das Potenzial, die wirtschaftliche Stabilität eines Landes und die physische Sicherheit der Bürger massiv zu gefährden.

Individueller Schutz nach Stand der Technik

Seit 2015 definieren das IT-Sicherheitsgesetz und in dessen Folge die KRITIS-Verordnung, welche Wirtschaftsbereiche aufgrund ihrer zentralen Bedeutung für die Bevölkerung als kritische Infrastrukturen gelten und besonders gegen Angriffe aus dem Netz geschützt werden müssen. Seit Inkrafttreten der Verordnung im Mai 2016 müssen Betreiber aus diesen kritischen Sektoren – darunter Energie, Wasser, Ernährung und Gesundheit – regelmäßig nachweisen, dass sie angemessene technische und organisatorische Maßnahmen nach dem „Stand der Technik“ ergriffen haben, um ihre Systeme zu schützen. Das beinhaltet unter anderem die Umsetzung eines Informationssicherheitsmanagementsystems, zum Beispiel nach dem international anerkannten Standard ISO/IEC 27001.

Im Rahmen dieses Managementsystems müssen sich Unternehmen sorgfältig mit allen bestehenden Risiken auseinandersetzen, ihre wichtigen Assets und betriebskritischen Systeme definieren und entsprechende Schutzmaßnahmen ableiten. Letztlich geht es um den konsequenten Aufbau einer mehrstufigen Tiefenverteidigung mit möglichst vielen Schutzwällen. Wichtige Hilfestellungen liefert dabei insbesondere Anhang A der ISO 27001.

Zertifizierung und Nachweisführung

Die Wirksamkeit der ergriffenen Maßnahmen muss regelmäßig

geprüft und im Audit nachgewiesen werden. Unabhängige Prüfstellen, wie zum Beispiel TÜV SÜD, helfen KRITIS-Betreibern bei der Erfassung und Bewertung von Sicherheitsrisiken, evaluieren die Einhaltung der Standards und unterstützen bei der Nachweisführung, zum Beispiel durch eine Zertifizierung nach ISO 27001. Um die Zertifizierung zu erhalten, definiert der Betreiber zunächst den Geltungsbereich des Informationssicherheitsmanagementsystems und erstellt einen Maßnahmenplan. Nach einem internen Vor-Audit muss zusätzlich ein unabhängiger Prüfer bestätigen, dass die IT-Sicherheitsvorkehrungen dem vom BSI geforderten „Stand der Technik" entsprechen.

Unternehmen sind zudem in der Pflicht, die Ursachen für Schäden, Störungen und Sicherheitsrisiken systematisch zu erfassen und zu bewerten. Im Zuge von Penetrationstests beispielsweise lassen sich Schwachstellen in den Systemen identifizieren. Darauf folgt eine Ursachenanalyse, da Sicherheitslücken häufig auf eine unterschwellige Prozessschwäche zurückzuführen sind. Wird beispielsweise ein System-Update nicht korrekt ausgeführt, genügt es nicht, die Versäumnisse nachträglich zu bereinigen. Vielmehr gilt es, die Ursache für das fehlerhafte Update aufzudecken und sicherzustellen, dass eine solche Lücke in Zukunft nicht mehr entsteht. Das kann beispielsweise durch Mitarbeiterschulung, Einspielen von Software-Updates oder Abschaltung eines bestimmten Systems geschehen.

Sicherheitsrisiken kennen: beliebte Angriffspunkte

Aller Vorsorge zum Trotz bestehen intern Restrisiken, die Unternehmen nur eingeschränkt beeinflussen können, wie veraltete Technik oder die Lieferkette über Lieferanten und Dienstleister. Zu den beliebtesten Angriffspunkten zählen außerdem die eigenen Mitarbeiter, die Hackern ungewollt Zugang zum Unternehmensnetzwerk verschaffen – ein einziger unbedachter Klick genügt.

Weit verbreitet sind beispielsweise Phishing-E-Mails, die Versprechungen oder Androhungen enthalten. Geht man von einem organisierten Angriff auf eine kritische Infrastruktur durch einen ausländischen Geheimdienst aus, sind Phishing-E-Mails in der Regel professionell aufgebaut und dadurch nicht mehr als Fälschung erkennbar, man spricht dann vom sogenannten Spear-Phishing. Sie wirken seriös und werden arglos geöffnet, um die Aufforderungen darin zu befolgen.

Durch gezielte Aufklärung und technische Einschränkungen lässt sich diese Gefahr reduzieren. Mitarbeiter müssen für die Bedrohungslage und gängige Methoden von Hackern sensibilisiert werden. Auf technischer Ebene gilt es, Zugriffsrechte für bestimmte Dokumente, Ordner und Strukturen genau festzulegen und so weit wie möglich zu limitieren.

Die Lieferkette im Fokus

Externe Geschäftspartner, wie Lieferanten und Dienstleister, stellen ein weiteres Risiko dar. Häufig können sie auf Teilbereiche des Unternehmensnetzwerks zugreifen, wodurch sich günstige Angriffspunkte ergeben. Im vergangenen Jahr wurden Unternehmen in mehreren Fällen nicht direkt, sondern über die Lieferkette attackiert, beispielsweise über die Nutzung von Drittanbietersoftware. KRITIS-Betreiber müssen sich dieser Gefahr bewusst sein und bei der Auswahl und im Umgang mit Lieferanten besondere Vorsicht walten lassen. ISO 27001 gibt zu diesem Thema ebenfalls einen verbindlichen Handlungsrahmen vor. Wichtig ist unter anderem, einen klar definierten Zugang sowie standardisierte Verfahren einzurichten, über die Lieferanten und Sub-Lieferanten an das Unternehmensnetzwerk angebunden werden.

Die lange Laufzeit von Energieanlagen bringt weitere Sicherheitsherausforderungen mit sich. Kraftwerke und andere kritische Infrastrukturen sind oft über mehrere Jahre oder gar Jahrzehnte hinweg in Betrieb. Unter dieser Voraussetzung wird das Einspielen von Sicherheitsupdates nach einer gewissen Zeit schwierig, weil die veralteten Komponenten nicht immer mit den aktuellen Updates kompatibel sind. Unternehmen müssen also Alternativen planen, um weiterhin konform zu sein. Eine nachträgliche Erweiterung der kritischen Infrastruktur darf bei aller Berücksichtigung der Wirtschaftlichkeit nie zulasten der Sicherheit gehen. Betreiber sind in der Pflicht, entsprechende Vorkehrungen zu treffen.

Ausblick

Das IT-Sicherheitsniveau in Deutschland ist vergleichsweise hoch, nicht zuletzt durch die verschärfte Gesetzgebung. Allerdings ist in den nächsten Jahren eine weitere Verschärfung der Bedrohungslage zu erwarten – Werkzeuge und Methoden für Cyberangriffe lassen sich einfacher denn je mit geringem Kostenaufwand beschaffen. Insgesamt zeichnet sich eine deutliche Professionalisierung der Attacken mit zunehmender Verlagerung in den politischen Raum ab. Unternehmen, insbesondere Betreiber kritischer Infrastrukturen, müssen sich dieser Dynamik kontinuierlich anpassen, um nicht schleichend in Rückstand zu geraten. Politik und internationale Organisationen sind gefordert, ihre Zusammenarbeit weiter zu verstärken, um auch in Zukunft Angriffe rechtzeitig erkennen und abwehren zu können. Angesichts der steigenden kriminellen Energie werden bisherige Schutzmaßnahmen zukünftig nicht mehr ausreichen. ■

Messestand: Halle 9, Stand 9-458

infodas

Ihre Sicherheit.
Unser Auftrag.

IT-Grundschutz hybrid managen

SAVe

Made in Germany
100%
BSI lizensiert

Besuchen Sie uns auf der it-sa 2018 I Halle 9 I Stand 315

–
Kontaktieren Sie uns:
+49 221 70912-0 I vertrieb@infodas.de I www.infodas.de

E-Mail-Security

Gezielter Schutz vor Advanced Threats

Immer gezieltere und intelligentere Cyberangriffe, sogenannte Advanced Threats, überschreiten längst die Möglichkeiten konventioneller Abwehrmechanismen. Gegen solche Attacken brauchen Unternehmen einen ebenbürtigen Schutz. Mit innovativen Funktionen einer zeitgemäßen Advanced-Threat-Protection sind sie auf der sicheren Seite.

Von Martin Mathlouthi, Retarus

Ein Großteil der elektronischen Kommunikation besteht aus unerwünschten Nachrichten: Neben der Flut aus Spam- und Viren-E-Mails sehen sich Unternehmen und Mitarbeiter zunehmend auch mit komplexen Bedrohungen wie Social Engineering oder ausgefeilten Phishing-Angriffen konfrontiert. Traditionelle Sicherheitsmechanismen bieten vor solchen individualisierten E-Mails oft keinen ausreichenden Schutz mehr. Zudem wird bereits bekannte Malware in immer kürzeren Zeitabständen abgewandelt und kursiert binnen kürzester Zeit in neuen Varianten, die von den gängigen Virenschutzlösungen häufig nicht gleich erkannt und somit nicht sofort herausgefiltert werden können. Einmal ins Postfach eines Users gelangt, breitet sich Malware ungehindert in der gesamten IT-Infrastruktur aus. Gezielter Datendiebstahl, Identitätsmissbrauch, gesperrte Festplatten, kompromittierte Infrastruktur und ein zeitweise sogar komplett lahmgelegter Geschäftsbetrieb sind die Folge.

Um den bestmöglichen Schutz der E-Mail-Kommunikation sicherzustellen und sich für neuartige Bedrohungen zu wappnen, müssen bestehende Sicherheitskonzepte kontinuierlich aktualisiert und an den aktuellen Stand der Technik angepasst werden. All diese Anforderungen mit selbst betriebenen Systemen zu erfüllen, ist nahezu unmöglich. Unternehmen benötigen daher eine intelligente Kombination aus bewährtem, präventiv blockierendem Virenschutz und neuen Methoden zur Reaktion und Analyse.

Schutz durch Advanced-Threat-Protection

Für ein erhöhtes Sicherheitslevel bieten professionelle E-Mail-Security-Services daher mittlerweile auch umfangreiche Funktionen zur Advanced-Threat-Protection, die auch E-Mail-Angebote aus der Cloud wie Office 365 oder G Suite sinnvoll ergänzen können. So umfassen beispielsweise die Retarus-Dienste ausgefeilte Schutzmechanismen wie Deferred Delivery-Scan, Sandboxing, External-Sender-Visibility-Enhancement, CxO-Fraud-Detection und Time-of-Click-Protection.

Beim Deferred Delivery-Scan handelt es sich um einen zeitlich versetzten Re-Scan ausgewählter Dateianhänge. Hierfür wird die Zustellung der E-Mail an den Empfänger für wenige Minuten verzögert: Bei einem nachgelagerten erneuten Scan können, insbesondere bei Angriffen mit brandneuer Malware, schon nach kurzer Zeit aktualisierte Virensignaturen vorliegen, die bei der ersten Überprüfung noch nicht verfügbar waren.

Insbesondere bei der Abwehr von Zero-Day-Exploits, also bei noch nicht öffentlich bekannten Schwachstellen, spielt Sandboxing eine entscheidende Rolle. Unbekannte, verdächtige Dateien im E-Mail-Anhang werden vor der Zustellung durch die Sandbox-Mechanismen in einer sicheren Testumgebung überprüft. Neben einer tiefgehenden Überprüfung auf ein mögliches ungewöhnliches Verhalten durch komplexe Simulationsverfahren werden auch bekannte global verfügbare Prüfergebnisse sowie Machine-Learning-Mechanismen für eine Überprüfung herangezogen.

Zusätzlich lassen sich mit Time-of-Click-Protection auch neuartige Phishing-Angriffe und der damit einhergehende Verlust sensibler Daten verhindern. Die Technik überprüft alle in E-Mails enthaltenen Links auf Phishing-verdächtige Zieladressen. Dafür werden zunächst alle URLs in eingehenden E-Mails automatisiert umgeschrieben (sogenanntes URL-Rewriting). Immer wenn Empfänger einen solchen Link

anklicken, wird die dahinterliegende Webseite erneut auf mögliche Schädlichkeit überprüft. Falls zwischenzeitlich neue Erkenntnisse vorliegen, wird diese blockiert und dem Nutzer stattdessen eine Sicherheitswarnung angezeigt.

External-Sender-Visibility-Enhancement und CxO-Fraud-Detection dienen der Abwehr von besonders raffinierten Social-Engineering-Attacken: Beim CEO-Fraud (auch als „Fake President Fraud" bekannt) handelt es sich um eine Betrugsmasche, bei der sich Cyberkriminelle als Geschäftsführer eines Unternehmens ausgeben und ihre Opfer per E-Mail dazu auffordern, im Rahmen einer dringlichen, vertraulichen Angelegenheit – wie beispielsweise der Akquisition eines Unternehmens – hohe Geldsummen zu überweisen. Um glaubwürdig zu wirken, recherchieren die Absender im Vorfeld der Attacke sowohl Namen und E-Mail-Adresse des Firmenchefs als auch von Personen, die Zugang zu sensiblen Daten haben oder zahlungsberechtigt sein könnten.

Hier setzt External-Sender-Visibility-Enhancement an. Die Funktion markiert bereits im Empfängerfeld eingehende Nachrichten deutlich, die im Absender eine nur scheinbar zum Unternehmen gehörige Absenderdomäne verwenden. Noch einen Schritt weiter geht die CxO-Fraud-Detection: Diese erkennt gefälschte Absenderadressen rechtzeitig und warnt die Empfänger der E-Mails. Dafür kommen neben einer fortschrittlichen Analyse des E-Mail-Headers auch spezialisierte Algorithmen zum Einsatz, die sogenanntes From- oder Domain-Spoofing zuverlässig identifizieren.

Post-delivery-Protection bei bereits zugestellten E-Mails

In Sachen E-Mail-Sicherheit optimal aufgestellt sind Unternehmen, die neben einer Lösung zur Advanced-Threat-Protection auch Mechanismen zur Post-delivery-Protection einsetzen. Denn häufig werden Virenpattern erst bekannt, wenn die Malware via E-Mail bereits in die Unternehmensinfrastruktur gelangt ist. Mittels Post-delivery-Protection lassen sich betroffene Systeme schnell identifizieren. So erzeugt die von Retarus entwickelte und zum Patent angemeldete Technologie Patient-Zero-Detection schon beim Eingang einer E-Mail einen digitalen Fingerabdruck aller Attachments sowie der enthaltenen URLs. Sobald Retarus E-Mail-Security später bei einem anderen Empfänger 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 Alarme dabei automatisiert verarbeiten. Da die Virenscanner bei Retarus kontinuierlich aktualisiert werden, können Administratoren in der Regel so schnell alarmiert werden, dass infizierte E-Mails noch gar nicht geöffnet wurden und unmittelbar gelöscht werden können.

Alles im Blick

Bei der Entscheidung für eine umfassende E-Mail-Security-Lösung sollten Unternehmen auch darauf achten, dass diese Monitoring- und Analyse-Methodiken zur Verfügung stellt. So bietet beispielsweise Retarus das zentrale Suchportal E-Mail-Live-Search. Damit können Administratoren für jede Nachricht genau nachvollziehen, wann welche E-Mail-Security-Filter und -Regeln angewendet wurden. Das Web-Interface liefert detaillierte Ergebnisse in Echtzeit und ermöglicht eine schnelle Analyse und IT-Forensik. Um die Unternehmensnetzwerke im Falle zukünftiger Angriffe besser zu schützen, lassen sich auf Basis der Suchergebnisse die Systemeinstellungen optimieren. Forensic-SIEM-Integration bietet zusätzlich die Möglichkeit, forensische Daten (Events) in Echtzeit bereitzustellen und per API einfach in bestehende SIEM-Tools zu integrieren. Auf diese Weise kann der Datenstrom unkompliziert mit zusätzlichen Details zur E-Mail-Sicherheit angereichert werden.

Messestand: Halle 10.1, Stand 10.1-710

Vorträge von Retarus auf der it-sa

Catch me if you can – Die Tricks der E-Mail-Betrüger
am Mittwoch, 10.10.2018, 11.45 Uhr oder
Donnerstag, 11.10. 2018, 10.30 Uhr
im Management Forum M10 in Halle 10.1 (26).
Sprecher: Martin Mathlouthi, Product Line Manager E-Mail-Security bei Retarus

Rezertifizierung von Zugriffsrechten auf schützenswerte Daten

Mit Netz und doppeltem Boden

Mitarbeiterberechtigungen sind im Laufe der Zeit einem unkontrollierten Wachstum ausgesetzt. Durch die Kombination einer Automatisierung des Zugriffsmanagements mit der regelmäßigen Überprüfung bestehender Rechte lassen sich das Pflichtbewusstsein in den Fachabteilungen und die Datensicherheit optimieren.

Von Svenja Winkler, BAYOONET AG

Need-to-know heißt das Prinzip, durch welches Mitarbeiter ausschließlich bei Bedarf Kenntnis von Daten im Unternehmen erlangen sollen. In Bezug auf Zugriffsrechte sollen sie nur solche Berechtigungen erhalten, die sie wirklich für ihre tägliche Arbeit benötigen. Häufig kommt diese Vorgehensweise bei der Vergabe zum Einsatz: Neue Mitarbeiter treten dem Unternehmen bei, Mitarbeiter wechseln eine Abteilung oder arbeiten in neuen Projekten, Auszubildende wandern durch verschiedenste Bereiche, um möglichst viele Erfahrungen zu sammeln. Um diese Mitarbeiter nicht warten zu lassen, werden Berechtigungen schnell und dabei großzügig, zum Beispiel auf Abteilungsebene, vergeben oder es werden Vergleichsbenutzer mit ähnlichem Aufgabengebiet herangezogen. Oft wird dabei jedoch vernachlässigt, diese schnellen Berechtigungsänderungen zu dokumentieren oder zu prüfen, ob bereits bestehende Berechtigungen weiterhin benötigt werden. In der Praxis gibt es hier zusätzlich Übergangsfristen, sodass das Wochen später anstehende Entfernen von nicht mehr benötigten Rechten durch diesen Zeitversatz häufig vernachlässigt oder vergessen wird. Somit steigen die Berechtigungen eines Mitarbeiters mit zunehmender Unternehmenszugehörigkeit immer weiter an – ob diese Rechte auch nach Jahren tatsächlich noch benötigt werden, ist offen.

Um diesem unkontrollierten Wachstum an Berechtigungen vorzubeugen, empfehlen Auditoren die Rezertifizierung oder auch Attestierung der Berechtigungen, wodurch zusätzlich die rechtlichen Anforderungen, wie der Sarbanes-Oxley-Act der Finanzbranche, erfüllt werden sollen. Datenverantwortliche sollen in regelmäßigen Abständen die bestehende Rechtesituation überprüfen. Werden hierbei nicht mehr erforderliche Berechtigungen entdeckt, sollen diese den entsprechenden Mitarbeitern als Maßnahme zur Risikominderung entzogen werden. Dieser wiederkehrende Prozess führt insbesondere bei Führungskräften zu wenig Begeisterung – bedeutet er doch erhebliche Mehraufwände sowie eine Auseinandersetzung mit technischen Details oder Papierbergen voll komplexer Matrizen über die vollständige Berechtigungssituation. Solche intransparenten und unübersichtlichen Informationen stellen massive Hürden dar, welche die Zielerreichung eines Überprüfungsprozesses erheblich gefährden.

Automatisierung schützt

Soll das Need-to-Know-Prinzip eingehalten werden, ist es erforderlich, bestehende Hürden so weit wie möglich zu reduzieren. Ein seit zehn Jahren erprobter Lösungsansatz stellt die Fileserver Management Suite durch ihre Automatisierung des Berechtigungsmanagements für Fileserver, SharePoint und Active Directory dar. Die Softwarelösung etabliert Datenschutz als Default und überwacht die tatsächliche Berechtigungssituation durch einen kontinuierlichen Abgleich mit dem genehmigten und auditierten Stand an Berechtigungen. Dabei wird die technische Umsetzung vollständig vom System übernommen, ein Mitwirken der IT-Administration kann auf Wunsch komplett entfallen. Diese Automatisierung ermöglicht eine Berechtigungsverwaltung direkt durch die Datenverantwortlichen. Sie können durch eine übersichtliche und leicht verständliche Darstellung der notwendigen Informationen ohne technisches Hintergrundwissen und ohne IT-Unterstützung transparent und revisionssicher Zugriffsrechte auf die von ihnen verantworteten Ressourcen verwalten.

Die Kombination einer Vergabe von persönlichen Berechtigungen mit dem Einsatz des integrierten Profilmanagements für die Abbildung von Organisationsstrukturen ersetzt die Notwendigkeit, Berechtigungen eines anderen Benutzers zu kopieren oder diese für gesamte Abteilungen vergeben zu müssen. Gemeinsam mit der Möglichkeit, Ablaufdaten zum automatischen Entfernen nicht mehr benötigter Rechte zu definieren, liefert die Fileserver Management Suite einen zuverlässigen Weg, das unkontrollierte Anhäufen von Berechtigungen

einzudämmen und dabei die Akzeptanz bei den Datenverantwortlichen durch Transparenz zu fördern.

Regelmäßige Prüfung bestehender Rechte

Um das Risiko ungewollter Zugriffe auf schützenswerte Daten weiter zu reduzieren, kommt ergänzend zum kontinuierlichen Abgleich des Zielsystems das Reapproval für alle verwalteten Zugriffsrechte auf Fileservern, SharePoint und im Active Directory zum Einsatz. Diese Funktion überträgt das Berechtigungsmanagementkonzept mit einer intuitiven Bedienung über den Browser, sodass der Prozess der Rezertifizierung vereinfacht und beschleunigt wird.

Datenverantwortliche erhalten zum Stichtag eine E-Mail, welche sie über die zu überprüfenden Ressourcen informiert. Auf der Weboberfläche werden daraufhin für den Prozess nicht relevante sowie bereits überprüfte Ressourcen ausgefiltert und lediglich anstehende Prüfungen dargestellt. Entscheidungen können so intuitiv und einfach per „ja/nein" bestätigt oder widerrufen werden.

Durch die Möglichkeit, multiple Datenverantwortliche pro Ressource zu definieren, kann die Bearbeitung auf verschiedene Köpfe verteilt werden. Somit wird der Prozess der Rezertifizierung für Datenverantwortliche so einfach wie möglich gestaltet. Sie werden nicht mit Papierbergen oder komplexem IT-Fachwissen konfrontiert und können ihre Aufgabe effizient bearbeiten. Das ermöglicht die Reduzierung der Rezertifizierungshürde, um so den Erfolg eines redundanten Monitorings für die im Unternehmen schützenswerten Daten zu gewährleisten.

DSGVO-Konformität

Auch für die Einhaltung der Datenschutzgrundverordnung ist die Kenntnis über bestehende Rechte und deren Notwendigkeit ein erheblicher Faktor. Um die Erstellung und Aufrechterhaltung des Verzeichnisses für Verarbeitungstätigkeiten zu unterstützen, müssen personenbezogene Daten gemäß Artikel 9 gekennzeichnet und der Verarbeitungszweck definiert werden. Insbesondere an dieser Stelle ist der Einsatz des redundanten Sicherungssystems Rezertifizierung relevant, um die Datenverantwortlichen zu verpflichten, das Thema Datensicherheit ernst zu nehmen. Das Reapproval wird hierfür mit den an den Kategorien der Datenschutzgrundverordnung orientierten Datenschutzklassifizierungen kombiniert. Erhält eine Ressource eine entsprechende Klassifizierung, ist sie automatisch ein Kandidat für die Überprüfung der Berechtigungen und wird zum folgenden Stichtag berücksichtigt.

Redundantes Monitoring für Zugriffsrechte

Fazit

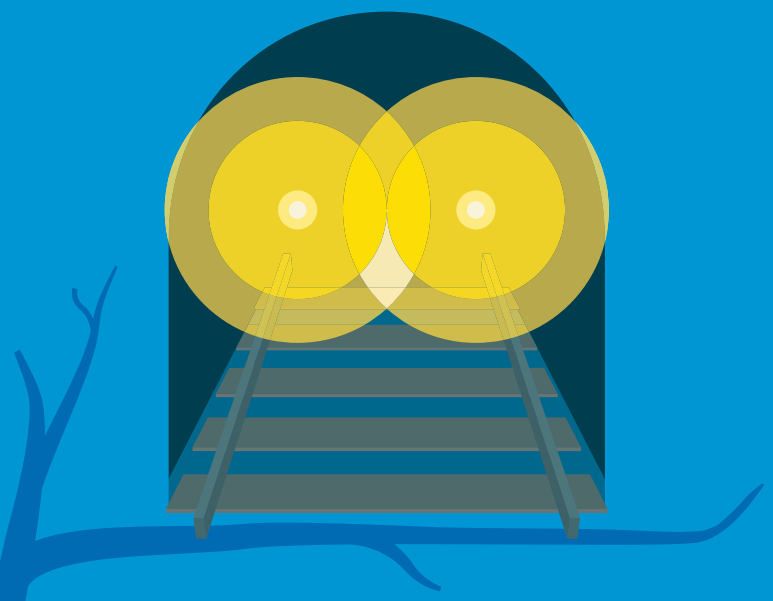
Berechtigungsänderungen aufgrund personeller oder struktureller Veränderungen führen häufig zu einer Abweichung vom Need-to-Know-Prinzip und sorgen damit langfristig durch ein unkontrolliertes Wachstum an Berechtigungen für einen Verlust der Datensicherheit. Durch den Ansatz der Automatisierung bietet die Fileserver Management Suite ein dauerhaftes Monitoring der Fileserver-, SharePoint- und Active-Directory-Rechte und wirkt diesem schleichenden Prozess dauerhaft entgegen. Gleichzeitig werden die Transparenz und das Bewusstsein für Datensicherheit im Unternehmen erhöht. Die Kombination von Datenschutzklassifizierungen als Kennzeichnung besonders schützenswerter Daten mit der redundanten Sicherung durch die leicht verständliche Überprüfung der Berechtigungssituation nehmen dabei die Datenverantwortlichen in die Pflicht, Verantwortung für die Erfüllung der Compliance-Anforderungen zu übernehmen.

Die Fileserver Management Suite ist ein probates Mittel, um dem Zugriffsmanagement im Unternehmen einen doppelten Boden für Datensicherheit zu verleihen und damit bei geringem operativem Aufwand eine dauerhaft revisionssichere Berechtigungssituation zu gewährleisten.

Messestand: Halle 10.0, Stand 10.0-412

Und plötzlich wird aus einem Tunnelblick Rundumsicht.

Verändern wir die Zukunft.
Schärfen wir Ihre Sinne für Cyber-Risiken.



Mehr Angriffe. Mehr Bedrohungen. Mehr Unsicherheit. Sagen Sie Zero-Day-Exploits, Ransomware und Advanced-Persistent-Threats den Kampf an. Denn jedes Unternehmen kann Ziel von Cyberattacken werden. Wenn nicht heute, dann morgen. Die digitale Transformation erfordert neue und veränderte IT-Sicherheitsstrategien. Als erfahrener Partner bieten wir Ihnen Schutz aus einer Hand, finden Ihre Sicherheitslücken, schließen sie und entwickeln mit Ihnen nachhaltige Sicherheitsmaßnahmen für die Zukunft. Die Zukunft ändert sich, weil wir sie ändern.

Erfahren Sie mehr auf **www.kpmg.de/changingfutures**

KPMG

Synchronized Security

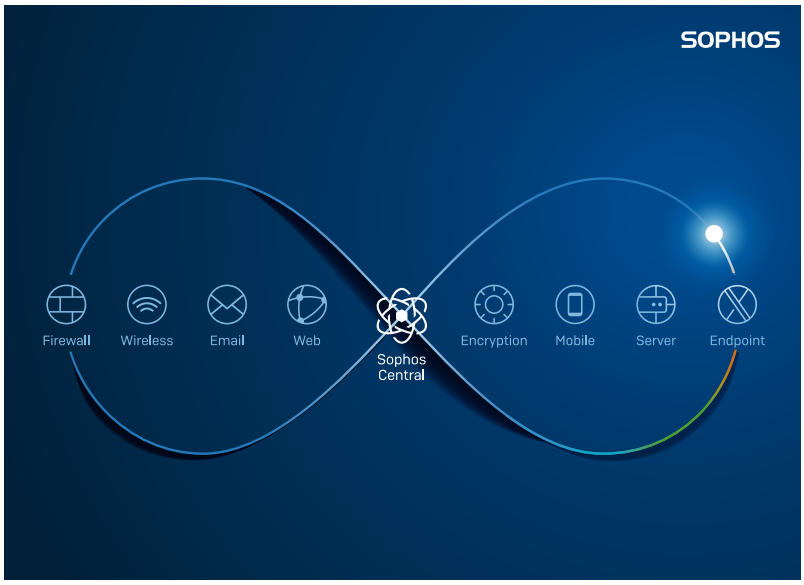
Start in eine neue IT-Security-Welt

Kommunizierende und intelligente Technologie auf dem Vormarsch

Eine moderne Cyberabwehr besteht schon lange nicht mehr aus verschiedenen Silo-Lösungen, sondern lässt ein System entstehen, das Informationen untereinander austauscht. So können in Kombination mit neuester Technologie wie Sandboxing oder Deep Learning auch Zero-Day-Attacken & Co. abgewehrt werden.

Von Michael Veit, Sophos

Jahrelang galt für Unternehmen und öffentliche Einrichtungen in puncto IT-Sicherheit die Maxime „Netzwerk ein Anbieter und Endpoint ein Anbieter – das sorgt für optimalen Schutz“. Doch dieses Mantra gilt heutzutage nicht mehr. Der Grund dafür ist die ständige Weiterentwicklung von Technologie. Das gilt sowohl für Hersteller von IT-Security-Lösungen als auch für die Hackerszene. Tradition ist gut und notwendig – das gilt auch für IT-Sicherheitslösungen. Ohne die Erfahrungen der letzten Jahrzehnte wären Infrastrukturen bei Weitem nicht so gut geschützt, wie sie es heute sind. Allerdings ist das alleinige Vertrauen auf Tradition eine Sackgasse. Es müssen neue Wege gefunden werden, modernen Hackerangriffen einen Riegel vorzuschieben und sich für die Herausforderungen durch immer weiter auflösende Peripherien sowohl in der Geschäfts- als auch Alltagswelt zu wappnen. Es ist heutzutage einfach nicht mehr ausreichend, zwei Produkte mit einer guten Erkennungsrate zu verbinden, um für genügend Schutz zu sorgen. Die Netzwerkgrenzen werden immer durchlässiger und die Verantwortlichen für IT-Sicherheit müssen neue Werkzeuge an die Hand bekommen, um auf die zunehmende Mobilität der Arbeitswelt reagieren zu können.



Synchronized Security über eine zentrale Plattform.

Drei Eckpfeiler sorgen für bestmögliche Sicherheit:

_____ Sicherheit muss umfassend sein: Eine Lösung muss alle Funktionen beinhalten, die notwendig sind, um die Sicherheitsanforderungen gänzlich zu erfüllen – egal ob Netzwerk, Server oder Nutzer.

_____ Sicherheit muss einfach zu managen sein: Diese Einfachheit darf sich nicht auf einzelne Bereiche beschränken, sondern muss sich auf alle Aspekte der Lösung erstrecken, zum Beispiel auf die Bereitstellung, Verwaltung, Lizenzierung, den Support und die Bedienung.

_____ Sicherheit ist effektiver im Teamplay: Wenn Technologiekomponenten kommunizieren und kooperieren, anstatt isoliert voneinander zu agieren, ergeben sich ganz neue Möglichkeiten.

Systeme müssen miteinander kommunizieren

Die immer häufigeren Schlagzeilen über gehackte Behörden, Konzerne oder öffentliche Ein-

richtungen wie Krankenhäuser machen deutlich: Wir stehen an einem Scheideweg in Sachen IT-Sicherheit. Egal ob Sony oder Bundestag, selbst Systeme, bei denen man getrost davon ausgehen darf, dass State-of-the-Art-Lösungen im Einsatz sind, lassen zu viele Lücken zu. Erkennungsraten top, die Firewall perfekt eingerichtet, Technologie wie Advanced-Threat-Protection installiert – und dennoch Einbrüche über den Onlinekanal. Wie kann das sein? Die Antwort ist recht einfach: Während bislang mit den traditionellen Herangehensweisen Hacker meist ausreichend in die Schranken gewiesen werden konnten, haben sich die Cyberkriminellen weiterentwickelt und sind sehr viel versatiler geworden. Diese Flexibilität macht den traditionellen Sicherheitssystemen zu schaffen, da ihnen die Schwarmintelligenz fehlt. Sämtliche Funktionen für sich gesehen funktionieren einwandfrei, aber entscheidend ist heute, dass alle diese Systeme intelligent miteinander verknüpft sind und miteinander kommunizieren. Nur so lassen sich die Lücken zwischen den Lösungen schließen und die immer ausgeklügelteren Attacken erfolgreich abblocken.

Sophos SG UTM und XG Firewall mit „Deep Learning"-Malware-Erkennung

Sophos weitet seine Next-Generation-Security-Strategie auf sein gesamtes Produktportfolio aus. Neben der vernetzten Synchronized Security setzt Sophos auf die Deep-Learning-Technologie, welche zusätzlich zu den bekannten Malware-Varianten auch neue und bisher unbekannte Bedrohungen anhand eines definierten Datenmodells erkennt.

Die Deep-Learning-Technologie wurde im ersten Schritt auf den Sophos Endpoint-Lösungen mit der zusätzlichen Security-Software Intercept X realisiert. Neben den Endpoint-Lösungen profitieren nun auch alle Sophos Firewalls mit der Sandstorm-Option von der Deep-Learning-Security-Technologie. Sowohl die SG UTM-Modelle als auch die XG Firewalls bieten mithilfe des neuronalen Netzwerks einen wesentlich höheren Schutz bei der Erkennung von Malware komplett ohne Signaturen. Die Technologie ermittelt automatisiert verdächtige Dateieigenschaften und kann so Malware erkennen, die speziell dafür entwickelt wurde, traditionelle Security-Lösungen zu umgehen.

Automatisierte Prozesse entlasten die Verwaltung

Synchronisierte Sicherheit beinhaltet einen sicheren Kommunikationskanal zwischen Endpoint- und Netzwerk-Sicherheitslösungen. Erkennt die Firewall schädlichen Datenverkehr, benachrichtigt sie umgehend den Endpoint-Agenten. Dieser reagiert dynamisch, identifiziert und hinterfragt den verdächtigen Prozess. In vielen Fällen kann er den Vorgang automatisch beenden und die restlichen infizierten Komponenten entfernen. Auf diese Weise werden IT-Abteilungen entlastet und können gleichzeitig einen besseren Schutz von Daten garantieren.

Für Entlastung sorgt auch künstliche Intelligenz. In der Cybersicherheits-Branche wird der Begriff „Machine Learning" oder „maschinelles Lernen" allerdings zur Zeit aus verschiedenen Gründen so inflationär gebraucht, dass oftmals gar nicht mehr klar ist, was damit gemeint ist. Am erfolgreichsten kommt zurzeit das sogenannte „Deep Learning", eine fortgeschrittene Form des maschinellen Lernens, in IT-Security-Lösungen zum Einsatz.

Diese Form des „Machine Learning" ähnelt der Funktion des menschlichen Gehirns am ehesten, da zahlreiche Schichten von Neuronen daran beteiligt sind. Genau daher stammt auch der Begriff „künstliches neuronales Netz", denn „künstlich" bedeutet in diesem Fall, dass es sich um eine Nachahmung des neuronalen Netzes des menschlichen Gehirns handelt. Ein künstliches Netz nimmt ebenso wie ein neuronales Netz im Gehirn Input auf, manipuliert diesen auf eine bestimmte Weise und gibt Informationen an andere Neuronen aus. Der größte Unterschied besteht darin, dass das menschliche Gehirn rund 100 Milliarden Neuronen umfasst, während ein künstliches neuronales Netz nicht einmal einen Bruchteil davon aufweist.

Hauptproblem bislang war die Tatsache, dass zur Erstellung eines effektiven Modells riesige Datenmengen und eine hohe Rechenleistung im GB-Bereich benötigt wurden. Das aktuelle Sophos-Trainingsmodell ist allerdings kleiner als 20 MB und benötigt nur selten Updates. Diese Entwicklung lässt nun ganz andere Einsatzmöglichkeiten im Bereich IT-Sicherheit zu. Da sich „Deep Learning" nun problemlos auf Hunderte Millionen Training-Samples skalieren lässt, können Bedrohungen heute genauer als jemals zuvor vorhergesagt werden – ein entscheidender Baustein einer schlagkräftigen Next-Gen-IT-Security-Strategie.

Messestand: Halle 9, Stand 9-426

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.

it sa 2018 Besuchen Sie uns: Halle 10 Stand 120

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

Mobile Smartcard

Das Smartphone als Sicherheitsschlüssel

Immer mehr Menschen verwenden ihr Smartphone für die Arbeit. Deshalb ist es für viele Unternehmen wichtig, auf mobilen Endgeräten ein gleichwertiges Sicherheitsniveau wie am Arbeitsrechner bereitzustellen. Mitarbeiter sollen beispielsweise vom Smartphone aus sicher auf Unternehmensdaten zugreifen können. Ebenso soll ihnen ermöglicht werden, ihre vom Smartphone gesendeten E-Mails zu signieren und zu verschlüsseln, sowie Dokumente von unterwegs zu unterzeichnen.

Von Thorsten Gahrmann, Nexus Group

Viele digitale Geschäftsprozesse verdanken ihre Sicherheit einer Public-Key-Infrastructure (PKI). Innerhalb einer PKI sorgen digitale Zertifikate für die Vertrauenswürdigkeit von Identitäten. Sie stellen sicher, dass sowohl Menschen als auch Geräte und Software einander eindeutig identifizieren und dadurch sicher miteinander kommunizieren können.

Traditionell werden zertifikatsbasierte Identitäten auf Smartcards ausgegeben. Um PKI-Funktionen am Rechner zu nutzen, wird ein Kartenleser benötigt – das ist für mobile Endgeräte alles andere als praktikabel. Viel bequemer ist es, das Mobiltelefon selbst in eine „mobile Smartcard“ zu verwandeln und von der erhöhten Sicherheit zu profitieren, ohne eine physische Karte mit sich führen zu müssen. Folgende Funktionen ließen sich damit bequem auf dem Smartphone nutzen:

- starke Authentifizierung mit PKI-basierter App
- E-Mail-Verschlüsselung und E-Mail-Signaturen (S/MIME)
- digitale Signaturen – Dokumente und Transaktionen „on the fly“ unterzeichnen

Dabei muss jedoch gewährleistet sein, dass die Zertifikate sicher auf dem Gerät bereitgestellt werden, für verschiedene Anwendungen verfügbar sind und über ihren gesamten Lebenszyklus hinweg verwaltet werden.

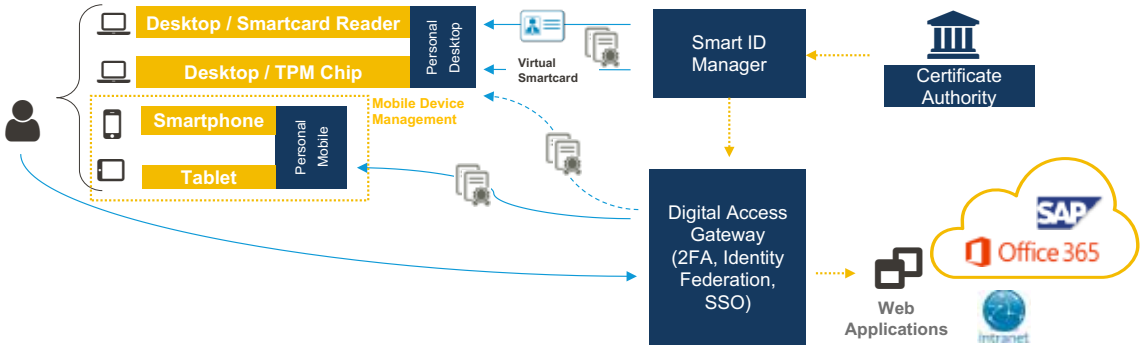
Sichere Zertifikatsbereitstellung

Häufig werden Zertifikate über ein Mobile-Device-Management-(MDM)-System verteilt. Das MDM-System generiert das Zertifikat serverseitig und sendet es an das mobile Endgerät. Diese Methode ist jedoch nicht besonders sicher, da sowohl der öffentliche als auch der private Schlüssel vom Server zum Gerät gesendet werden. Auch wenn diese Verbindung gesichert und verschlüsselt ist – sie bleibt eine Schwachstelle.

Der mobile PKI-Client von Nexus – die App „Personal Mobile“ – generiert das Schlüsselpaar auf dem mobilen Gerät selbst. Dadurch entfällt die Notwendigkeit, privates oder geheimes Schlüsselmaterial über ein Netz zu übertragen. Der private Schlüssel verlässt das Gerät niemals und ist dadurch besonders gut geschützt.

Viele Anbieter von mobilen PKI-Apps greifen bei der Speicherung des privaten Schlüsselmaterials auf standardisierte hardwaregeschützte Bereiche (z. B. System Key Chain) zurück. Der mobile PKI-Client von Nexus kann gleich mehrere Speicherorte bedienen: Ökosysteme von MDM-Anbietern, System Key Chain sowie Speicherung innerhalb der Nexus App selbst. Letztere Möglichkeit bietet wohl den höchsten Grad an Sicherheit: Neben einer Vielzahl von eigenentwickelten Sicherheitsmechanismen und der sicheren Provisionierung nutzt die App moderne Verschlüsselungsalgorithmen zur Absicherung

System-übersicht



des privaten Schlüsselmaterials und führt eine Härtung der App mittels eines Applikationsschutz-Frameworks durch. Darüber hinaus wird die App regelmäßig von unabhängigen Sicherheitsexperten evaluiert.

Nutzung von Zertifikaten

Nexus Personal Mobile kann digitale Zertifikate an drei Stellen speichern:

- im Mobile-Device-Management-App-Ökosystem: Nexus Personal Mobile kann mithilfe entsprechender SDKs Zertifikate (sogenannte „derived credentials") in das App-Ökosystem von MDM-Systemen publizieren, welches sie dann auf sichere Weise allen Anwendungen im System zur Verfügung stellt.
- in der System Key Chain: Hier gespeicherte Zertifikate können auch von Apps außerhalb des MDM-Ökosystems verwendet werden, wie beispielsweise vom E-Mail-Client des Smartphones, von Webbrowsern oder von maßgeschneiderten Geschäftsanwendungen, die mit dem Nexus SDK erstellt wurden.
- in der App selbst (Out-of-Band-Authentifizierung): Die zertifikatsbasierte Authentifizierung und Transaktionssignierung bietet ein Höchstmaß an Sicherheit, da die hier besonders geschützten privaten Schlüssel innerhalb der App zum Einsatz kommen. Darüber hinaus wird die Authentifizierung über einen zweiten, von den eigentlichen Nutzdaten unabhängigen Kanal, durchgeführt („Out-of-Band"). Für die Anmeldung per Smartphone – beispielsweise am Unternehmensnetzwerk – erhalten Anwender nach Eingabe ihres Benutzernamens die Push-Aufforderung zur Authentifizierung in der App und können sich anschließend durch die Eingabe einer PIN, per Fingerabdruck oder Gesichtserkennung eindeutig identifizieren.

Personal Mobile kann mit Nexus oder anderen Identity-Providern verwendet werden. App-Anbieter und Service-Provider können so Authentifizierung und Signatur auslagern und sich auf ihr Kerngeschäft konzentrieren. Kunden profitieren von einer einheitlichen Authentifizierungslösung an allen Webservices. Solche Lösungen können mittlerweile sogar als Service bezogen werden. Personal Mobile bietet darüber hinaus auch die Möglichkeit der Authentifizierung über OTP.

Zertifikats-Lifecycle-Management

Zertifikate müssen über ihren gesamten Lebenszyklus hinweg in einem zentralen System verwaltet werden, um sie nutzbar zu machen. Nexus Smart ID ist ein Identity- und Access-Management-System (IAM) und bietet standardisierte und anpassbare Prozesse für die Ausstellung und Verteilung digitaler Zertifikate, die Beantragung und Genehmigung von Berechtigungen, die Überwachung und Erneuerung der Zertifikatsgültigkeit sowie die Sperrung und Reaktivierung von Zertifikaten.

Mit diesen Workflows lassen sich Szenarien wie „neues Mobiltelefon", „vorübergehende Abwesenheit", „temporärer Zugang zum Serverraum", „aktualisierte Zuständigkeiten", „Erneuerung von Zertifikaten" oder „Beendigung des Arbeitsverhältnisses" komfortabel verwalten.

Fazit

Mit einer PKI-App bringen Unternehmen PKI-Technologie und PKI-basierte Identitäten auf das Smartphone und erhöhen so die Sicherheit maßgeblich. Damit lassen sich Funktionen wie E-Mail- und Dokumente-Verschlüsselung sowie digitale Signatur auch auf dem Smartphone nutzen. Außerdem wird das Smartphone zum ultrasicheren „Authenticator". Die App Nexus Personal Mobile stellt somit Zertifikate für den universellen Einsatz auf mobilen Geräten zur Verfügung. ■

Messestand: Halle 10.0, Stand 10.0-420 (IAM-Area)

Hintergrund: Was sind digitale Zertifikate und warum sind sie so sicher?

Das Herzstück einer Public-Key-Infrastructure ist die Certificate-Authority (CA), die als vertrauenswürdige Instanz digitale Zertifikate ausstellt. Die PKI sorgt für die sichere Verteilung der Zertifikate und bietet die Infrastruktur, um deren Echtheit zu prüfen.

Ein digitales Zertifikat ist eine Datei, die eine Reihe von Informationen enthält, wie beispielsweise Informationen über den Zertifikatsinhaber, eine Seriennummer und ein Ablaufdatum. Sie enthält auch die digitale Signatur der ausstellenden CA, sowie den öffentlichen Schlüssel des Zertifikatsinhabers.

In der Kryptografie ist ein Schlüssel eine Information, die für einen kryptografischen Algorithmus verwendet wird. PKI basiert auf einem asymmetrischen Verschlüsselungsverfahren: Jeweils ein öffentlicher und ein privater Schlüssel werden paarweise erzeugt und sind mathematisch verknüpft.

Der öffentliche Schlüssel ist für jedermann zugänglich und der private Schlüssel steht nur dem Schlüsselinhaber zur Verfügung. Wenn ein öffentlicher Schlüssel zum Verschlüsseln von Daten verwendet wird, ist die einzige Möglichkeit, die Daten zu entschlüsseln, die Verwendung des entsprechenden privaten Schlüssels. Wenn ein privater Schlüssel zum Signieren einer Nachricht verwendet wird, wird der entsprechende öffentliche Schlüssel zur Überprüfung der Signatur verwendet. Die Verwendung von zwei verschiedenen Schlüsseln gibt der asymmetrischen Kryptografie ihren Namen.

Eine PKI stellt sicher, dass private Schlüssel nur von den Eigentümern verwendet werden können, während die öffentlichen Schlüssel von der CA für alle Teilnehmer zugänglich gemacht werden.

Neues Produkt-Portfolio:

ESET bietet Enterprise-Netzwerken mehr Schutz dank Hybrid-Security

Das europäische Sicherheitsunternehmen ESET stellt auf der diesjährigen it-sa sein erweitertes und aktualisiertes Produktportfolio für Business-Anwender vor. Die weiterentwickelte Hybrid-Security – also die Verknüpfung von proaktiver Sicherheitstechnologie mit „Künstlicher Intelligenz" und „Machine Learning" – verspricht ein hohes Maß an Sicherheit speziell auch für Enterprise-Netzwerke.

Von Michael Klatte, ESET

Der größte Produktlaunch der Firmengeschichte umfasst insgesamt acht Lösungen, die Unternehmen jeglicher Größe noch mehr Sicherheit und vereinfachte Administration versprechen. Sie berücksichtigen auch die Bedürfnisse von Großrechenanlagen, wie sie in Regierungsstellen, im Militär, in Banken und in Konzernen zu finden sind. Diese stehen schon lange im Visier von professionellen Hackern und konnten sich bislang gut behaupten. Doch es mehren sich die erfolgreichen Angriffe. So wurde zu Beginn des Jahres bekannt, dass die Hacker-Gruppe Turla im Laufe der letzten zehn Jahre immer wieder groß angelegte Cyberangriffe gestartet hat und so neben dem Auswärtigen Amt auch weitere Behörden in EU-Staaten ausspionieren konnte.

Für Sicherheitsexperten war diese Entwicklung abzusehen. Aus der zunehmenden Professionalisierung von Cyberkriminellen entsteht logischerweise ein höheres Gefahrenpotenzial mit digitalen Waffen, die auch Enterprise-Netzwerken Kopfzerbrechen bereiten. Insbesondere der Einsatz von „Künstlicher Intelligenz" aufseiten der Hacker hat die Lage extrem verschärft.

Vor diesem Hintergrund hat ESET die seit Jahren bewährte Hybrid-Security mit Hochdruck weiterentwickelt. Der intelligente Mix aus praxiserprobten Methoden zur Malware-Erkennung sowie weiterer, proaktiver Netzwerktechnologie auf der einen Seite und „Künstlicher Intelligenz" (KI) plus „Maschinellem Lernen" (ML) auf der anderen stellt eine sinnvolle Verteidigung gegenüber allen möglichen Szenarien künftiger Cyberkriminalität dar.

Zwiebelschalenprinzip

Alle ESET-Sicherheitslösungen besitzen eine Reihe von unterschiedlichen Sicherheitsmechanismen. Diese sogenannten Security-Layer arbeiten anhand des bekannten Zwiebelschalenprinzips. Die Überprüfung des Datenstroms sowie die verhaltensbasierte Erkennung bilden die ersten Schichten. Gleichzeitig überprüft die ESET-Technologie an unterschiedlichen Punkten die Reinheit des Systems. Dazu kommen zum Beispiel Ransomware Shield, Exploit Blocker, Botnet-Erkennung oder die erweiterte Speicherprüfung („RAM-Schutz") zum Einsatz. Diese bewahren auch dann den Endpoint, wenn andere Erkennungsroutinen keinen Alarm geschlagen haben sollten. Bestes Beispiel hierfür ist das Feature „Schutz vor Netzwerkangriffen". Mit diesem Abwehrmechanismus konnte ESET die Ransomware WannaCry bereits stoppen, bevor sie überhaupt als solche bekannt wurde.

Das zweite Standbein der hybriden Sicherheitsstruktur ist die Kombination aus „Künstlicher Intelligenz" und „Machine Learning". Bereits seit 1995 setzt ESET auf KI und ML in seinen Produkten – also schon lange, bevor das Thema zum Hype wurde. Beide sind von unschätzbarem Wert für die Wahrung der Cybersicherheit, insbesondere beim Erkennen von Malware. Als Schutzlösung funktioniert beispielsweise „Machine Learning" so: Es basiert auf großen Datenmengen und Erfahrungen aus der Vergangenheit, bestehend sowohl aus als gutartig gekennzeichneten als auch bösartigen Materialsammlungen. Das ist die Grundlage, auf der ML zwischen „gut" und „schlecht" unterscheidet. So kann es potenzielle Bedrohungen für Benutzer schnell analysieren, identifizieren und Malware abwehren.

Das erweiterte Produktportfolio bietet mehr als die reine Erkennung/Abwehr von Bedrohungen und Verwaltung von Endpoint-Security-Lösungen. Vielmehr erhalten Anwender den übergeordneten Einblick in das „große Ganze": ein umfängliches IT-Security-Management, das auch

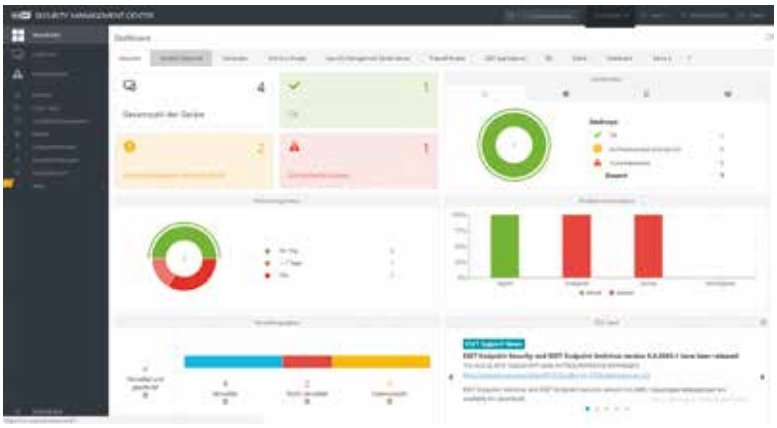
die Vorhersage und transparente Auswertung von Bedrohungen sowie umfangreiche Reaktionsmöglichkeiten und Vorfallsanalysen beinhaltet. Das Lösungsangebot bietet alle (security-) technischen Voraussetzungen, um sowohl in kleineren Unternehmen als auch im Enterprise-Sektor eingesetzt zu werden.

NEU: ESET Security Management Center

Als Herzstück der neuen Produktreihe für Unternehmen bezeichnen die Entwickler das brandneue ESET Security Management Center. Dabei handelt es sich um den Nachfolger des bekannten ESET Remote Administrator. Mit der Umbenennung wird vor allem deutlich, dass es sich nicht mehr nur um ein Remoteverwaltungstool handelt, sondern um die erste Anlaufstelle zum Thema Sicherheit, Systemmanagement, Reporting und der Integration weiterer ESET-Dienste, die sich bereits in der Pipeline befinden.

Neu sind unter anderem Funktionalitäten wie eine Hardwareinventarisierung der installierten Komponenten, ein wesentlich verbessertes Troubleshooting mit Möglichkeiten zur Remotediagnose, Logauswertung und vielem mehr, einer überarbeiteten Webkonsole inklusive touch-fähigem, interaktivem Dashboard, einer nativen Unterstützung für VDI-Umgebungen, der Integration von ESET Dynamic Threat Defense hinsichtlich Sichtbarkeit, Reports und Konfiguration und insgesamt einer Erweiterung der gesammelten Benachrichtigungsmöglichkeiten und Reports über alle Plattformen hinweg.

Das ESET Security Management Center (ESMC) lässt sich dabei, wie bisher der ESET Remote Administrator, auf Windows- und Linux-Server-Systemen installieren und ist darüber hinaus als fertige, virtuelle Maschine verfügbar. Alle ESET-Business-Lösungen, die für Windows, macOS, Linux, Android und iOS verfügbar sind, lassen sich über das ESET Security Management Center installieren, konfigurieren und betreuen. Über das Regelwerk können neben Benachrichtigungen auch automatische Aktionen, etwa bei Bedrohungsfund, hinterlegt werden. Zusätzlich bietet das ESMC Schnittstellen zu Drittanbieter-Lösungen, wie SIEM-Tools, und kann Log-Informationen in den verbreiteten Formaten JSON und LEEF ausgeben.



Dashboard von ESET Security Management Center

NEU: ESET Dynamic Threat Defense

ESET Dynamic Threat Defense bietet eine tiefgehende Analyse von Samples. Diese können über das ESET Security Management Center oder direkt aus ESET Mail Security und den Endpoint-Lösungen eingereicht werden. Zur Analyse wird das eigenentwickelte „Sandbox-System" in ESETs Rechenzentren verwendet – ein Clouddienst also. Es gibt Aufschluss darüber, welche Folgen das Ausführen einer Datei oder eines Programms hat. Aus diesen Informationen wird ein Score gebildet, der zwischen den vier Stadien Clean, Suspicious, Highly Suspicious und Malware unterscheidet. Vor allem Zero-Day-Malware und Ransomware können somit effektiver abgewehrt werden.

Neben der Erweiterung des Angebots wurde bei den Endpoint-, Mail- und Security-Lösungen technologisch aufgerüstet. Zudem wurde eine Harmonisierung der unterschiedlichen Security-Layer bei allen Lösungen vorgenommen. Angesichts der vielfältigen Bedrohungen im Cyberspace ist der Einsatz von vielschichtigen Sicherheitsmethoden unabdingbar. Die aktualisierten Versionen zeichnen sich besonders aus durch eine native 64-Bit-Architektur, UEFI-Scanner zum Schutz vor Bedrohungen auf Chipsatzebene, einer weiter verbesserten Botnet-Erkennung, voll integriertem Ransomware-Schutz, Schutz vor Netzwerkangriffen, der vollen Unterstützung von Microsoft-Office-365-Umgebungen, zeitbasierten Einstellungen für Web- und Medienkontrolle sowie einem verbesserten Phishing-Schutz. ■

Messestand: Halle 9, Stand 9-326.

Die neuen und aktualisierten Produkte im Überblick

- ESET Endpoint Antivirus für Windows v7
- ESET Endpoint Security für Windows v7
- ESET Security für Microsoft SharePoint Server v7
- ESET File Security für Microsoft Windows Server v7
- ESET Mail Security für Microsoft Exchange Server v7
- ESET Mail Security für IBM Domino v7
- ESET Security Management Center v7
- NEU: ESET Dynamic Threat Defense

Security Management für vernetzte Automatisierungs-anlagen

geprüfte Sicherheit

Der Mittelstand und die kritischen Infrastrukturen benötigen Security mit einfacher Bedienbarkeit

- Die automatische und passive Erkennung der Assets (Teilnehmer) im Netzwerk
- ITSiG Branchenspezifische Sicherheitsstandard (B3S) für Wasser / Abwasser
- Standard-basiertes Risikomanagement (vgl. ISO27005) für das Security Management
- Die grafische Darstellung des gesamten Netzwerkes sowie Auswertungen zu jedem Teilnehmer
- Alarmierung und Integration in den Leitstand
  (z.B. Potentialfreier Kontakt, SNMP) oder Alarmierungssystem (z.B. AIP)

Besuchen Sie uns auch auf der

IT-SA 2018 in Nürnberg
Halle 9 Stand 506 9. – 11. Oktober 2018

Wir informieren Sie:
www.videc.de

VIDEC.

Neue Web-Application-Firewalls

Sicherheit auf allen Ebenen

Die für Webapplikationen eingesetzten Protokolle HTTP und HTTPS lassen sich nur mit speziellen Web-Application-Firewalls schützen. Bisher arbeiteten diese allerdings unpräzise und waren schwer zu bedienen. Neue Konfigurationsansätze erleichtern die Handhabung und erhöhen die Sicherheit.

Von Walter Schumann, 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, wurden nicht für die heute üblichen komplexen Anwendungen konzipiert. Deshalb lassen sich Schwachstellen kaum vermeiden und der Anteil an Datenlecks durch Angriffe auf Webanwendungen steigt 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-Datenschutzgrundverordnung (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.

Verdächtige Inhalte stoppen

Wer Angriffe auf Webanwendungen abwehren will, braucht eine spezielle Web-Application-Firewall. Denn nur solche Firewalls können Daten überprüfen, die im HTTP- beziehungsweise HTTPS-Protokoll auf der Anwendungsebene verkehren. Eine Web-Application-Firewall wird dazu als Reverse Proxy installiert. Sie kann deshalb den gesamten Datenaustausch zwischen Clients und Webserver analysieren und verdächtige Inhalte stoppen. 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. Die Anzahl solcher falschen Alarmmeldungen kann schnell bei mehreren Hundert am Tag liegen. Bedrohungen werden erkannt, wo gar keine sind. Damit verursacht die Firewall häufig eher Mehrarbeit, als dass sie einen entscheidenden Vorteil bringt.

Um das zu umgehen, wird sie nicht selten einfach 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

Neue Web-Application-Firewalls erhöhen die Sicherheit und sind gleichzeitig einfacher zu bedienen.

jedoch erheblich reduzieren, ohne dass Mitarbeiter komplexe Einstellungen vornehmen müssen. Die wichtigsten Methoden sind:

Verhaltensbasierte Technologie und Workflow-Konzept

Statt Datensätze nur aufzulisten, werden Internetbedrohungen anhand ihrer Aktivitäten und spezifischen Verhaltensweisen identifiziert. Durch diese automatische Präzisierung der Daten sind aufwendige Voreinstellungen durch den IT-Administrator nicht mehr nötig. Auch Mitarbeiter ohne Spezialwissen können die Web-Application-Firewall installieren. 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 zum Beispiel 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.

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 die sogenannte Sandboxing-Technologie, mit der sich zu schützende Bereiche komplett isolieren lassen.

Einfache und sichere Authentifizierung

Auch die Authentifizierung spielt für die Sicherheit einer Webanwendung eine entscheidende Rolle. Nichtautorisierten 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 zu erschweren.

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

Fazit

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. ■

Messestand: Halle 10.0, Stand 10.0-112

Neue Sicherheitslösungen auf der it-sa

Rohde & Schwarz Cybersecurity stellt auf der it-sa die neuen Generationen seiner Sicherheitslösungen R&S Web Application Firewall und R&S Trusted Gate vor. Außerdem präsentiert das Unternehmen den völlig neu entwickelten R&S Trusted Communicator, eine Kommunikations- und Kollaborationsplattform, die einen hochsicheren Messenger samt verschlüsselter Telefonanrufe in einem bietet.

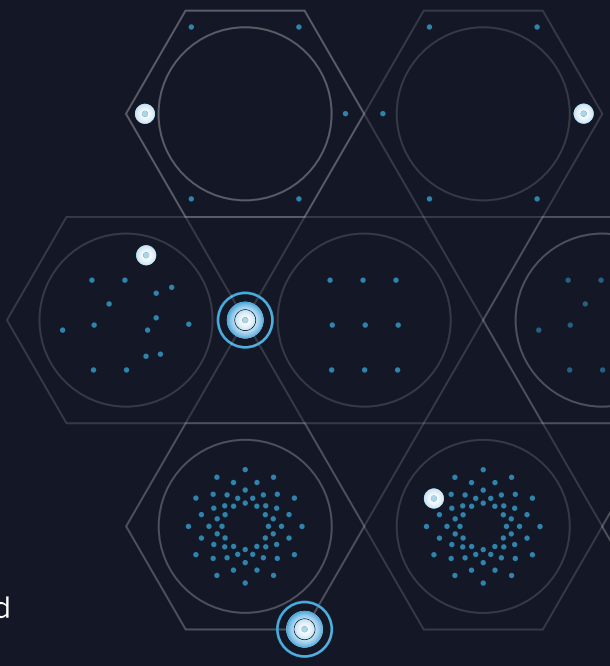
Bei der neuen Generation seiner R&S Web Application Firewall lassen sich mit neuen Konfigurationsmethoden bspw. False-Positives erheblich reduzieren, ohne dass Mitarbeiter komplexe Einstellungen treffen müssen. Die umfassende Lösung beinhaltet nicht nur Standardfunktionen herkömmlicher Lösungen, sondern erweitert sie um das Vulnerability Scanning, Virtual Patching und Web-Access-Management für webbasierte Anwendungen wie z. B. von SAP, E-Mail-Anwendungen wie Outlook Web Access oder CRM-Anwendungen.

Die Sicherheitslösung R&S Trusted Gate schützt Daten in der Cloud. R&S Trusted Gate ist eine neue Technologie, die Verschlüsselung, Virtualisierung und Fragmentierung der Daten in einer ganzheitlichen Lösung verbindet. Außerdem unterstützt R&S Trusted Gate bei der Umsetzung der Vorgaben der Datenschutzgrundverordnung (EU-DSGVO) beim Umgang mit personenbezogenen Daten und lässt sich nahtlos in bereits bestehende Cloud-Umgebungen, Microsoft SharePoint oder Office 365 einbinden.

Auf der it-sa zeigt Rohde & Schwarz Cybersecurity erstmals seine App R&S Trusted Communicator für iOS und Android. Über diesen lassen sich sowohl Telefonate als auch Textnachrichten hochsicher übertragen. Der neuen Lösung liegt das Verschlüsselungsverfahren „AES-256“ zugrunde. Mit diesem werden alle versendeten Informationen sowie alle Telefonate lokal auf dem Smartphone verschlüsselt und erst auf dem Empfänger-Smartphone wieder entschlüsselt. Durch die durchgängige Ende-zu-Ende-Verschlüsselung haben Man-in-the-Middle-Angriffe keine Chance. Auch die lokal gespeicherten Kontakte bleiben für Dritte unter Verschluss.

Ihre Daten.

Unser Auftrag.



Sind Ihre Daten sicher?

Erschreckenderweise scheitern die meisten Unternehmen dabei, ihre wertvollsten Daten zu schützen - und können nicht sagen, ob sie angefasst oder gestohlen wurden. Bei Varonis steht der Schutz Ihrer Datei- und E-Mail-Systeme vor Cyberattacken und Insiderbedrohungen im Vordergrund. Wir verfolgen seit unserer Gründung einen anderen Ansatz als die meisten IT-Sicherheits-Anbeiter, indem wir die Unternehmensdaten ins Zentrum der Sicherheitsstrategie stellen.

Mehr erfahren: www.varonis.com/it-sa

Nutzen Sie diesen Gutschein für eine leckeren Kaffee auf der it-sa bei uns am Stand 9-435!

Weitere Informationen finden Sie unter: varon.is/it-sakaffee

VARONIS

Die Annäherung von Grundschutz und ISO 27001

Mit seinen neuen 200-x-Standards hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiter der ISO 2700x-Normenreihe angenähert. So haben zum Beispiel die Anforderungen des IT-Grundschutz-Kompendiums jetzt einen ähnlichen Charakter wie die Controls der ISO-Standards. Die HiScout GmbH hat daher im Zuge der Modernisierung auch seine beiden Module „HiScout Grundschutz nach BSI IT-Grundschutz" und „HiScout ISM nach ISO 27001" angenähert und stärker miteinander verbunden.

Von Thomas Eimecke, HiScout GmbH

Für viele Unternehmen und Behörden ist die Einführung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) eine der größten Herausforderungen, denen sie sich bislang stellen mussten. Das Ziel, ein integriertes GRC-Managementsystem zu etablieren, scheint daher häufig unerreichbar.

Oftmals sind allein schon die organisatorischen Hürden unüberwindbar und eine Zusammenarbeit der jeweiligen Fachbereiche ist nicht immer selbstverständlich. Spätestens aber bei der Frage der Tool-Unterstützung wird es kompliziert. Denn für die einzelnen Bereiche des GRC-Umfelds gibt es viele hoch spezialisierte und gut geeignete Tools. Da diese aber eben nur einen Teilbereich bedienen, sind in den meisten Unternehmen mehrere parallel im Einsatz. Diese müssen dann, sofern überhaupt möglich, über Schnittstellen miteinander verbunden werden. Zusätzlich gibt es dann meist noch verschiedene Systeme für die Erfassung und Pflege der Stammdaten (z. B. Assets).

Diese komplexen Strukturen können mit einem geeigneten, integrativen GRC-Tool vermieden beziehungsweise abgelöst werden. Hierfür sollten im Tool die einzelnen Anwendungsgebiete zwar separat darstellbar sein, aber eben auf eine gemeinsame Datenbasis (Stammdaten) zugreifen.

Die HiScout GmbH verfolgt mit ihrer Plattform genau diesen Ansatz. Alle Module basieren auf einem flexiblen objektorientierten Datenmodell mit einem individuell konfigurierbaren Berechtigungssystem. Die einzelnen Module sind dabei speziell für ihr Anwendungsgebiet gestaltet, aber immer über die gemeinsame Datenbasis miteinander verbunden.

Geschäftsprozesse – Ein weiterer Schritt

Neben der gemeinsamen Datenbasis werden die Module der HiScout-Plattform aber auch über die Zusammenführung gemeinsamer Arbeitsschritte miteinander verbunden. So sind die Prozessschritte „Strukturanalyse" und „Schutzbedarfsfeststellung" des „HiScout Grundschutz" und „HiScout ISM" seit jeher gleich gestaltet und nutzen das gleiche Vorgehen.

So waren im HiScout-Standard auch schon für die alte Grundschutz-Vorgehensweise die Geschäftsprozesse die Basis der Schutzbedarfsaufnahme. Über die hohe Flexibilität und Anpassbarkeit der Plattform war es immer möglich, diese Erfassung, wie in den 100-x-Standards beschrieben, auf die Anwendungen umzustellen, aber eine Erfassung auf Ebene der Geschäftsprozesse war auch nie ein Hinderungsgrund für die Zertifizierung nach den 100-x-Standards.

Mit seinen neuen 200-x-Standards hat das BSI nun offiziell die Geschäftsprozesse in den Fokus der Bewertung gestellt. Das ist ein sehr guter und wichtiger Schritt in der Annäherung an die ISO 2700x-Normenreihe. Denn durch die Schutzbedarfsaufnahme auf Ebene der Geschäftsprozesse werden die größten Wissensträger der im Unternehmen verarbeiteten Informationen in den Informationssicherheitsprozess einbezogen. Damit kann eine größere Detailtiefe und Qualität der erfassten Daten erreicht, aber gleichzeitig auch mehr Awareness für die Informationssicherheit bei den Fachanwendern geschaffen werden. Auf diese Weise kann insgesamt ein höherer Reifegrad des ISMS erreicht werden.

Grundschutzanforderungen und ISO-Controls

Die neuen 200-x-Standards ergeben aber noch weitere Annäherungspunkte an die ISO 2700x-Normenreihe. So haben die An-

forderungen des IT-Grundschutz-Kompendiums im Vergleich zu den Grundschutzmaßnahmen der alten Grundschutzkataloge jetzt einen höheren Abstraktionsgrad und damit einen vergleichbaren Charakter zu den Controls der ISO 27001 erlangt.

In der HiScout-Plattform werden daher die Grundschutzanforderungen und die anwendbaren ISO-Controls gleich behandelt. Diese können so beispielsweise auch im IT-Grundschutzcheck herangezogen werden. Gleichzeitig können aber auch die Grundschutzanforderungen als Prüfpunkte im Self-Assessment des „HiScout ISM" genutzt werden. Damit wird den Anwendern beider Vorgehensweisen eine breitere und umfassendere Basis an Prüfkriterien zur Verfügung gestellt.

Risikoklassifikation über den matrixbasierten Ansatz

Einen weiteren wichtigen Schritt hat das BSI mit seinem 200-3-Standard gemacht. Über die Einführung des matrixbasierten Risikoansatzes kommt endlich eine belastbare Klassifizierungsmöglichkeit in das Risikomanagement der Grundschutz-Vorgehensweise. Eine solche Klassifizierung anhand von Eintrittswahrscheinlichkeit und Schadenshöhe ist im Bereich der ISO 2700x-Normenreihe bereits seit einigen Jahren ein etablierter Standard. Über die Einstufung der Risiken anhand der Matrix wird eine größere Detailtiefe der Bewertung erreicht. Die einzelnen Risiken können dadurch besser miteinander verglichen und priorisiert werden.

Des Weiteren lassen sich durch diese Annäherung die Ergebnisse der Grundschutz-Risikoanalyse auch besser in ein OpRisk-Management integrieren. Denn über die Klassifizierung werden sie vergleichbarer mit den Ergebnissen der Risikoanalysen aus anderen Managementsystemen.

In der HiScout-Plattform ist dieser matrixbasierte Ansatz übergreifend eingebunden. Das bedeutet, dass eine für das Unternehmen festgelegte Bewertungslogik die Basis der Risikoeinstufung in den unterschiedlichen Managementdisziplinen bildet. Die Matrix ist über die Oberfläche frei konfigurierbar und bildet die Grundlage für die im Hintergrund laufende automatische Einstufung in eine Risikoklasse. Der für die jeweilige Risikoanalyse Verantwortliche muss also nur die Eintrittswahrscheinlichkeit und Schadenshöhe bewerten und es ergibt sich automatisch die entsprechende Risikoklasse.

Bausteine als Risikoprofile

Ein Vorteil, den die Grundschutz-Vorgehensweise seit jeher bietet, ist die Vernetzung von Bausteinen und Gefährdungen. Schon für die alte Grundschutz-Vorgehensweise war im „HiScout Grundschutz" eine automatisierte Übernahme der aus der Modellierung mit Bausteinen resultierenden Gefährdungen möglich. Auch für das neue Vorgehen ist diese Übernahme weiterhin möglich und schafft somit eine wesentliche Erleichterung für den jeweiligen Risikomanager.

Diese Erleichterung kann auch im „HiScout ISM" genutzt werden. Hierbei dienen die Bausteine als eine Art Risikoprofil für die Assets. Bei der Erstellung einer Risikoanalyse kann so über die zugeordneten Profile ein Vorschlag für möglicherweise relevante Gefährdungen direkt in die Risikoanalyse übernommen werden.

Die im Vorfeld durchzuführende Zuordnung zu den Profilen kann dabei, in Anlehnung an die Modellierung des Grundschutzes, auf Einzel-Asset-Ebene (z. B. Anwendung „Outlook") durchgeführt werden, aber ebenso auch auf der Basis von Asset-Typen (z. B. E-Mail-Anwendung) erfolgen. Die Zuordnung der Grundschutzbausteine zu einzelnen Asset-Typen bildet im „HiScout Grundschutz" auch die Grundlage für die automatisierte Modellierung und wird von HiScout mitgeliefert.

Die Nutzung der neuen Grundschutzbausteine als Risikoprofile bietet eine fachlich fundierte Basis und kann natürlich durch eigene Profile erweitert werden. Diese können dann wiederum im „HiScout Grundschutz" als benutzerdefinierte Bausteine genutzt werden.

Annäherung schafft Synergieeffekte

Insgesamt lässt sich feststellen, dass sich die Grundschutz-Vorgehensweise durch die Annährungen an die ISO 2700x-Normenreihe zu einem immer kompletter werdenden Standard entwickelt hat. Während in der alten Vorgehensweise noch die umfänglichen Kataloge und die darin enthaltenen Verknüpfungen der Hauptvorteil waren, verbindet die aktuelle Vorgehensweise nun die guten Ansätze der ISO 2700x-Normenreihe mit einem umfangreichen Kompendium. Des Weiteren ist festzustellen, dass sich die über diese Annäherungen entstehenden Synergieeffekte durch ein Tool mit einem integrativen Ansatz sehr gut nutzen lassen.

Messestand: Halle 10.0, Stand 10.0-310

DeviceLock und die Datenschutzgrundverordnung:

Fahrlässigen Umgang mit Unternehmensdaten vermeiden

Seit dem 25. Mai 2018 besteht ein erhöhter Schutzbedarf durch erweiterte gesetzliche Anforderungen zum Datenschutz aus der EU-Datenschutz-Grundverordnung (EU-DSGVO) und zusätzlich aus dem angepassten Bundesdatenschutzgesetz. Die EU-DSGVO gilt unmittelbar in der gesamten Europäischen Union (Art. 288 Abs. 2 AEUV) und schreibt im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien fort. Zur Gewährleistung dieser gesetzlichen Anforderungen empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Einsatz einer Data-Leakage-Prevention (DLP), um Datenbewegungen zu kontrollieren und den unerwünschten Datenabfluss zu verhindern.

Von Thomas Tuckow, DeviceLock Europe GmbH

DeviceLock erfüllt diese Bedingungen und schützt vor Datenabfluss durch unbeabsichtigte Fehler von Mitarbeitern und vor Personen mit böswilligen Absichten des Datendiebstahls. Somit sorgt DeviceLock für die strikte Durchsetzung unternehmenseigener Sicherheitsrichtlinien und sichert gleichzeitig die Einhaltung gesetzlicher Vorgaben. Einfaches Blockieren nur von USB-Schnittstellen durch Zusatzfunktionen anderer Sicherheitsprodukte reicht definitiv nicht.

Als professionelle DLP umfasst DeviceLock die notwendige Kontextkontrolle lokaler Schnittstellen wie u. a. Wechseldatenträger, verbundene Smartphones, die Zwischenablage auch in RDP/Terminal-Sessions.

DeviceLock bietet eine Kontextkontrolle der wichtigen Web- und Netzwerkkommunikation auf Protokollebene und unabhängig von den verwendeten Ports und Anwendungen. Zusätzlich sind ein Event-Logging sowie die Datenspiegelung für überwachte Datenkanäle und Alarmierung enthalten. Um aussagekräftige Reports zu erstellen und Datenströme oder Kommunikationsbeziehungen zu analysieren, stellt DeviceLock eine auf Log-Daten basierende grafische Auswertungsfunktion bereit.

Die Endpoint-DLP-Suite von DeviceLock kontrolliert Datenströme im Unternehmen

DeviceLock nutzt auf jedem geschützten Computer einen ressourcenschonenden Agenten. Zur Administration wird ein zentrales Gruppenrichtlinien-MMC-Snap-In verwendet, das auf jede Größe und jeden Typ von Unternehmensnetzwerken angepasst werden kann. Zentrale Konsolen können für die Verwaltung von Macs, Nicht-AD-LDAP-Umgebungen und/oder Windows-Arbeitsgruppen verwendet werden.

Ergänzend zum Kontext prüft und bewertet ein Content-Filter den Inhalt der Datenbewegungen. DeviceLock blockiert oder erlaubt den Datenfluss in Abhängigkeit davon, welcher Mitarbeiter was, über welches

Interface, Gerät oder Protokoll, mit welchem Ziel, mit welchem Inhalt und zu welchem Zeitpunkt bewegt. Neben Dateityperkennung auf binärer Ebene und der Auswertung von Dokumenteneigenschaften erkennt DeviceLock sensible Textinhalte auch mithilfe von Wortübereinstimmungen und Mustern regulärer Ausdrücke.

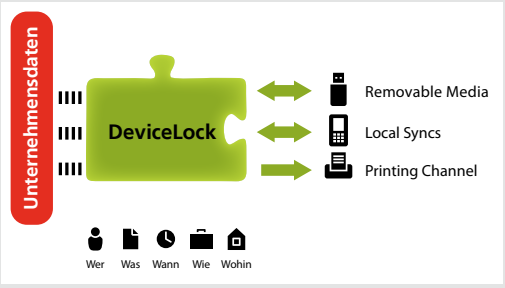
Zusätzlich extrahiert eine integrierte OCR-Engine präzise Textdaten aus Bildern und Grafikdateien. Ein Fingerprinting ergänzt die inhaltliche Erkennung durch digitale Fingerabdrücke, um vollständige Kopien sowie Teile von Dokumenten zu identifizieren. Zudem werden die von Boldon James Classifier an Dateien und Dokumenten zugewiesenen Klassifizierungen erkannt und zur inhaltlichen Filterung verwendet. Die vorgenannten Varianten lassen sich auch in Form boolescher Kombinationen miteinander verbinden. Durch Zulassen oder Blockieren der entsprechenden Datenbewegungen stellt DeviceLock sicher, dass nur die zuvor geprüften Daten mit für den Benutzer freigegebenen Informationen ihre erlaubten Ziele erreichen.

DeviceLock bietet ein komplettes DLP-Management und kann zentral definierte DLP-Richtlinien anwenden. Für die Konfiguration der Endpoint-Agenten verwenden DeviceLock Administratoren die Windows-Active-Directory-Gruppenrichtlinienobjekte oder alternativ in DeviceLock enthaltene Mechanismen. Eine DeviceLock-Konsole ist unmittelbar in die Microsoft-Management-Console der Active-Directory-Gruppenrichtlinien-Verwaltung integriert. Entsprechend einfach wird die Steuerung über die Gruppenrichtlinien-Verwaltungskonsole ermöglicht. Dadurch binden Administratoren die Konfiguration der Zugriffsrechte in ihre allgemeinen Systemmanagement-Aufgaben ein. Eine zusätzliche Web-Konsole ermöglicht die Steuerung der Komponenten über jeden Webbrowser. ■

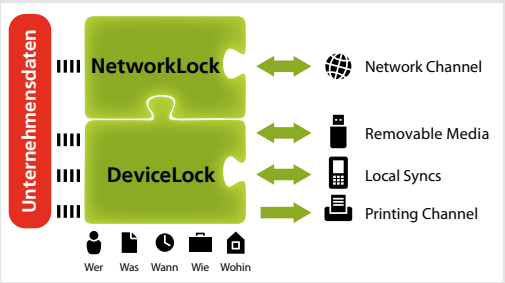
Messstand: Halle 9, Stand 9-209

Modulare Funktionsübersicht von DeviceLock

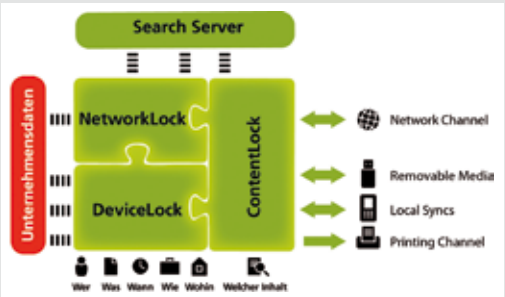
Kontextkontrolle lokaler Schnittstellen/Geräte
- Kontrolle lokaler Ports (Windows und macOS)
- Daten- und Gerätekontrolle in Terminalsitzungen
- Kontrolle der Zwischenablage
- Dateitypenfilterung (binär)
- Druckerkontrolle inkl. virtuelle Drucker (pdf)
- Smartphone-Synchronisationskontrolle
- Whitelist für USB und CD-/DVD-Medien
- Anti-Keylogger
- Verschlüsselungsintegration
- DL-Administratorrechte (Dienst + Server)
- AD-Integration (GP-MMC + Template)
- Zentrale Managementkonsole
- White- und Blacklisting für CAWR
- Live Monitoring
- Flexible Verteilungsstrategien des Service
- Online/Offline-Richtlinien
- Temporary Whitelist und Offline-Import der Settings



Kontextkontrolle der Web- und Netzwerkkommunikation
- Netzwerkprotokollkontrolle FTP, FTP über SSL, HTTP(S), MAPI (MS Exchange), IBM Notes, SMB, SMTP
- Kontrolle von Cloud-Diensten (File Sharing)
- Webmail-, Messenger- und Skype-Kontrolle
- Kontrolle sozialer Netzwerke
- Erzwingung einer sicheren Übertragung
- Whitelist für alle Kontrollmöglichkeiten
- Online/Offline-Richtlinien



Kontrolle aller Inhalte auf binärer Ebene
- Digitales Fingerprinting
- Inhaltskontrolle für Gerätezugriffe (100+ Dateiformate und 40+ Archive)
- Inhaltskontrolle für Webzugriffe (NetworkLock)
- Schlagwortkatalog (branchenspezifisch)
- Kontrollregeln mit RegExp definierbar (reguläre Ausdrücke und/oder Schlagwörter)
- vordefinierte Schablonen für RegExp
- Dokumentenfilterung anhand von Dateiattributen
- Online/Offline-Richtlinien
- Volltextsuche inkl. Wortstammfilterung und OCR



Informationsmanagement
- Echtzeit-Alarme, zentrale Protokollierung und Alarme für alle virtuellen DLP-Szenarien
- Richtlinienbasierte Auditierung der Zugriffe (Geräte, Protokolle und Inhalte)
- Schattenkopien von Schreibzugriffen in Abhängigkeit von Richtlinien (Inhalt, Dateityp etc.)
- Grafisches Reporting
- Zentrale Log-Erfassung mit /Priorisierung, SYSLOG
- Alarmierungsmethoden mit SMTP, SNMP, SYSLOG
- Zentrale Datenbank für Auditing/Shadowing
- Indexierung und Volltextsuche in zentralen Auditing/Shadowing-Datenbanken (DLSS)

retarus

ENTSPANNEN

Sie Ihre E-Mail Kommunikation

retarus.de/it-sa

Intelligentes Security-Sourcing

Mehr Sicherheit durch die richtige Strategie

Die Zeiten, in denen sich Unternehmen selbst um ihre gesamte IT-Sicherheit kümmern konnten, sind vorbei. Denn heutzutage funktioniert zum einen kein Business mehr ohne IT und zum anderen hat sich die Bedrohungslage deutlich verschärft. Dadurch sind die Aufgaben der IT-Security so komplex geworden, dass sie intern kaum mehr zu bewältigen sind. Weil die Branche zusätzlich mit einem massiven Fachkräftemangel zu kämpfen hat, kommen Unternehmen nicht umhin, Teile ihrer Security auszulagern, um ihr Geschäft ausreichend zu schützen. Welcher Weg aber führt zur optimalen Sourcing-Strategie? Welche Services können ausgelagert, welche sollten besser intern betrieben werden?

Von Lutz Feldgen, Computacenter

Unternehmen stehen unter Zugzwang, ihre Cyberabwehr gut aufzustellen und für Prävention, Detektion und Reaktion die richtigen Lösungen und den passenden Service-Provider zu finden. Hinzu kommt die Frage: Alles auslagern oder nur bestimmte Teilbereiche? So wollen Finanzinstitute in der Regel die Kontrolle intern behalten. Deshalb kann ein Service-Provider zwar den technischen Betrieb von Cyberabwehr-Systemen übernehmen, der fachliche Input und die Analyse der Ergebnisse bleiben jedoch im Unternehmen.

Im Fokus aller Überlegungen zur Sourcing-Strategie für die Cyberabwehr sollte immer das perfekte Zusammenspiel zwischen Menschen, Tools und Prozessen stehen. Wer übernimmt welche Aufgaben, was sollte selbst erbracht, was kann ausgelagert werden? Wie lässt sich eine reibungslose Zusammenarbeit sicherstellen? Und: wohin auslagern? Denn oft lässt sich die Sicherheit nicht aus einem Haupt-Service ausgrenzen – um die Endpoint-Security kümmert sich der Workplace-Provider, um die Firewalls der Netzwerk-Provider. Gleichzeitig muss der fachliche Nutzen aus den dazugehörigen präventiven Technologien wie Endpoint-AV, NIPS, Firewall & Co. für Detektion und Prävention zentralisiert bezogen werden – aus dem Cyber-Defence-Center. Ein guter Service-Provider muss das Verständnis mitbringen, Security-Technologie und deren Abhängigkeiten zueinander einzuordnen und die bestehenden präventiven Security-Lösungen fachlich zu orchestrieren – auch wenn er sie nicht zwingend selbst betreibt.

Unternehmen sind daher gut beraten, auf starke Partner zu setzen, die sich in allen Gebieten der Unternehmens-IT auskennen und ein durchdachtes eingebettetes Sicherheitskonzept anbieten. Als Secure IT-Provider bietet Computacenter im Bereich Managed Services genau das und prüft diese Punkte darüber hinaus im Rahmen seiner Security-Strategieberatung. Damit kann ein intelligentes Sourcing geplant werden, um für mehr Sicherheit zu sorgen und von Synergien zu profitieren. Wichtig dabei ist, die IT-Sicherheit als Ganzes zu betrachten, um optimale Lösungsmodelle zu entwickeln. Doch welche Sicherheitsservices ein Unternehmen auch auslagert, die Entscheidung über die Maßnahmen und Risiken sowie die Verantwortung über die Datensicherheit verbleiben immer beim Unternehmen.

Effizienter dank Orchestrierung und Automation

Wer intelligentes Sourcing betreiben will, sollte einen weiteren Aspekt berücksichtigen: Auch die IT-Sicherheit entwickelt sich immer mehr in Richtung Automatisierung und Orchestrierung. Denn der durchschnittliche Zeitraum, bis ein Angriff entdeckt wird, liegt noch immer zwischen 9 und 22 Monaten. Auch wenn sich die Zeitspanne stetig verkürzt, vergeht zwischen dem Entdecken eines Angriffs und der Analyse, um welchen Vorfall es sich handelt, sowie der Reaktion darauf, nach wie vor deutlich zu viel Zeit. Um die Reaktionszeit zu verkürzen, unterstützt beispielsweise „Security Orchestration and Automated Response“ (SOAR). Ist eine SOAR-Plattform mit weiteren Quellen etwa für ein automatisiertes, komplexes Event Enrichment oder mit Maßnahmen

Abb.1: Ebenen-Modell für Managed Security-Services

der Endpoint- oder Network-Security verknüpft, ermöglicht sie eine automatisierte Analyse und Reaktion. Eine vollständige Automation ist jedoch nicht erstrebenswert, da neben der technischen Integration auch Organisation und Prozesse flexibel bleiben müssen. Denn bei neuartigen Bedrohungen oder möglichen Fehlalarmen sind die automatisiert aufbereiteten Sicherheitsvorfälle manuell nachzuprüfen. Nach der Überprüfung kann das System auch auf diese Vorfälle automatisch reagieren. Ist SOAR strategisch gesetzt, muss der Sourcing-Partner dabei unterstützen und sich entsprechend vorbereiten. Und das gilt für jede relevante Sicherheitstechnologie.

Managed Security-Services

Bei der Sourcing-Frage unterstützt Computacenter seine Kunden im Rahmen von Security-Strategieberatung, in der auch das intelligente Sourcing ein wichtiger Bestandteil ist. So kann der Secure IT-Provider sowohl dabei unterstützen, den richtigen Service-Provider für die Anforderungen des Unternehmens zu ermitteln, als auch selbst Managed Security-Services erbringen. Um erfolgreiche Cyberangriffe einzudämmen und deren Folgen zu beseitigen, setzt Computacenter auf eine Kombination der drei Kerndienstleistungen: Security Incident and Event Management (SIEM), Vulnerability Management und Information Security Officers.

Die ersten beiden Services konzentrieren sich auf die proaktive Identifizierung von Risiken, Vorfällen, Schwachstellen und Angriffen. Der Information Security Officer fokussiert sich auf die Kontextualisierung der identifizierten Probleme. Die Kombination aller drei Services ermöglicht es, einen Angriff schnell zu bewältigen. Dabei bieten SIEM- und Vulnerability-Services die notwendige technische Expertise und Einblicke. Der Sicherheitsmanager bildet die Schnittstelle zum Kunden und hat den erforderlichen Überblick über die individuellen Gegebenheiten des Unternehmens, um die optimale Reaktion zur Eindämmung und Beseitigung aller identifizierten Bedrohungen durchzuführen.

Um die unterschiedlichen Bedürfnisse der Unternehmen an IT-Sicherheit bestmöglich zu erfüllen, hat Computacenter seine Cyber-Defence-Services an einem Layer-Modell ausgerichtet. Damit können Unternehmen schnell erkennen, wo sie stehen und wie sie aufgestellt sind. Auf dieser Basis entwickelt Computacenter anschließend das passende Betriebsmodell (vgl. Abb. 1).

Die unterste, beziehungsweise erste Ebene umfasst den nativen Betrieb von präventiv wirkenden Sicherheitskomponenten, der sich in der Art und Weise kaum vom Betrieb der Netzwerk- oder Client/Server-Komponenten unterscheidet. Hier geht es vor allem um die Verfügbarkeit der Komponenten, das fehlerfreie Arbeiten und die Aktualität der Software.

Auf der zweiten Ebene kommen Security-Komponenten zum Einsatz, die zur Detektion von Angriffen dienen. Eine erste Basisanalyse findet hier mit dem Ziel statt, Angriffe zu erkennen.

Auf der dritten Ebene wird die Basisanalyse durch eine tiefgehende Analyse von Sicherheitsvorfällen erweitert. Hier ist sehr individuelles Know-how Voraussetzung, um die geeignete Reaktion auszulösen.

Auf der vierten Ebene ermöglichen detaillierte forensische Untersuchungen die notwendige und richtige Reaktion auf Vorfälle.

Verantwortung bleibt immer im Unternehmen

Beim Auslagern verschiedener Services sollten Unternehmen stets berücksichtigen, wie sie von den größtmöglichen Synergien profitieren können. So sorgt die Auslagerung von Cyber-Defence-Services zusätzlich zu weiteren Services in eine Hand beispielsweise für einen kurzen Informationsfluss. Nachteilig hierbei ist ein erhöhter Aufwand bei der Governance durch den Kunden, da die Funktionstrennung nicht mehr gegeben ist. Eine Alternative ist es, einem Service-Provider nur die Cyber-Defence zu übertragen. Hier ist weniger Governance gefragt, allerdings sind mehr Prozesshürden zwischen den Service-Providern zu überwinden.

Egal welchen Weg ein Unternehmen geht: Wichtig ist immer, dass eine durchdachte Strategie hinter allen Sourcing-Entscheidungen steht und Unternehmen sich bewusst sind, dass die Entscheidung über Maßnahmen und Risiken sowie die Verantwortung für die Datensicherheit immer beim Unternehmen verbleibt. ■

Messestand: Halle 10.0, Stand 10.0-216

it sa 2018

Die IT-Security Messe und Kongress

HOME OF IT SECURITY

* **Congress@it-sa**
Start: 8.10.2018 – einen Tag vor Messebeginn

Aktuelles IT-Security-Wissen wartet auf Sie!

Nürnberg, Germany
8.-11. Oktober 2018

it-sa.de

NÜRNBERG MESSE

Zertifizierungen von Rechenzentren

Vergleichbarkeit herstellen

Wer bei Zertifikaten genauer hinschaut, kann daraus viele Informationen für die Evaluierung von Rechenzentrumsdienstleistern gewinnen. Intensive Gespräche und Vor-Ort-Termine bleiben selbstverständlich Pflicht, eine vorausgehende Analyse von Zertifikaten aber spart Zeit und Kosten.

Von Marcel Kempe, noris network

Wer einen Rechenzentrumsdienstleister sucht, kann über die Zertifizierungen der Kandidaten eine erste Vorauswahl auf Basis von gewünschten Mindeststandards treffen. Basis sind dabei die Anforderungen, die das eigene Geschäft vorgibt. Sprich: Ist er ein Zulieferer, dessen Kunden oder Märkte bestimmte Standards fordern? Müssen beispielsweise Kreditkartendaten verarbeitet werden, dann sollten nur RZ-Betreiber in die engere Wahl kommen, die für den Bereich Housing und Colocation bereits PCI-DSS-zertifiziert ist. Das Zertifikat zeigt, dass der auf die Rechenzentrumsinfrastruktur bezogene Teil der für eine PCI-DSS-Zertifizierung verlangten rechtlichen Anforderungen bereits vollumfänglich abgedeckt sind.

Neben branchenspezifischen Anforderungen wie der PCI-DSS gibt es weitere, allgemeinere Zertifikate zu Aufbau, Infrastruktur und Sicherheit von Rechenzentren, die eine zeitsparende Hilfestellung sind. So teilt die noch relativ junge Norm DIN EN 50600 Rechenzentren in verschiedene Klassen ein. Das neue Rechenzentrum München Ost von noris network ist beispielsweise bereits gemäß DIN EN 50600 mit den höchsten Kategorien der entsprechenden Verfügbarkeitsklassen VK4 (Verfügbarkeitsklasse 4 von 4), SK4 (Schutzklasse 4 von 4) und EK3 (Energieeffizienzklasse 3 von 3) ausgestattet. Insbesondere die Anforderungen der DIN EN 50600 in Bezug auf Gebäudekonstruktion, Stromversorgung, Regelung der Umgebungsbedingungen, Infrastruktur der Telekommunikationsverkabelung sowie das Sicherungssystem und Maßgaben für Management und den Betrieb des Rechenzentrums werden hier aus externer Sicht überprüft. Eine weitere Richtlinie, die in diesem Zusammenhang an Bedeutung gewinnen wird, ist VdS 3406 „Sicherheitsmanagement für bauliche Objekte“, die über alle Einzelaspekte der Gefahrenerkennung und -abwehr die Abrundung zwischen physischer Sicherheit, Betrieb bis hin zur Informationssicherheit und der Sicherheitsorganisation herstellt.

Scope beachten

Die ISO/IEC 27001, eine der wichtigsten Normen im Bereich der Informationssicherheit, macht beispielsweise deutlich, dass man auch bei Zertifikaten genauer hinschauen muss. Ohne einen Check von Prüfkriterien, Abdeckungsbereich (Scope) und Gültigkeitszeitraum sagen Zertifikate wenig aus. Wichtig ist die Anwendungserklärung auf Basis des „Annex A“. Hier wird der Geltungsbereich der Normenanwendung definiert. Hintergrund: Bei der ISO 27001 können die geprüften Dienstleister beim Audit gewisse Bereiche ausschließen. Folge: Das Zertifikats-Siegel schmückt oft sehr pauschal die Webseiten von Dienstleistern und kann in die Irre führen, weil faktisch nur ein sehr kleiner Bereich des Unternehmens tatsächlich einbezogen wurde. Potenzielle Kunden sind somit gut beraten, bei der Evaluierung des Dienstleisters den Scope und die erfassten Bereiche in den Vergleich einzubeziehen. Also: Sind wirklich alle Rechenzentren, beziehungsweise alle relevanten Bereiche einbezogen? Sind zum Beispiel einzelne Kapitel des „Statements of Applicability“ (SoA) als nicht anwendbar definiert, kann es passieren, dass die Prozesse nur unzureichend oder nur teilweise hinsichtlich der Informationssicherheit geprüft und zertifiziert wurden.

Umsetzung selbst evaluieren

Wer es in die engere Auswahl geschafft hat, sollte nach Abschluss der Vorrecherchen persönlich besucht werden. Erst vor Ort lässt sich erkennen, wie Sicherheit konkret gelebt und implementiert wird. Wie wurden die in der DIN EN 50600 beschriebenen, nach einem Schalenprinzip angeordneten Schutzzonen baulich realisiert? Werden Zugangsbeschränkung und Vereinzelung zwischen den Sicherheitszonen zum Beispiel auch zwingend durchgehalten, wenn Lkw-weise Equipment angeliefert wird? Erst wenn die – oft aus Bequemlichkeit oder falsch verstandener Effizienz genutzten – Ausnahmen durch bauliche Maßnahmen an Schleusen, Türen und Wegen faktisch unmöglich sind, kann der Kunde sicher sein, dass hier Sicherheit gelebt und nicht nur für Audits inszeniert wird. ■

Messestand: Halle 9, Stand 9-405

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

Drei wichtige Forderungen, um Sicherheit und Performance in modernen Cloudumgebungen in Einklang zu bringen

IT-Sicherheit in der hybriden Cloud

Unternehmen können die Verantwortung für die Sicherheit ihrer Daten in der Cloud nicht abgegeben, auch dann nicht, wenn sie mit einem IaaS-Cloud-Provider zusammenarbeiten. Daher ist es für sie wichtig, genau zu verstehen, welche speziellen Anforderungen hybride Cloud-Umgebungen an die IT-Sicherheit haben. Doch wie lassen sich Workloads in der Cloud zuverlässig und lückenlos schützen, ohne die Vorteile der Cloud zunichte zu machen?

Von Liviu Arsene, Bitdefender

Unternehmen setzen zunehmend auf neue Konzepte wie Software Defined Datacenter (SDC), Hyperkonvergenz und die hybride oder Multi-Cloud. Egal welches Konzept für ein Unternehmen das passende ist, ein Faktor steht immer im Vordergrund: die Sicherheit der Daten. Um die Sicherheit des neuen, transformierten Rechenzentrums zu gewährleisten, sind drei Maßnahmen notwendig.

1. Übersicht erhöhen

Egal welche Form der Cloud, die Migration auf eine solche Infrastruktur ist mit vielen Herausforderungen verbunden, zum Beispiel mangelnde Transparenz hinsichtlich der auf verschiedene Strukturen verteilten Workloads. Darüber hinaus ringen IT-Sicherheitsexperten und Führungskräfte erfahrungsgemäß mit einem Mangel an Richtlinien und dem Umgang mit dem Zugriff nicht autorisierter Geräte. In hardwarezentrierten Umgebungen war es relativ einfach zu erkennen, was vor sich ging. Hosts und die meisten Workloads waren fest mit der Hardware verbunden. Mit der Virtualisierung und der folgenden Cloud-Technologie ging in vielen Rechenzentren, die nicht in entsprechende Lösungen investiert haben, die Übersicht zu einem gewissen Grad verloren.

Der alte, hardware-zentrierte Ansatz benötigte zudem ein deutlich größeres IT-Team für seine Wartung. Aus betrieblicher Sicht war das natürlich ein Albtraum. Einer der willkommenen Nebeneffekte der Virtualisierung war daher, dass immer kleinere Teams notwendig wurden, um die IT zu verwalten. Das moderne Rechenzentrum lässt sich im Idealfall mit nur einer softwaredefinierten Ebene verwalten, mit den Komponenten Server-Virtualisierung sowie software-definiertem Netzwerk (SDN) und Speicher (SDS).

In Sachen Sicherheit stellen diese größeren und komplexeren Netzwerke im virtualisierten Zeitalter jedoch komplett neue Anforderungen an die IT. In ihnen ist es deutlich schwieriger geworden herauszufinden, ob, wie und wann ein Netzwerk kompromittiert wurde – und IT-Teams verbringen seitdem sehr viel mehr Zeit damit, ihr Netzwerk zu schützen, als vorher. Eine der sicherheitsrelevanten Aufgaben besteht darin, tote Winkel im Netzwerk zu beseitigen, also Bereiche, die sich im Dunklen befinden, wie etwa die Schatten-IT oder gut versteckte Angriffe auf das Unternehmensnetzwerk durch Cyberkriminelle. Es bedarf einer Sicherheitsstrategie, die für höhere Transparenz sorgt und tote Winkel beseitigt. Um das zu erreichen, muss in Lösungen für Sicherheit und Netzwerküberwachung investiert werden, die alle Bestandteile der verwalteten Infrastruktur abdecken, egal wo sie sich befinden.

2. Die richtigen „Waffen" auswählen

Sicherheitslösungen müssen speziell für das moderne, flexible Rechenzentrum entwickelt worden sein, um sicherzustellen, dass Unternehmen maximalen Nutzen aus den ausgewählten Strukturen ziehen können. Herkömmliche Sicherheitslösungen für Endpoint Security wurden ursprünglich für hardwaredefinierte, standortbasierte Infrastrukturen konzipiert. Sie sind für das moderne Rechenzentrum komplett ungeeignet, da sie ineffizient in der Wartung und Bereitstellung und oft unwirksam gegen ausgeklügelte, gezielte Angriffe sind. Das moderne Rechenzentrum erfordert Sicherheitslösungen zur Abwehr von

Angriffen, die sowohl lokale als auch virtuelle Umgebungen adressieren können.

3. Sicherheit genauso skalieren wie die Cloud

Einer der wichtigsten Vorteile der digitalen Transformation besteht darin, Infrastrukturen flexibel nutzen zu können. Bei hohem Bedarf kann man die Infrastruktur schnell erweitern und wenn der Bedarf dann wieder nachlässt, „schrumpft" man wieder auf „Normalgröße" zurück. Mit modernen Verwaltungslösungen funktioniert das automatisch: Ressourcen wie Speicher, Bandbreite oder Rechenpower werden anhand des Bedarfs bereitgestellt und provisioniert. Diese Flexibilität macht die Absicherung dieser Workloads jedoch zum Problem – zumindest für traditionelle Sicherheitslösungen, die für hardware-zentrische Workloads entwickelt wurden. Die Absicherung von Workloads in virtualisierten Umgebungen bedarf daher der gleichen Grundsätze der Skalierung: Die Sicherheitslösungen müssen genauso wie die Workloads automatisch und flexibel skalierbar sein. Grundlage für die automatische Provisionierung von jeglichen Ressourcen, inklusive der dazugehörenden Sicherheit, sind die auf das jeweilige Unternehmen speziell zugeschnittenen Richtlinien. Das ermöglicht es auch, das Sicherheitsniveau an den Bedarf anzupassen.

Webserver sind beispielsweise die am meisten bereitgestellten virtuellen Maschinen (VMs). Das bedeutet, dass eine geeignete Sicherheitslösung immer dann, wenn neue Webserver-VMS bereitgestellt werden, jeden neu erzeugten Workload automatisch absichert und standardmäßige Sicherheitsrichtlinien anwenden muss. Und das, ohne die Gesamtleistung und Stabilität der Infrastruktur zu beeinträchtigen.

Fazit

Die Modernisierung des Rechenzentrums kann zweifelsohne einen sehr positiven Einfluss auf ein Unternehmen als Ganzes haben. Sie vergrößert die Flexibilität des Unternehmens und senkt gleichzeitig die Betriebskosten. Doch sowohl die Anzahl als auch die Gewieftheit der Cyberattacken steigt ständig an und für die meisten Chief Information Security Officer ist es nur eine Frage der Zeit, bis eine der Attacken auch ihr Unternehmen erreicht, sollte es nicht optimal gesichert sein. Um das Unternehmen adäquat zu schützen, müssen IT-Verantwortliche jetzt die Transparenz in ihre Systeme erhöhen und geeignete Sicherheitslösungen einsetzen, die sich genauso flexibel skalieren lassen, wie die virtualisierten Systeme, die sie schützen sollen.

Messestand: Halle 10.0, Stand 10.0-621

NEVIS zeigt Anomalie-Erkennung und „Mobile Authentication“

Die NEVIS Security Suite sichert Portale von Banken, Versicherungen und Behörden und wird heute von Unternehmen weltweit eingesetzt. Sie schützt in der Schweiz über 80 Prozent aller E-Banking-Transaktionen und zahlreiche kritische E-Services weltweit. Auf der it-sa präsentiert das Unternehmen nevisDetect und eine neue Lösung für die mobile Authentisierung.

Von Stephan Schweizer, NEVIS Security GmbH

Es genügt längst nicht mehr, dass Unternehmen die Kundendaten schützen und gegen Diebstahl sichern, es ist inzwischen von zentraler Bedeutung, dass die Sicherheitsinfrastruktur feststellen kann, ob die Person, die sich online – egal von welchem Gerät – einloggt, auch wirklich der Nutzer ist, zu dem die Credentials gehören. Hierbei spielen zahlreiche Faktoren eine Rolle und nur eine durchgängige und auf verschiedene Authentisierungsmethoden zugeschnittene Lösung ist in der Lage, Abhilfe zu schaffen. Allerdings leiden bei vielen herkömmlichen Methoden das Bedienerlebnis und die Benutzerfreundlichkeit – niemand möchte im Urlaub automatisch aus seinen Accounts ausgesperrt werden, nur weil man sich aus einem anderen Land einloggt oder den Hardware-Token zu Hause vergessen hat. Die Balance zwischen Sicherheit und Einfachheit wird für viele Unternehmen zur Mammutaufgabe, bei der häufig an einem der beiden Enden gespart wird.

Die NEVIS Security GmbH ist auf der it-sa 2018 mit mehreren Neuheiten vertreten, die genau auf die veränderte Bedrohungslandschaft und die Kundenbedürfnisse zugeschnitten sind.

„Continuous Behaviour Analytics“

Inzwischen haben sich Online-Kriminelle bereits darauf eingestellt, dass sie beim Login in einen fremden Account Sicherheitsmaßnahmen umgehen müssen. Genau aus diesem Grund ist es wichtig, nicht nur den Login-Vorgang, sondern die gesamte Session kontinuierlich auf verdächtiges Verhalten zu untersuchen. Sich so vor Attacken zu schützen genießt höchste Priorität. Das gilt sowohl für Leistungsanbieter, die finanzielle Verluste und Reputationsschäden vermeiden wollen, als auch für Kunden, die ein Höchstmaß an Sicherheit erwarten.

Aktuell wurde eine neue Komponente zur Anomalie-Erkennung in die NEVIS Security Suite integriert, mit der „Continuous Behaviour Analytics“ – also Sicherheit durch durchgängige Mechanismen – ermöglicht wird. Diese hochsichere, aber gleichzeitig User-freundliche Komponente reiht sich als nevisDetect in die Security-Suite ein und wird auf der it-sa anhand von Live-Demos zu sehen sein.

Bei der Entwicklung der Komponente wurde beachtet, dass eine herkömmliche Zwei-Faktor-Authentisierung keinen ausreichenden Schutz mehr vor Identitätsdiebstahl oder Man-in-the-Browser-Angriffen bietet, die auf Schadprogrammen basieren. Hinzu kommt, dass eine Authentisierung mit mehreren Faktoren das Nutzererlebnis beeinträchtigt und so die Kundenbindung schwächt. Um die Sicherheit kritischer Dienste zu erhöhen, ohne Abstriche bei der Benutzerfreundlichkeit zu machen, sind deshalb neue, ganzheitliche Sicherheitskonzepte gefragt. Genau diese Anforderungen standen bei der Entwicklung von nevisDetect im Mittelpunkt. nevisDetect erkennt Verhaltensanomalien und berechnet für jede Benutzerinteraktion im Hintergrund einen Risikowert. Werden dabei gewisse Schwellwerte überschritten, so ist das System in der Lage, entsprechende Gegenmaßnahmen bis hin zum Session-Abbruch zu ergreifen.

Mobile Authentisierung

Ergänzend zur kontinuierlichen, verhaltensbasierten Authentisierung wird NEVIS auf der it-sa 2018 ihre neue Lösung für mobile Authentisierung einem breiten Publikum vorstellen. Jeder Mensch beschäftigt sich heute im Durchschnitt

mehr als drei Stunden täglich mit seinem mobilen Gerät. Egal, was verkauft oder gekauft werden möchte, es muss eine Möglichkeit bestehen, das einfach und sicher über ein mobiles Gerät erledigen zu können. Zudem wollen Kunden ihre Mobilgeräte zunehmend als primären oder sogar alleinigen Kanal für den Kontakt zu Unternehmen nutzen.

Technisch basiert die Mobile-Authentication-Lösung auf dem FIDO UAF-Standard. NEVIS unterstützt damit das Konzept „Mobile as a Token", bei dem das Mobilgerät als Speicherort von Schlüsselmaterial für die Authentisierung dient. Die neue Lösung erlaubt eine benutzerfreundliche starke Authentisierung auf dem Mobilgerät mit gängigen Mechanismen wie Fingerabdruckerkennung oder Face-ID. Die Authentisierung kann direkt in einer App (In-App) geschehen, oder auch für eine Webapplikation via Out-of-Band Push-Nachrichten. Auf dieselbe Weise lässt sich die Lösung auch für das Bestätigen von Transaktionen nutzen. Damit deckt die Mobile-Authentisierungs-Lösung zentrale Anwendungsfälle ab, wie sie für Angebote wie das Mobile-Banking gebraucht werden.

NEVIS MobiIe Authentication ist eine gute Ergänzung für die verhaltensbasierte, kontinuierliche Authentisierung. Einerseits ermöglicht sie eine benutzerfreundliche 2-Faktor-Authentisierung, andererseits kann sie aber auch im Verlauf der Session dazu benutzt werden, um Situationen mit erhöhtem Risiko aufzulösen, indem der Benutzer über einen separaten Kanal die Möglichkeit hat, seine Identität zu bestätigen.

Die Mobile-Authentication-Lösung erfüllt dabei höchste Ansprüche im Bereich Datenschutz und Sicherheit. So werden beispielsweise keinerlei biometrische Daten (Fingerabdruck etc.) an den Dienstanbieter übertragen, sämtliche Daten zur biometrischen Benutzererkennung verbleiben auf dem Gerät des Benutzers. Aufseiten des Dienstanbieters wird lediglich ein öffentlicher Schlüssel hinterlegt, mit dem sämtliche Interaktionen über kryptografische Mechanismen verifiziert werden können. Damit erfüllt die Lösung auch vollumfänglich die Anforderungen neuer Regulatorien, wie der DSGVO oder PSD2.

Die Bausteine „Mobile Authentication" und „Continuous Behaviour Analytics" bilden in Kombination mit klassischen Identity-Management-Funktionen ein umfassendes Customer-Identity-and-Access-Management-(CIAM)-System, das die effiziente, sichere und benutzerfreundliche Bewirtschaftung von digitalen Kunden-Identitäten ermöglicht.

CIAM-System

Die NEVIS Security Suite bietet neben der reinen sicheren Verwaltung von Identitäten und deren Authentifizierungsfaktoren auch eine Rundumsicht auf den Kunden. „Know your customer" dient als Basis für die Erstellung maßgeschneiderter Angebote und bildet somit die Grundlage für die Stärkung der Marktposition und der Kundenzufriedenheit jedes Unternehmens. Heute bedeutet ein solides CIAM-System nicht nur mehr Sicherheit, es spart durch höhere Benutzerfreundlichkeit auch Zeit und verringert Support-Anfragen. Damit wird es für jedes Unternehmen, das auf Nutzerkonten setzt, ein Muss. ■

Vorträge von NEVIS auf der it-sa

Dienstag, 09.10.2018, 11:00 bis 11:15 Uhr, M10 – Management Forum in Halle 10.1
Digitale Transformation – Business-Disruptor oder kalter Kaffee?
Stephan Schweizer, Chief Product Officer (CPO) – AdNovum Informatik AG

Dienstag, 09.10.2018, 15:30 bis 15:45 Uhr, T10 – Technology Forum in Halle 10.0
AdNovum – Live-Hacking: Cybercrime in der Realität – ist Ihr Unternehmen „richtig" geschützt?
Konstantin Luttenberger, Pre-Sales – AdNovum Informatik AG

Dienstag, 09.10.2018, 16:30 bis 16:45 Uhr, NEVIS-Stand
Live-Hacking-Demo
Konstantin Luttenberger, Pre-Sales – AdNovum Informatik AG
anschließend: Apéro/Umtrunk

Mittwoch, 10.10.2018, Congress@it-sa im NCC Mitte
Kongress FSP – Präsentationen von NEVIS, Partnern und Kunden

Messestand: Halle 10.0, Stand 10.0-316

Intercept X for Server

Innovativ. Umfassend. Stark.

Schutz für kritische Anwendungen und Daten in Ihrer Organisation, dank mehrerer Schutztechnologien:

- Neuronales Deep-Learning-Netzwerk: Schutz vor bislang unbekannter Malware
- Anti-Exploit: Verhindert, dass Angreifer mit gängigen Hacking-Techniken Erfolg haben
- Server Lockdown: Ermöglicht das Whitelisting von Anwendungen mit nur einem Klick

Kostenlos testen:
www.sophos.de/server

SOPHOS

Cybersecurity made simple.

WAVELINE-MAR.COM

Platin-Award „Enterprise Firewalls" von SecurityInsider | Platin-Award „Identität und Sicherheit" von eGovernment Computing | Platin-Award „Business Antivirus" von SecurityInsider | ITK-Produkte des Jahres im Bereich „Cybersecurity" von der Funkschau | „Hersteller des Jahres Security" von dem Channel-Fachmagazin CRN

Digitalisierung in Staat und Wirtschaft:

Mehr Leistung durch IT-Sicherheit

Die Digitalisierung ist mit dem Versprechen angetreten, unsere Welt effizienter werden zu lassen: Prozesse werden beschleunigt, Aufwände verringert und Kommunikation erleichtert. Wie sehr das in vielen Bereichen bereits gelungen ist, zeigen der tiefgreifende Wandel der Arbeitswelt seit Beginn der digitalen Revolution und die Beschleunigung, die viele Abläufe dadurch erfahren haben. Aber dort, wo besonders sensible oder gar eingestufte Informationen ins Spiel kommen, gerät die Digitalisierung oft noch ins Stocken. Moderne, ganzheitliche IT-Sicherheitsansätze helfen jedoch dabei, Hindernisse aus dem Weg zu räumen. Zudem erhöhen sie oftmals sogar die Performance von Systemen. In vielen Fällen macht IT-Sicherheit, die früher nicht selten als Bremsklotz empfunden wurde, eine weitere Digitalisierung überhaupt erst möglich – und fungiert somit als Motor für den weiteren Fortschritt.

Von Patrick Franitza, secunet Security Networks AG

Ganzheitliche IT-Sicherheit wirkt auf zwei Ebenen. Zum einen sind Staat, Gesellschaft und Wirtschaft konkreten Gefahren ausgesetzt. Wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) Anfang dieses Jahres meldete, wurden knapp 70 Prozent der Unternehmen und Institutionen in Deutschland in den Jahren 2016 und 2017 Opfer von Cyberangriffen. Jeder zweite erfolgreiche Angriff führte dabei zu Produktions- beziehungsweise zu Betriebsausfällen. Behörden und Großunternehmen sind sich dieser Gefahr und der Notwendigkeit, Gegenmaßnahmen zu ergreifen, durchaus bewusst. Doch insbesondere in Industrie, kritischen Infrastrukturen und im Mittelstand klaffen noch große Lücken, die es zu schließen gilt.

Zum anderen können aktuelle IT-Sicherheitslösungen, richtig eingesetzt, die Leistung von Prozessen, Netzwerken und Infrastrukturen erhöhen. Somit ist IT-Sicherheit kein notwendiges Übel. Ganz im Gegenteil trägt sie dazu bei, das zentrale Effizienzversprechen der Digitalisierung einzulösen. Auf der it-sa 2018 zeigt secunet eine Reihe von Produkten und Lösungen, die das belegen.

SINA

Ein Beispiel dafür ist die SINA Workstation. Als Teil des SINA Produktportfolios ist diese Familie von Krypto-Clients für den Umgang mit eingestuften Daten zugelassen, in speziellen Varianten bis zur Geheimhaltungsstufe GEHEIM. Dabei verbindet die SINA Workstation ein hohes Maß an Sicherheit mit komfortabler Handhabung: So lassen sich etwa Daten unterschiedlicher Sicherheitseinstufungen parallel verarbeiten. Der Anwender bewegt sich jederzeit sicher in der vertrauten Arbeitsumgebung (z. B. MS Windows) – online wie offline, im Büro oder unterwegs. Auf der it-sa 2018 stehen vor allem (ultra-)mobile SINA Client S Innovationen im Fokus.

SINA stellt zudem Funktionen bereit, die den Verwaltungsaufwand in großen und komplexen Sicherheitsarchitekturen erheblich reduzieren: Mit SINA SOLID etwa lassen sich sehr große und flexible IPsec-Netze automatisiert konfigurieren – und das bei gesteigerter Performance.

Die Kooperationsplattform SINA Workflow ermöglicht den medienbruchfreien, vorschriftenkonformen Umgang mit digitalen Verschlusssachen (VS) über deren gesamte Lebensdauer, das heißt von der Erstellung über die Bearbeitung bis zur Vernichtung. Papierbasierte VS-Registraturen haben somit ausgedient.

Innere Sicherheit und IT-Grundschutz

Bei der Identitätsfeststellung sind Polizisten heutzutage vermehrt auf hochmobile Systeme angewiesen, die relevante Prüfergebnisse in

Echtzeit liefern. secunet präsentiert auf der it-sa die Lösung secunet bocoa android, eine Smartphone-App, die der mobilen Identitätsfeststellung sowie zur Prüfung elektronischer Ausweisdokumente dient.

Ein angemessenes IT-Sicherheitsniveau nach IT-Grundschutz zu managen, ist angesichts sich verkürzender Produktlebenszyklen und immer komplexer werdender IT-Infrastrukturen nicht einfach. Der „automatisierte Grundschutz" (aGS) von secunet ist eine völlig neue Methodik, mit der innerhalb kürzester Zeit sichere Soll-Konfigurationen gezielt umgesetzt werden können – ein weiteres Beispiel für die Kombination von Sicherheit und Effizienz, das sich bereits in der Praxis bewährt.

Sichere IT für kritische Infrastrukturen

Kritische Infrastrukturen (KRITIS) erfordern grundsätzlich einen hohen Schutz, da sie direkt von IT-gestützten Systemen abhängig sind und Ausfälle sowie Beeinträchtigungen zu dramatischen Folgen für Wirtschaft und Gesellschaft führen können. Doch auch hier lässt sich ein hohes Sicherheitsniveau mit Effizienzsteigerungen verbinden. Denn erst durch den Einsatz hochwertiger IT-Sicherheitslösungen werden sichere und manipulationsgeschützte Verbindungen zwischen Netzen und ein geschützter Fernzugang zu sensiblen IT-Bereichen wie zum Beispiel Prozessleit- und Automatisierungssystemen möglich, die bisher undenkbar waren. Das Ergebnis: wirksamer Schutz bei gleichzeitiger Effizienz- und Leistungssteigerung.

Speziell für KRITIS-Betreiber hat secunet das Konzept der Security Infrastructure entwickelt, das Netzzonen zuverlässig absichert. Durch ganzheitliche Sicherheitskonzepte und -prozesse können Cyberangriffe, Spionage und Sabotage wirksam abgewehrt werden.

Bei der künftigen Kommunikation aus der Arztpraxis in die Telematikinfrastruktur ist der secunet konnektor das sicherheitstechnische Herzstück. Der äußerst leistungsstarke Konnektor bietet eine schnelle und reibungslose Anbindung, einen verlässlichen Betrieb und Erweiterungen um künftige Anwendungen.

Sicher surfen und telefonieren

Uneingeschränkt sichere Internetzugänge für Organisationen mit erhöhtem Schutzbedarf bietet secunet safe surfer. Durch die strikte Trennung von Ausführung und Darstellung aktiver Inhalte ermöglicht die intelligente IT-Sicherheitslösung allen Mitarbeitern sicheres und komfortables Arbeiten. Die Lösung basiert auf dem Ansatz „Remote Controlled Browser System" (ReCoBS) des BSI. Dabei wird der Internetbrowser nicht auf dem schützenswerten lokalen System ausgeführt, sondern in einem Quarantäne-System außerhalb des sensiblen Netzwerkbereichs. So können das Ausnutzen von Schwachstellen, das Einnisten von Schadsoftware oder unbemerkter Datenabfluss wirkungsvoll unterbunden werden.

Der Trend zu Web- und Cloud-Anwendungen führt zu einer Vielfalt an Portaltechnologien und Protokollen. secunet protect4use realisiert eine benutzerfreundliche und sichere Multi-Faktor-Authentisierung für internetbasierte Dienste wie Web- oder Kundenportale – unabhängig von Browser, Plattform, Betriebssystem und Protokoll.

Eine sichere Voice-over-IP-Telefonie (VoIP-Telefonie) zwischen verschiedenen Unternehmen oder Unternehmensbereichen wird mit secunet SBC als Session Border Controller möglich. Die Lösung setzt eine optimale Verknüpfung von verschiedenen VoIP-Netzen um und ist zentraler Zugangspunkt für diese Netze. Weiterhin übernimmt secunet SBC als Firewall zentrale Aufgaben zum Schutz des internen Netzes und bietet zudem Fraud Detection und Prevention, um vor weiteren Angriffen von außen zu schützen.

In Nürnberg zeigt secunet neben den dargestellten Lösungen viele weitere Leistungen und Produkte für Sicherheitsbehörden, öffentliche Bedarfsträger, militärische Organisationen und Behörden, KRITIS-Betreiber und die Automotive-Industrie. ■

Messestand: Halle 10.0, Stand 10.0-307

Vorträge von secunet auf der it-sa

Mittwoch, 10.10.2018, 10:30 Uhr, Management Forum, Halle 10.1
Red Teaming: Advanced threat assessment through simulated attacks
Referent: Kevin Ott, Berater und Penetrationstester bei secunet

nexus Enabling trusted identities

Identity und Access Management

Virtuelle Smartcards **Public Key Infrastructure**

Multi-Faktor-Authentifizierung Informationssicherheit

Single Sign-On **Credential Management**

Chipkarten **IoT-Sicherheit** Card- und Hardware

Zertifikatsmanagement Elektronische Signaturen

Zugriffskontrolle **Ausweismanagement**

Berechtigungsmanagement

Treffen Sie uns auf der it-sa:
IAM-Area, Stand 10.0-420

nexusgroup.com

Herausforderung hybride Umgebungen

Wie man auch beim Einsatz von Office 365 seine Daten schützen kann

Nach einer aktuellen Gartner-Befragung setzen 61 Prozent der Unternehmen Office 365 ein und weitere 23 Prozent planen es innerhalb der nächsten sechs Monate. Die wenigsten nutzen Office 365 jedoch als reine Cloud-Lösung und speichern nach wie vor (sensible) Daten auch lokal. Hieraus ergeben sich in Sachen Datensicherheit jedoch große Probleme.

Von Thomas Ehrlich, Varonis Systems

Die Datenwelt wird hybrid: Neben dem immer verbreiteteren geschäftlichen Einsatz von mobilen Endgeräten hat dazu insbesondere Office 365 beigetragen. Zahlreiche Unternehmen verfolgen zwar einen Cloud-First-Ansatz, dennoch werden gerade geschäftskritische Anwendungen und sensible Daten nach wie vor lokal gehostet. Für die IT-Sicherheit bedeutet das jedoch eine große Herausforderung, da sie lokalen Schutz und Cloud-Security vereinen muss.

Office 365 verfügt über eingebaute Sicherheits-Features, die je nach gewähltem Abo einen gewissen Schutz bieten – allerdings nur für solche Dateien, die innerhalb der Plattform bleiben und diese nie verlassen. Tatsächlich sind Daten jedoch mobil und ständig in Bewegung, wandern etwa von E-Mails auf SharePoint und auf lokale Speicher. Spätestens hier greift jedoch der native Schutz nicht mehr: Office 365 ist blind für Daten, die lokal gespeichert werden. IT-Sicherheitsverantwortliche können dadurch nicht oder nur äußerst schwierig nachvollziehen, wer wann was mit den Daten macht, geschweige denn wer überhaupt auf welche OneDrive-Ordner, SharePoint-Websites und Exchange-Postfächer zugreifen kann. Defizite gibt es zudem bei der Identifizierung gefährdeter Dateien und sensibler Ordner, die extern freigegeben wurden, sowie nicht mehr benötigter Berechtigungen.

Cloud-Security ist auch keine Lösung

Ähnlich verhält es sich bei Cloud-Security-Lösungen: Sie stoßen vor allem dann an Grenzen, wenn es darum geht, eine einheitliche, umfassende Sicht auf die Daten zu erhalten. Cloud-Access Security Broker (CASB) eignen sich hervorragend dafür, die unbefugte Nutzung von Cloud-Diensten zu unterbinden, den Zugriff auf nicht genehmigte Cloud-Anwendungen zu blockieren und unbefugte Daten vor einer externen Freigabe zu schützen. Aber so nützlich und wichtig diese Funktionen auch sind, reine Cloud-Lösungen haben dennoch keinen Zugriff auf und keine Informationen über die lokale Infrastruktur und weisen entsprechend Schwierigkeiten mit hybriden Umgebungen auf.

Die Frage lautet also: Wie kann man beide Welten so vereinen, dass die Datensicherheit zu jedem Zeitpunkt sichergestellt ist und die gesetzlichen Anforderungen eingehalten werden? Gerade Audits und ein übersichtliches Reporting werden durch die hybride Speicherlandschaft deutlich erschwert. In aller Regel müssen Informationen aus diversen Quellen mit teilweise unterschiedlichen Informationen und Kriterien geprüft, bewertet, zusammengefasst und manuell erstellt werden. Diese Herangehensweise ist jedoch zeitaufwendig und fehleranfällig. Auch droht wesentlicher Kontext übersehen zu werden, durch den sich auffälliges abnormales Nutzerverhalten identifizieren lassen könnte.

Varonis Office 365 Suite

Vor diesem Hintergrund hat Varonis seine Office 365 Suite entwickelt, die auf der it-sa vorgestellt wird. Sie ist in der Lage, sämtliche Datenzugriffe unabhängig vom Speicherort zu managen und zu kontrollieren und damit die Sicherheit und Integrität der Dateien zu gewährleisten:

- **Einheitliche Kontrolle über lokal gespeicherte Daten und Office-365-Daten:** Als einheitliche Plattform stellt Varonis sicher, dass nur die richtigen Personen jederzeit Zugriff auf die Daten haben, wobei die komplette Nutzung überwacht und Missbrauch gemeldet wird.
- **Vollständige Transparenz und Verwaltung von Berechti-**

Drei Sicherheitstipps für Office 365

Versteckte sensible Daten identifizieren!
Unternehmen müssen jederzeit in der Lage sein, alle Dateien zu finden, die sensible und personenbezogene Informationen enthalten. Die integrierte Klassifizierung von Microsoft erfordert eine manuelle Erstellung und Kennzeichnung von Regeln – was in großen Umgebungen angesichts von Zehntausenden von Dateien besonders umständlich und zeitraubend sein kann – und erstreckt sich nicht auf lokale Datenspeicher. Entsprechend ist Automatisierung hierbei der Schlüssel, wobei darauf zu achten ist, dass diese alle Speicherorte einbezieht.

Minimale Rechtevergabe!
Bei Microsoft sind die Berechtigungen nur eingeschränkt sichtbar und die Möglichkeiten zum Auffinden von sensiblen Daten begrenzt. Durch die Einführung eines Privilegienmodells auf Basis der minimalen Rechtevergabe wird sichergestellt, dass jeder Mitarbeiter nur Zugriff auf diejenigen Dateien erhält, die er für seine Arbeit tatsächlich benötigt (Need-to-know-Prinzip). Hierdurch wird das Risiko signifikant reduziert.

Auf Datenverantwortliche setzen!
Die Einbeziehung von Datenverantwortlichen in den Prozess der Berechtigungsprüfung ist entscheidend für die Durchsetzung eines Privilegienmodells auf Basis der minimalen Rechtevergabe. Sie sind nicht in der IT-Abteilung, sondern in den entsprechenden Fachabteilungen oder Projektgruppen beheimatet und verantworten und gewähren die Zugriffsrechte. Das hat den Vorteil, dass sie genau wissen, wer welchen Zugriff benötigt.

gungen: Innerhalb von Sekunden kann die IT-Abteilung potenzielle Zugriffe für jeden Benutzer oder jede Gruppe in Active Directory, Azure AD oder einem lokalen System visualisieren oder melden, gefährdete sensible Daten lokalisieren und zu weit gefasste Berechtigungen identifizieren.

Erkennen sensibler Daten: Um Risikobewertungen durchführen sowie Bedrohungen überwachen und entsprechend adressieren zu können, müssen Office-365-Kunden wissen, wo sich ihre sensiblen Daten befinden. Mit Bordmitteln ist das nur manuell und sehr aufwendig möglich. Varonis klassifiziert automatisiert sensible Daten in OneDrive, SharePoint Online und lokalen Speichersystemen und liefert unverzichtbaren Kontext zu gefundenen sensiblen Inhalten.

Umfassende Audit- und Überwachungsprozesse: Varonis stellt zentralisierte Audit- und Benachrichtigungsfunktionen für Exchange Online, SharePoint Online und OneDrive bereit. Ein einheitlicher, durchsuchbarer Audit-Trail führt die Office-365-Aktivitäten eines Benutzers mit lokalen Zugriffsaktivitäten auf NAS-Geräten, Active Directory, Dateifreigaben, UNIX, Exchange und mehr zusammen.

Erweiterte Bedrohungserkennung (UEBA): Varonis analysiert Benutzeraktivitäten und -verhaltensweisen in hybriden Umgebungen und erstellt verhaltensbasierte Normalszenarien für jeden Account. Datenzugriffe werden unter Berücksichtigung des Sensibilitätsgrads der Daten, von Berechtigungen und Active-Directory-Metadaten analysiert und damit abnormales Verhalten identifiziert, weshalb sie präzise Warnmeldungen ausgeben kann und seltener Fehlalarm auslöst.

Fazit

Mit der Varonis Office 365 Suite steht damit erstmals eine Lösung für einheitliche Datensicherheit und Kontrolle der Zugriffsrechte auf Dateien zur Verfügung – unabhängig davon, ob sie in der Cloud oder lokal gespeichert werden. Durch entsprechende Automatisierungsmöglichkeiten und einheitliches Management der Zugriffsrechte unabhängig vom Speicherort wird zudem die IT-Abteilung deutlich entlastet. ■

Messestand: Halle 9, Stand 9-435

Vorträge von Varonis auf der it-sa

Dienstag, 9. Oktober 2018, 11:15 bis 11:30 Uhr, M9 – Management Forum in Halle 9
Next-Gen Dateisicherheit trifft auf Next-Gen Cloud Dateidienste
Sprecher: Christoph Spitzer, Senior Customer Success Manager DACH, Varonis und Zeljko Dodlek, RSM Dach, Nasuni

Dienstag, 9. Oktober 2018, 15:00 bis 15:20 Uhr, I10 – Forum International in Halle 10.1
3 Schritte zur Sicherstellung der Compliance im Zeitalter der DSGVO
Sprecher: Matthias Schmauch, Enterprise Sales Representative, Varonis

Mittwoch, 10. Oktober 2018, 16:30 bis 16:45, T9 – Technik Forum in Halle 9
7 bewährte Vorgehensweisen für Datensicherheit in hybriden Umgebungen
Sprecher: Matthias Schmauch, Enterprise Sales Representative, Varonis

Donnerstag, 11. Oktober 2018, 11:45 bis 12:00, M9 – Management Forum in Halle 9
3 Schritte zur Sicherstellung der Compliance im Zeitalter der DSGVO
Sprecher: Matthias Schmauch, Enterprise Sales Representative, Varonis

NCP Enterprise Management als Mittler zwischen IT und operativer Technologie

Sicherheit als zentrale Instanz

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 GmbH

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 (engl. IIoT), immer mehr einzelne Punkte miteinander. Die Verständigung wird dadurch aber immer schwieriger. Das 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.

Produktionsumgebung treibt Cloud-Nutzung

Berücksichtigt werden muss dabei auch das Thema Cloud. Vielen 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.

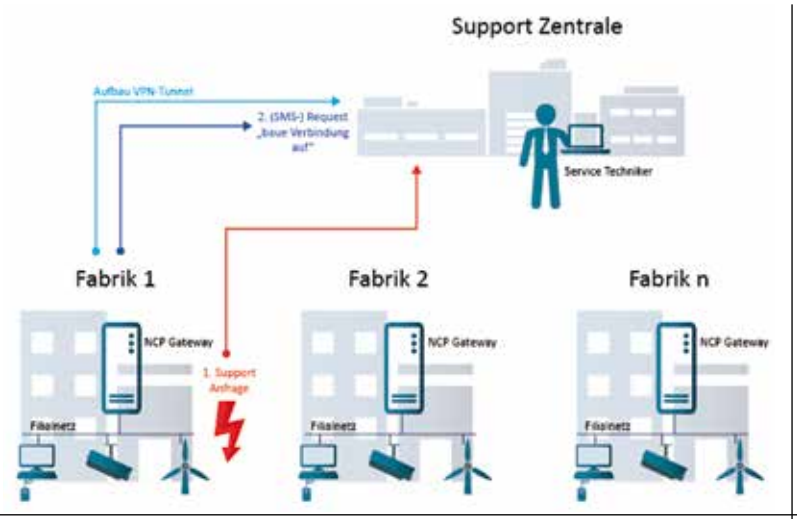
Wie lassen sich diese Sicherheitsanforderungen der Produktionsumgebung in ein übergreifendes Sicherheitskonzept eingliedern? Traditionell handelte es sich bei IT und OT um technisch und organisatorisch getrennte Welten ohne Berührungspunkte. Heute werden abteilungsübergreifend alte und neue Produkte, Techniken 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 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.

Das ermöglicht jedoch nicht jede VPN-Lösung. Zwar nutzen VPNs etablierte Techniken und sind von vielen Herstellern verfügbar, allerdings mit maßgeblichen 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 unübersichtliche Dimensionen. Es kommt beim effektiven Schutz darauf an, auch große Verbindungsmengen mit möglichst geringem Aufwand zu verwalten und einen Überblick zu behalten.

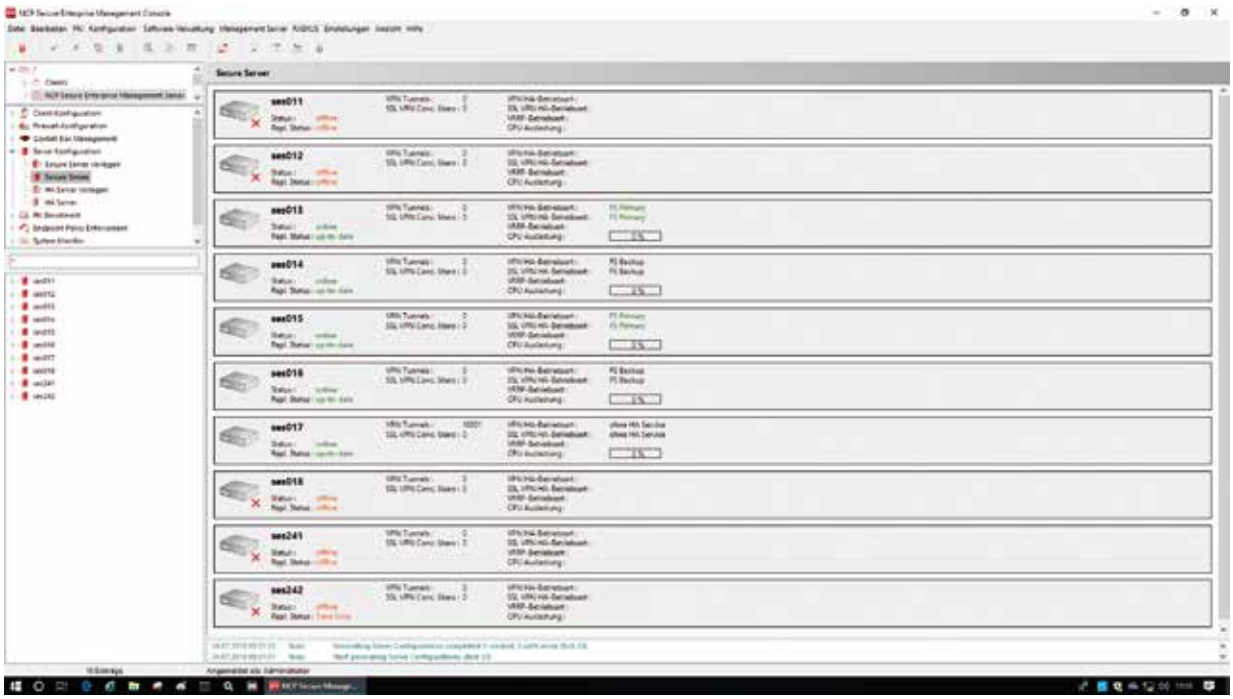
Unterstützung bei der einheitlichen Verwaltung erhalten die IT- und OT-Abteilungen von Geschäftsleitung und Controlling. Eine Konsolidierung ist nicht nur aus Sicht der Sicherheit sinnvoll, auch die Kosten lassen sich mit einer homogenen Lösung besser kontrollieren. Das lokale Netz kann auf externe Teilnehmer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



Kontaktaufnahme: NCPs IIoT-Gateway kann selbstständig eine Verbindung initiieren

VPN-Gateways für OT und IT von NCP

Für den Nürnberger VPN-Hersteller NCP sind diese Anforderungen mittlerweile Tagesgeschäft. Aus deren VPN-Gateways, die traditionell im Bereich IT eingesetzt wurden, ist eine universelle Plattform geworden, die in beiden Welten zu Hause ist. Die Produkte sind seit Jahren im Einsatz und sichern in Hunderten von Installationen die Verbindungen ab. Die neuen Anforderungen aus der OT wie automatische Authentifizierung und hohe Skalierbarkeit spiegeln sich in



Zentrale Instanz für Sicherheit: NCP VPN Gateways können die Brücke zwischen IT und OT schlagen

Erweiterungen der Standard-VPN-Server und speziellen Gateways für IIoT-Umgebungen wider. Darüber hinaus können mit der Management-Plattform auch große Mengen von Verbindungen weitgehend automatisiert verwaltet werden. Viele Schnittstellen zu Drittanbietern ermöglichen die Integration in bestehende Umgebungen.

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 das 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 vor dem 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. Die IIoT-Gateways 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 unterstützt das Gateway. Ebenfalls möglich sind 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 von 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

Messestand: Halle 10.0, Stand 10.0-120

Ein Siegel – Volle Sicherheit ISO 27001 und KRITIS

Ob mit dem Internet verbunden oder nicht: Kein IT-System ist sicher. Gleichwohl müssen bis zum 30. Juni 2019 die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr dem BSI nachweisen, dass ihre IT-Sicherheit dem „Stand der Technik" entspricht.

Ein guter Ausgangspunkt ist die ISO 27001. Lassen Sie jetzt Ihr Informationssicherheits-Managementsystem zertifizieren. Profitieren Sie dabei von der langjährigen Expertise von TÜV SÜD: Sicherheit, Vertrauen und Qualität – dafür steht unser Siegel.

Wir prüfen Ihre IT-Infrastruktur und sorgen gemeinsam mit Ihnen dafür, Ihre IT-Sicherheit zu verbessern. Sprechen Sie uns an!

www.tuev-sued.de/ms/iso-27001

TÜV SÜD

Management Service

Mehr Wert.
Mehr Vertrauen.

BESUCHEN SIE UNS AUF DER IT-SA
Halle 9, Stand 9-458

TÜV SÜD Management Service GmbH Ridlerstrasse 65, 80339 München, Deutschland
Tel.: 0800 5791-5000 ms-anfragen@tuev-sued.de www.tuev-sued.de/ms/iso-27001

TÜV®

Wie sicher sind Industrieanlagen?

Die Bedrohung durch Cyberangriffe auf Industrieanlagen steigt. Sie werden aggressiver, technisch komplexer und sind besser organisiert denn je. Um den künftigen Anforderungen zu entsprechen, muss die Sicherheit von Endgeräten, Maschinen und Anlagen über den gesamten Lebenszyklus hinweg gewährleistet sein.

Von Thomas Gronenwald, KPMG AG Wirtschaftsprüfungsgesellschaft

Die Welt der vernetzten Dinge entwickelt sich zu einem milliardenschweren Wachstumsmarkt. Durch das Internet of Things (IoT) werden Alltagsgegenstände, Fahrzeuge, Häuser, Fabriken und ganze Städte miteinander vernetzt. Das eröffnet ungeahnte Möglichkeiten für Verbraucher sowie enorme Effizienzsteigerungen und resultierende Kostensenkungen für Unternehmen.

In der Fabrik von morgen sind die Abläufe zunehmend digital vernetzt. Das erfolgt zum einen, um sehr flexibel und unternehmensübergreifend agieren zu können. Zum anderen gilt es, die Digitalisierung der Wertschöpfungskette vom Lieferanten bis zum Endkunden voranzutreiben. Eine derart umfängliche automatisierte Vernetzung ermöglicht es, schneller zu handeln, effizienter zu fertigen und konventionelle Geschäftsfelder durch neue Business-Modelle zu ergänzen.

Trotz aller Chancen birgt die zunehmende Vernetzung bekanntlich auch Risiken, deren Art und Ausmaß oftmals nicht bekannt sind – von Datendiebstahl und Serviceunterbrechungen bis hin zum gänzlichen Kontrollverlust über die einzelnen Geräte.

Wertschöpfungsfaktor Cybersicherheit

Unverzichtbare Grundvoraussetzung ist daher ein an die spezifischen Unternehmensbelange angepasstes Cybersicherheitsniveau. Um das enorme Potenzial von Industrie 4.0 erfolgreich umsetzen zu können, ist der sichere und vertrauensvolle Umgang mit Daten unabdingbar. Zudem muss ein verlässlicher Schutz der unternehmensübergreifenden Kommunikation vor Angriffen von außen gewährleistet sein. Infolgedessen entwickelt sich Cybersicherheit für Unternehmen immer mehr von einem reinen Kosten- zu einem wichtigen Wertschöpfungsfaktor. Nur die smarten Fabriken von morgen, die in der Lage sind, verlässlich und ohne größere Ausfallzeiten gleichbleibend hochwertige Produkte zu entwickeln und zu produzieren, werden den zukünftigen Markt- und Wettbewerbsanforderungen gerecht werden können.

Um den komplexen Anforderungen zu entsprechen, muss die Sicherheit von Endgeräten, Maschinen und Anlagen über den gesamten Lebenszyklus hinweg gewährleistet sein. Zugleich sollten Sicherheitsaspekte bereits bei der Produktentwicklung berücksichtigt werden. Auch müssen sich Unternehmen frühzeitig darüber Gedanken machen, wie sie nach einem Sicherheitsvorfall adäquat mit Cyberangriffen und deren Auswirkungen umgehen wollen. Das gilt vor allem im Hinblick auf die Kommunikation mit internen und externen Stakeholdern. Angesichts der zunehmenden Digitalisierung dürften Cyberangriffe im Zeitalter von Industrie 4.0 zum Tagesgeschäft gehören.

Daher ist es künftig unumgänglich, Cybersicherheit als integralen Bestandteil des Produktes oder der Dienstleistung zu betrachten – von der ersten Idee über den gesamten Produktlebenszyklus hinweg. Das bedeutet auch ein verstärktes Zusammenspiel von Geräteherstellern, Maschinenintegratoren und Anlagenbetreibern. Nur wenn allen Beteiligten die jeweiligen spezifischen Anforderungen bekannt sind, können Bedrohungen fundiert analysiert, Schutzziele ermittelt und Risiken gemanagt werden. Ein solcher ganzheitlicher Risikomanagementansatz versetzt Unternehmen darüber hinaus in die Lage, übergreifende Schutzmaßnahmen zu ermitteln, zu bewerten und effizient umzusetzen.

Doch nicht nur im Zusammenhang mit der zunehmenden Digitalisierung von Industrieanlagen und deren Wertschöpfungsketten gewinnen Sicherheitsaspekte immer größere Bedeutung. Auch im Internet of Things – der steigenden Vernetzung von Millionen intelligenter (Alltags-)Geräte und Sensoren – werden Sicherheitsfragen relevant. Das Internet der Dinge macht den Alltag angenehmer, die neuen Möglichkeiten erstrecken sich auf alle Lebensbereiche. Damit ergeben sich aber zugleich unzählige Angriffsflächen.

Im privaten Umfeld etwa kommunizieren bereits heute der Fernseher oder Kühlschrank mit dem Lieferanten – zum Beispiel durch automatisierte Nachbestellungen.

Und selbst eigentlich Harmloses birgt plötzlich Gefahren: Wer hätte je gedacht, dass die Bundesnetzagentur gegen spionagefähiges Kinderspielzeug vorgeht?

Industrie 4.0 erfordert spezifische Sicherheitsstrategien

Umfängliche Schutzmaßnahmen sind also unumgänglich – ob im Internet of Things oder bei der Absicherung vernetzter Industrieanlagen. Patentrezepte gibt es dabei nicht: Cybersicherheit in der Industrie 4.0 kann nur individuell für jedes Unternehmen umgesetzt werden, entsprechend der jeweiligen Anforderungen.

Mit unternehmensspezifischen, bedarfsgerechten Sicherheitskonzepten, die zudem bewährte Industriestandards wie etwa die Normenreihe IEC 62443 berücksichtigen, lassen sich auch vernetzte Industrieumgebungen schützen, die bislang aus autarken Steuerungs- und Automatisierungsanlagen bestanden. Dass dies nötig ist, beweisen die immer gezielteren Angriffe mit ausgeklügelter Schadsoftware, die auf bestimmte Anlagen und Steuerungen zugeschnitten ist. Auch infolge der zunehmenden Vernetzung von IT und OT (Operational IT) im Internet der Dinge steigen die Herausforderungen in puncto Cybersicherheit. Dabei stellt bereits heute der Netzübergang zwischen der Office-IT und dem Produktionsnetzwerk ein erhebliches Einfallstor für Cyberkriminelle dar. So können beispielsweise Würmer, Trojaner oder andere unerwünschte Programme von der herkömmlichen Infrastruktur aus in die Produktionsumgebung gelangen und dort den Produktionsprozess erheblich beeinträchtigen. Künftig dürften die immer professionelleren Angriffsmethoden hier für noch mehr Gefährdungspotenziale sorgen.

Unternehmen sollten die Bedeutung von Sicherheitsvorfällen nicht unterschätzen. Selbst kurze Ausfallzeiten im Produktionsumfeld können bereits hohe Schäden verursachen – von zerstörten Anlagen ganz abgesehen. Um solchen Bedrohungen effizient entgegenzuwirken, empfiehlt sich der Einsatz einer gestaffelten Verteidigung (Defense-in-Depth) zur Steigerung der Robustheit. Die Basis hierfür liefert das sogenannte Zonenmodell das schutzbedürftige Güter (Assets) entsprechend ihrer Kritikalität in verschiedene Sicherheitszonen unterteilt. Die zonenübergreifende Kommunikation erfolgt dabei ausschließlich über definierte, sichere und geschützte Kanäle. Informationen können dabei je nach Zone uni- oder bidirektional ausgetauscht werden. Auf Basis der mittels des Zonenmodells gewonnenen Ergebnisse können weitere Sicherheitsmaßnahmen und -prozesse (zum Beispiel Schwachstellenmanagement) definiert und umgesetzt werden.

Entwicklung effizienter Sicherheitskonzepte

Die KPMG unterstützt Unternehmen bei der Entwicklung ihrer Sicherheitskonzepte ganzheitlich von der Konzeption bis hin zur Implementierung. Dabei werden sowohl die erforderlichen organisatorischen als auch die prozessualen und technischen Aspekte berücksichtigt.

Die Cybersicherheits-Dienstleistungen sind integraler Bestandteil der Industrie-4.0-Expertise von KPMG. So führen die Berater zum Beispiel Potenzialbestimmungen und Benchmark-Vergleiche durch oder unterstützen bei der Identifizierung und Bewertung von Anwendungsfällen oder neuen Geschäftsmodellen. Aufgrund eines multidisziplinären Ansatzes kann KPMG sowohl bei technologischen und steuerlichen als auch bei Compliance-, Cybersicherheits- sowie bei rechtlichen Fragestellungen unterstützen.

Auch stellt KPMG mit „Atlas“ (https://atlas.kpmg.de) Unternehmen eine digitale Beratungsplattform zur Verfügung. Atlas bietet strukturiertes Expertenwissen: Business Assessments zu unterschiedlichsten Themen, Trendanalysen, ein ständig aktualisiertes Benchmarking, Know-how-Vermittlung und (online-buchbare) Workshop-Formate.

Messestand: Halle 9, Stand 9-647

Vorträge von KPMG auf der it-sa

Dienstag, 9. Oktober 2018, 15:00 Uhr, Forum M9 - Management
Wieder eine neue Pflichtübung? – Nicht Bestandene Security Prüfungen als Showstopper im Vergabeprozess
Referent: Wolf von Waldthausen, Cyber Security, KPMG AG Wirtschaftsprüfungsgesellschaft

Mittwoch, 10. Oktober 2018, 9:30 Uhr, Congress@it-sa, NCC Mitte, Raum Mailand
CISO der Zukunft - zwischen steigenden Risiken, Fachkräftemangel und künstlicher Intelligenz
Referent: Dr. Michael Falk, Cyber Security, KPMG AG Wirtschaftsprüfungsgesellschaft

Donnerstag, 11. Oktober 2018, 13:15 Uhr, Technik Forum, Halle 9
Sind Ihre Industrieanlagen sicher?
Referent: Thomas Gronenwald, Cyber Security, KPMG AG Wirtschaftsprüfungsgesellschaft

Anwenderbericht

Druckhaus Mundschenk investiert in webbasierte Zeitwirtschaft

Druckerzeugnisse erzielen auch im Zeitalter der Digitalisierung weiterhin große Nachfrage. So liefert die Mundschenk Nachrichtengesellschaft mbH & Co. KG seit mehr als 150 Jahren erfolgreich Druckerzeugnisse wie Zeitungen, Werbeträger und Organisationsmittel. Bei der internen Personalorganisation hat das Unternehmen jedoch unlängst einen bedeutenden Wandel vollzogen: Mit der Einführung eines neuen, webbasierten Zeiterfassungssystems von Interflex gelang es, interne Prozesse rund um das Personalmanagement deutlich effizienter zu gestalten – für die Personalabteilung und auch für die Mitarbeiter selbst.

Mundschenk setzte bereits seit einigen Jahren eine maßgeschneiderte Zeitwirtschaftslösung ein. Das System stammte – wie auch die neue Lösung – von Interflex und arbeitete stets zuverlässig. Im Lauf der Jahre hatten sich jedoch große Datenmengen angesammelt, die sich aus den verschiedenen Arbeitszeit- und Schichtmodellen von rund 130 Mitarbeitern aus Produktion und Verwaltung zusammensetzten. Durch die Weiterentwicklung des Unternehmens ergaben sich auch neue Anforderungen an die Zeiterfassung. Eine wesentliche Herausforderung bestand darin, die Arbeitszeit gemäß dem entsprechenden Arbeitszeitmodell auf bestimmte Zuschlagskonten zu buchen, sodass sich Arbeitsverträge, Tarifvereinbarungen sowie Nacht- und Sonntagszuschläge korrekt und ohne manuelle Eingabe zuweisen ließen. Mit diesen Prozessen ergab sich ein zunehmend hoher administrativer Aufwand für die Personalabteilung, sodass Mundschenk entschied, in ein Zeitwirtschaftssystem der neuen Generation zu investieren.

Interflex bleibt die erste Wahl

Aufgrund der guten Zusammenarbeit mit Interflex in den letzten Jahren tauschte sich Mundschenk mit den zuständigen Beratern erneut zu den aktuellen und künftigen Anforderungen sowie den verschiedenen Lösungsmöglichkeiten aus. Nach intensiven Gesprächen und Analysen fiel die Wahl auf die neueste Version der IF-6020 und die Einführung des Moduls WebClient. Mundschenk entschied sich für das System, da es bereits ausgereift, erprobt und verlässlich ist. Neu daran ist unter anderem die Integration des Employee-Self-Service, der Selbstverwaltung durch die eigenen Mitarbeiter. Diese sollten vom Erneuerungsprozess ebenso profitieren und aktiv in die Organisation ihrer Zeitdaten eingebunden werden. So stellt das neue System unter anderem elektronische Antragsverfahren zur Verfügung, mit denen Mitarbeiter Genehmigungsprozesse rund um ihre Arbeitszeit- und Urlaubskonten deutlich vereinfachen und beschleunigen können.

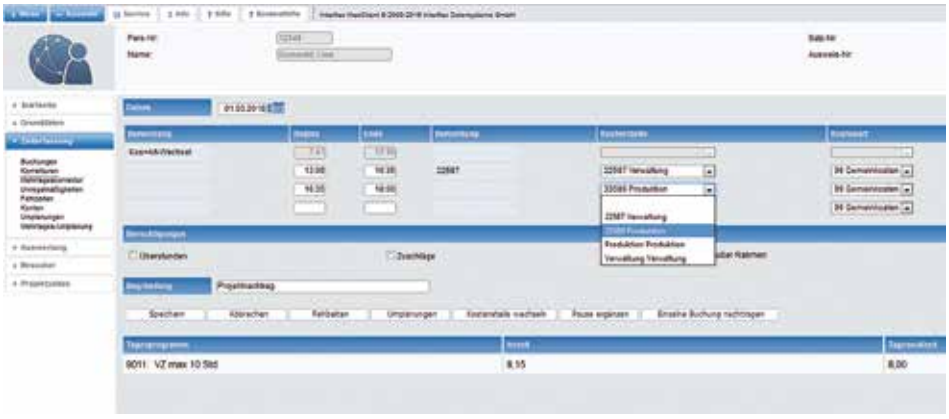
eVAYO – Moderne Terminals für die Zeiterfassung

Bisher waren bei Mundschenk Infrarot-Terminals für die Zeiterfassung installiert, die jedoch zwischenzeitlich das Ende ihres Lebenszyklus erreicht hatten. Um künftig Zeitdaten zu erfassen, wurden moderne Hardwaregeräte der Interflex-Serie eVAYO vor Ort von erfahrenen Beratern implementiert und in Betrieb genommen. Als Nachfolger empfahl sich die ID-Technologie. Ausgestattet mit den neuesten Mifare-Desfire-Leseverfahren identifizieren die Geräte gängige RFID-Leseausweise. Damit werden Zeitdaten durch das Buchen am Zeiterfassungsterminal automatisch und in Echtzeit an die Software übermittelt, dort abgebildet und auf entsprechende Konten gebucht. Abhängig vom hinterlegten Zeitprofil lassen sich Zulagen oder Tarife dabei automatisch zuweisen. Die umfassenden Daten werden über Schnittstellen an das Gehaltssystem übertragen und sorgen für eine leistungsgerechte und pünktliche Vergütung der Mitarbeiter. Neben der lückenlosen Abbildung diverser Informationen zu Arbeitsverträgen, Schichtmodellen oder Tarifvereinbarungen wurde zudem der Administrationsaufwand reduziert. Künftig können Nachtzuschläge, Antrittsgebühren oder Sonntagszuschläge ohne manuelle Eingabe zugewiesen werden.

Kosteneffizient auf dem neuesten technologischen Stand

Durch die Implementierung der neuesten Version der IF-6020 war

es möglich, bestehende Systeme von Mundschenk weiterhin zu nutzen und zu übernehmen. So wurden etwa die vorhandenen Arbeitszeitmodelle übertragen. Neue Softwaremodule, wie WebClient, Workflow, Genehmigungsprozess für Urlaubsanträge oder Korrekturen, kamen hinzu. Der modulare Aufbau ermöglicht, dass sich das System kostenschonend um zusätzliche Module erweitern lässt. Mit dem Employee-Self-Service stellen die Mitarbeiter elektronisch ihre Urlaubsanträge. Dieses Verfahren erleichtert und beschleunigt den Genehmigungsprozess um ein Vielfaches, da mithilfe hinterlegter Workflows die Anträge automatisch den Vorgesetzten vorgelegt werden. Die Mitarbeiter freuen sich über das deutlich vereinfachte Antragsverfahren. Darüber hinaus funktioniert die automatische Zuweisung der Zeitzuschläge einwandfrei. Anstelle der manuellen Bearbeitung rund um das Zeitmanagement können sich die Teams von Mundschenk künftig sinnvolleren Tätigkeiten widmen.



Zeitmanagement mit dem System IF-6020 von Interflex: mehr Transparenz – weniger Administrationsaufwand

Insgesamt bietet das System IF-6020 von Interflex dem Druckhaus Mundschenk entscheidende neue Funktionen, die den Administrationsaufwand um ein Vielfaches verringern und unternehmensweit für mehr Transparenz sorgen:

— Arbeitszeitkonten verwalten
— detaillierte Informationen einsehen (Zeitkonten, Urlaubsstände, Entgeltbelege, Beurteilungen)
— Anträge und Genehmigungen papierlos stellen und bearbeiten (Gleitzeit, Urlaub, Dienstreisen etc.)
— Korrekturen in Zeitdaten und falschen Buchungen vornehmen
— Stundenkontierungen überblicken (Projekte, Kostenstellen etc.)
— Arbeitszeitsalden und Einsatzpläne abfragen
— geplante Arbeitszeiten mit geeigneten Mitarbeitern tauschen

Im Trend: Investitionen in HR-Systeme

Einen Großteil der Aufgaben in Personalabteilungen nehmen administrative und stets wiederkehrende Tätigkeiten ein. Das betrifft etwa die Aktualisierung von Personaldaten, die Genehmigung von Urlaubsanträgen oder auch Korrekturen von Falschbuchungen der Mitarbeiter. Oft verlaufen diese Prozesse auch heute noch formlos und werden mithilfe von Papieranträgen bearbeitet. Daraus resultieren eine stark überlastete Personalabteilung sowie ineffiziente und teilweise redundante Abläufe. Laut der Studie „Innovatives Personalmanagement“ des Marktanalyse- und Beratungsunternehmens PAC sehen deutsche Unternehmen einen konkreten Handlungsbedarf, die Effizienz ihrer HR-Prozesse zu steigern. Dabei geht es vor allem darum, Datenanalysen zu verbessern, die Benutzerführung zu erleichtern sowie die für die HR-Abteilung erforderlichen Daten und Workflows bereitzustellen. Knapp 40 Prozent sind bereit, in HR-Software zu investieren, um fehlende Funktionen zu ergänzen. Für etwa 90 Prozent sind Effizienzsteigerung und Kostenreduktion die wichtigsten Aspekte für den Softwarekauf, gefolgt vom Wunsch, HR-Anwendungen zu modernisieren (86 Prozent) sowie die Transformation des Personalmanagements als Unternehmensstrategie zu forcieren (63 Prozent). [1] Doch in welche konkreten Lösungen investieren Betriebe, um ihre Personalprozesse zu verbessern? An der Spitze der am häufigsten verwendeten HR-Software stehen Programme für Arbeitszeitmanagement und Zeit- sowie Zutrittserfassung, so der HR-Software-Report 2016. Im Vergleich zum Vorjahr ist die Nutzung in diesem Bereich nochmals um zwei Prozent gestiegen. Eine größere Veränderung zeigt sich beim Thema Self-Service. Setzten 2015 nur 29 Prozent eine professionelle Software dafür ein, waren es 2016 schon 54 Prozent. [2] Personalabteilungen optimieren ihre Abläufe, indem sie die Mitarbeiter aktiv in die Personalwirtschaft sowie Planungs- und Erfassungsprozesse einbinden – etwa zur Regelung von Arbeitszeiten. Produkte wie das Zeiterfassungssystem IF-6020 von Interflex erlauben die aktive Selbstverwaltung durch die Mitarbeiter. Somit lassen sich Vorgänge über die reine Zuständigkeit der Personalabteilungen hinaus deutlich beschleunigen, vereinfachen und für alle Beteiligten transparenter gestalten.

Literatur
[1] Studie „Innovatives Personalmanagement“, PAC, März-April 2016, www.pac-online.com/pac-studie-zum-personalmanagement-herausforderungen-sorgen-f-r-modernisierungsdruck-bei-hr-software
[2] Studie „HR-Software-Report 2016“, Magazin personal manager mit Unterstützung der Netzwerkportale HRM.at, HRM.de und HRM.ch

Governance, Risk and Compliance

BSI IT-Grundschutz und EU-DSGVO mit DocSetMinder umsetzen

Positive Erfahrungen aus einer Vielzahl von Migrationsprojekten und lobendes Feedback von Sicherheitsexperten diverser Organisationen bescheinigen eine praxisnahe und intelligente Abbildung des modernisierten IT-Grundschutzes und der EU-DSGVO mit DocSetMinder. Die Benutzerführung bei der Umsetzung der Standards, der Funktionsumfang und die Bedienbarkeit von DocSetMinder sind nur einige wichtige Vorteile. Unser Beitrag skizziert einzelne Implementierungsaspekte eines Managementsystems für Informationssicherheit (ISMS).

Von Krzysztof Paschke, GRC Partner GmbH

Die hohe Akzeptanz von DocSetMinder ist vor allem der sehr guten Umsetzung der BSI-Standards 200-2/-3, der Option eines Parallelbetriebes für den Übergang der BSI-Standards 100-2/-3 zu 200-2/-3 sowie seinem an die oftmals überschaubaren Ressourcen von Organisationen angepassten Lizenzmodell zuzuschreiben. Einen wesentlichen Beitrag zur Entwicklung der Software haben, neben dem Berater- und Softwareentwicklungsteam der GRC Partner GmbH, mehrere zertifizierte IT-Grundschutz-Experten aus diversen Organisationen geleistet. DocSetMinder setzt mit dem Modul „IT-Grundschutz" konsequent alle Anforderungen und die Methodik des modernisierten IT-Grundschutzes um. Durchdachte Softwarefunktionen unterstützen die Anwender aktiv in jeder Phase des Sicherheitsprozesses, von der Planung über die Umsetzung und Dokumentation, bis hin zum Audit. Der folgende Beitrag skizziert einige wichtige Aspekte der Umsetzung in einem ISMS-Projekt.

Strukturanalyse – Fundament eines Sicherheitskonzeptes

Die Dokumentation der Geschäftsprozesse einer Organisation und Identifizierung der zugehörigen Informationen liefern die Grundinformationen für die Umsetzung des BSI-Standards 200-2, 200-3, 100-4 und des Datenschutzes nach EU-DSGVO. Für eine effiziente Durchführung der Strukturanalyse stehen im DocSetMinder zwei Module zur Verfügung: „Organisation" und „IT-Dokumentation". Das Modul „Organisation" bietet die notwendigen Strukturen und Dokumentklassen für die Dokumentation der Organisation im erforderlichen Detaillierungsgrad. Erfasst werden können sämtliche Organisationseinheiten, Geschäftsprozesse und die Verantwortlichkeiten (Rollen) in der Organisation. Für die Dokumentation der IT-Prozesse steht die ITIL-V.3-Struktur zur Verfügung. Die Organigramme und die Prozesslandschaft können mit dem integrierten DocSetMinder-Flowchart-Editor grafisch nach ISO- und BPMN-Standards abgebildet werden. Das Modul enthält ein sehr effizientes Richtlinienmanagement, zur Verwaltung aller notwendigen Leit- und Richtlinien (EU-DSGVO, ISMS, QM etc.). Für eine effektive Einbindung der externen Dienstleister und deren Aufgaben steht ein leistungsfähiges Vertragsmanagement für die Erfassung der Dienstleistungs- und Datenschutzverträge (SLAs und ADVs) zur Verfügung. Das Modul „IT-Dokumentation" unterstützt die Anwender bei der systematischen Dokumentation der IT-Infrastruktur: Netzwerkkomponenten, Kommunikationsverbindungen, Server-Systeme, Arbeitsplätze, Peripheriegeräte, Dienste und Anwendungen sowie Standorte, Gebäude, Gebäudesicherheit und Räume. Die Dokumentation stellt alle logischen Zusammenhänge zwischen Geschäftsprozessen, Anwendungen, Serversystemen inklusive Cloud-Landschaft, sowie den Speicherorten für die entstehenden Informationen (Daten) dar. Die beiden Module „Organisation" und „IT-Dokumentation" stellen das Fundament eines jeden Sicherheitskonzeptes dar.

Modellierung

DocSetMinder bildet das Schichtenmodell des IT-Grundschutz-Kompendiums, für die Modellierung der prozess- und systemorientierten Bausteine, detailliert ab. Für die Übergangsphase vom BSI 100-2/-3 zu 200-2/-3 können beide Schichtenmodelle angezeigt werden. Das Schichtenmodell kann individuell erweitert werden. Während der Modellierung der einzelnen Schichten und Zielobjekte werden

die entsprechenden Bausteine automatisch vom DocSetMinder vorgeschlagen. Bausteine, die bereits bei Zielobjekten gleicher Art verwendet wurden, können optional mit den Inhalten übernommen werden. In Abhängigkeit vom gewählten Sicherheitsniveau (Basis-, Standard-Anforderung und Anforderungen für erhöhten Schutzbedarf) werden bei den modellierten Bausteinen nur die Sicherheitsanforderungen und Umsetzungshinweise angezeigt, die zu der ausgewählten Kategorie, gemäß dem BSI IT-Grundschutz-Kompendium, gehören. Bei einem Wechsel auf eine höhere Kategorie der Absicherung werden die Sicherheitsanforderungen automatisch erweitert angezeigt.

Risikoanalyse

Die Identifikation der Risiken erfolgt unter Einbeziehung des BSI G0-Kataloges des IT-Grundschutz-Kompendiums. Bei der Zuordnung der elementaren Gefährdungen werden die BSI-Kreuzreferenztabellen genutzt. DocSetMinder erkennt den Typ der jeweiligen Zielobjekte mit den bereits modellierten Bausteinen und schlägt die dazu gehörigen Gefährdungen vor. Die Risikobewertung definiert sich als Produkt von Eintrittswahrscheinlichkeit und Auswirkung (Schadenshöhe) und wird mithilfe einer 4x4-dimensionierten Matrix durchgeführt. Die Dimension der Matrix kann individuell angepasst werden. Bei der Betrachtung der Grundwerte können drei Optionen gewählt werden: BSI-Standard (Vertraulichkeit, Integrität und Verfügbarkeit). Zusätzlich stehen Authentizität und das Standard-Datenschutzmodell (SDM der Datenschutzbehörden des Bundes und der Länder) zur Auswahl. Mit einer gut geplanten Risikoanalyse können EU-DSGVO, ISMS, Notfallmanagement und weitere Normen in der Organisation gleichzeitig effektiv und effizient behandelt werden. Ähnliches gilt auch für eine Reihe von technisch-organisatorischen Maßnahmen, die gleichermaßen für EU-DSGVO und ISMS gelten können.

Klassifikation von Informationen

Ein angemessener Schutz der Informationen beginnt mit ihrer Kennzeichnung. Dafür stehen im DocSetMinder® optional drei unterschiedliche Methoden zur Verfügung: Klassifikationsschema gemäß dem staatlichen Geheimschutz (VS), Traffic Light Protocol (TLP) und Basisklassifikation (öffentlich, interner Gebrauch, vertraulich). Bei der Erstellung der Informationen wird im Hintergrund protokolliert, wer der Ersteller, Prüfer und Genehmiger ist. Über die Systemberechtigung wird bestimmt, wer die Informationen nutzen darf. Bei der Ausgabe des Sicherheitskonzeptes, zum Beispiel in Microsoft Word, wird die Dokumentation automatisch mit einem Wasserzeichen, gemäß der ausgewählten Kennzeichnungsstufe, deutlich sichtbar markiert.

GSTOOL und die Datenübernahme

Die Praxis zeigt, dass eine vollständige Datenübernahme aus dem GSTOOL nicht möglich ist. Der wesentliche Grund dafür sind die Unterschiede zwischen den BSI-Standards 100-2/-3 und 200-2/-3. Es besteht zwar die Möglichkeit einer teilweisen Datenübernahme, ihre zukünftige Verwendbarkeit ist aber mehr als fraglich. Die „Anleitung zur Migration von Sicherheitskonzepten“ und die Migrationstabellen des BSI sind zwar wichtige Hilfsmittel, entpflichten allerdings nicht vom konzeptionellen Aufwand. Erfahrungsgemäß ist es sinnvoll zu bewerten, inwieweit eine Neuerfassung der Zielobjekte und ihre Modellierung effizienter ist als die Datenübernahme und die nachträgliche manuelle Nachbereitung. Leider wird die vollständige Datenübernahme aus dem GSTOOL in vielen Ausschreibungen als K.-o.-Kriterium genannt und führt zur Wettbewerbsverzerrung.

Reporting

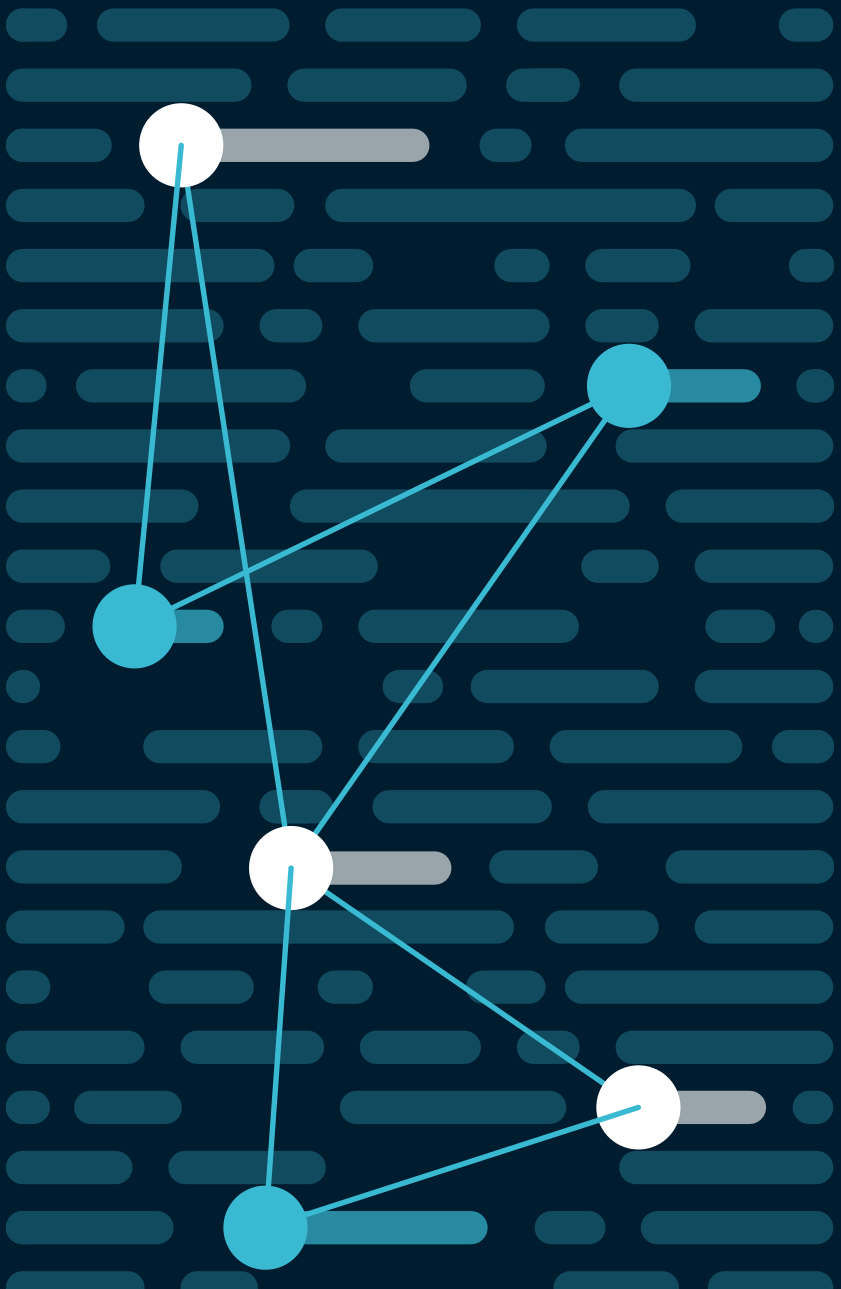
Für die Auswertung des Sicherheitskonzeptes steht den Anwendern eine sehr leistungsfähige Reporting-Funktion zur Verfügung. Neben den erforderlichen Reports A0-A6 kann der Anwender selbstständig und ohne Wirkung des Herstellers weitere Reports erstellen oder die Bestehenden anpassen. Dafür sind keine besonderen SQL oder sonstige technische Kenntnisse erforderlich. Die Reporting-Funktion ist benutzerfreundlich und verfügt über einen Report-Layout-Generator. Beliebige Werte können „verdichtet“ und in Form von Grafiken (Torte, Balken etc.) angezeigt werden.

Fazit

DocSetMinder bildet die Normen und Standards von Informationssicherheit und Datenschutz vollständig ab. Der Funktionsumfang von DocSetMinder macht den Einsatz weiterer Tools oder Office-Anwendungen für die Dokumentation und Zertifizierung der umgesetzten Normen und Standards überflüssig. Die Lösung ist einfach zu implementieren und intuitiv bedienbar. Die gemeinsame Nutzung der erfassten Informationen bietet allen beteiligten Mitarbeitern und Verantwortlichen einen enormen Mehrwert durch die Aktualität der Dokumentation und eine signifikante Zeitersparnis bei der Vorbereitung interner und externer Audits. DocSetMinder ist Best Practice – und Sie sind jederzeit „Ready for Audit“. ■

ENDPOINT PROTECTOR

Next Generation DLP



EndpointProtector.de

it sa 2018

Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Treffen Sie uns in

Halle 10.0 am Stand #109

Zertifikate-Management in virtualisierten Docker-Umgebungen

Docker-Images benötigen für ihre Betriebsfähigkeit Geheimnisse wie Kennwörter und Schlüsselmaterial. Der Artikel zeigt Möglichkeiten auf, wie der sichere und effiziente Umgang mit Schlüsseln in Containerplattformen gelingt.

Von Werner Zügel, essendi it GmbH

Anwendungskomponenten in Docker-Images müssen notwendige Vorkehrungen für die IT-Sicherheit, Authentifizierung und Autorisierung mitbringen, beispielsweise Signaturzertifikate für Webservices oder Dokumente, Private-Keys, Datenbank-Kennwörter und andere Geheimnisse. Der Umgang mit sicherheitsrelevanten Artefakten wie Schlüsselpaaren stellt dabei eine spezielle Herausforderung dar. Deswegen werden die Entwicklungsstufen voneinander getrennt und für jede Umgebung ein eigenes Docker-Image für eine jeweils eigene Test-Umgebung angelegt. Insofern sind in jedem Stage wieder andere, passende Zertifikate, Schlüssel oder Kennwörter notwendig, die verwaltet werden müssen. Zudem ist die Speicherung von Sicherheitsartefakten direkt in den Docker-Images kein sicherer Ablageplatz.

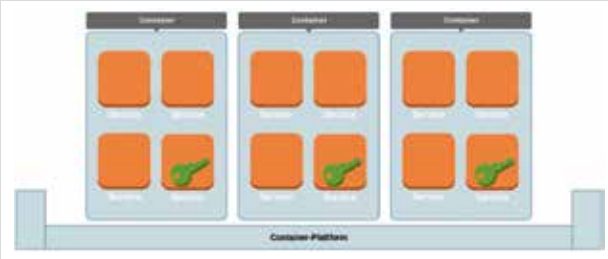
Hier entsteht zudem ein nicht unerheblicher administrativer und logistischer Aufwand. Für agile Softwareprozesse sind daher intelligente Lösungen mit hohem Automationsgrad bei gleichzeitig hohen Sicherheitsanforderungen erforderlich. Abhilfe schafft hier ein Bundle, bestehend aus einer Docker-Plattform, dem „essendi xc“-Zertifikatemanager in Kombination mit Hardware-Security-Modulen (HSM).

Management von Zertifikaten mit essendi xc

Mit essendi xc wird das Management von Zertifikaten wesentlich vereinfacht und automatisiert. DevOps-Teams sollen alle Aufgaben – auch administrative Dinge wie die Anforderung von Zertifikaten – innerhalb des Lösungsteams erledigen können. Dabei unterstützt essendi xc diese agilen Teams: Durch die Self-Service-Funktion von essendi xc wird der Bediener mittels vorkonfigurierter Zertifikatsprofile und dem Rollen- und Rechtekonzept vom System geführt. Gleichzeitig wird gewährleistet, dass die Regeln und Konventionen des Unternehmens, wie beispielsweise die Belegung von CN-Namen oder Schlüsselalgorithmen, eingehalten werden.

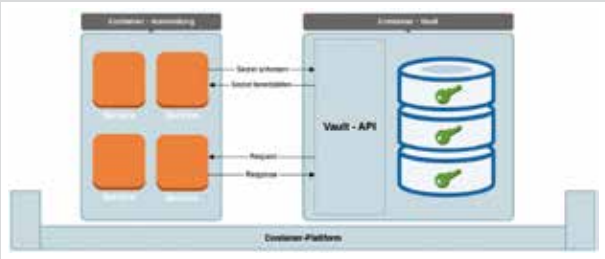
Die Key-Generierung, Anforderung und Beglaubigung bis hin zum Enrolment von Zertifikaten durch interne oder öffentliche Zertifizierungsstellen wird damit weitgehend automatisiert und standardisiert. Über Interfaces können die Vault-Stores der Containerplattformen an den „essendi xc“-Zertifikatemanager direkt angebunden werden. Damit wird bereits ein hoher Grad an Standardisierung

Geheimnisse und Schlüsselmaterial für Container im Überblick



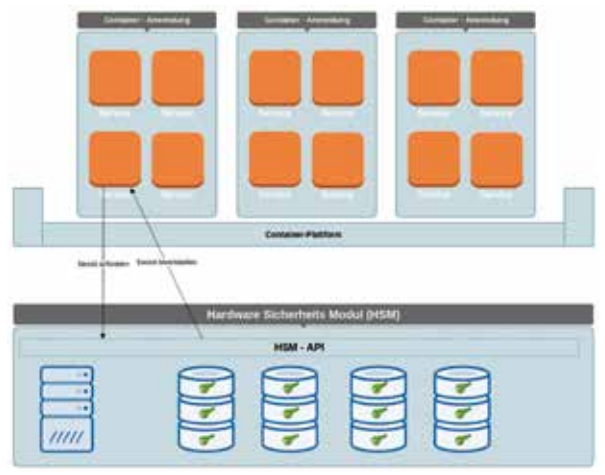
Stufe 0 – Schlüsselmaterial im Container

- Geheimnisse sind Bestandteil der Docker-Images
- Bestandteile des Quellcodes oder in Java-Keystores
- Schlüsselmaterial incl. Private Keys einfach zugänglich
- Transport / Deployment der Schlüssel über unsichere Kanäle
- Images sind über die Entwicklungsstufen hinweg nicht gleich



Stufe 1 – Schlüsselmaterial im Vault der Plattform

- Geheimnisse liegen in sicherem Vault-Speicher der Containerplattform
- geregelter, sicherer Zugang zum Vault über Multifaktor-Authentifikation
- stufenweises Autorisierungskonzept
- Transport der Schlüssel über unsichere Kanäle
- Images sind über die Entwicklungsstufen hinweg identisch



Stufe 2 – Schlüsselmaterial im HSM

- Geheimnisse liegen ausgelagert in sicherem Hardware-Speicher
- performante und umfangreiche Krypto-Algorithmen
- geregelter, sicherer Zugang zum HSM über Multifaktor-Authentifikation
- Mandanten- oder anwendungsbezogene Segmentierung der Speicherorte im HSM
- Autorisierungskonzept passend zur Segmentierung des HSM
- kein Transport der Schlüssel über unsichere Kanäle
- Schlüssel werden im HSM erzeugt, private Schlüssel und andere Geheimnisse müssen das HSM nicht verlassen, da z. B. die Signatur von Webservice-Nachrichten direkt im HSM erfolgt
- Images sind über die Entwicklungsstufen hinweg identisch

und Vereinfachung der Prozesse des Zertifikatsmanagements im Zusammenspiel mit Docker-Plattformen erreicht. essendi xc kann zudem über das JCA-Interface ein HSM direkt ansprechen und Schlüsselmaterial darin erzeugen beziehungsweise ablegen.

Management sensibler Daten in HSMs

Die beste Variante zur Verwaltung von Geheimnissen ist der Einsatz von HSMs. Denn eine solche Infrastruktur ist sicherer als ein bloßer Schutzmechanismus über die Software, da sie schwerer angreifbar ist. Eine gute Integration mit der Verwaltungsapplikation essendi xc ist mit HSM-Geräten der Firma Securosys gegeben. Mit essendi xc werden Zertifikate auf sehr einfache Art und Weise, teilweise hoch automatisiert, angefordert und direkt im HSM hinterlegt. Die Schlüssel werden dort erzeugt und verlassen das HSM niemals. HSMs liefern eine umfangreiche und breite Palette an leistungsfähigen Verschlüsselungsalgorithmen und Funktionen für Krypto-Infrastrukturen. ■

Messestand: Halle 10.0, Stand 10.0-520

Vorträge von essendi it auf der it-sa

Dienstag, 09.10., 14:45 bis 15:00 Uhr, Technik Forum (Forum Blau)
Sicheres Zertifikatsmanagement in Docker-Betriebsumgebungen

Donnerstag, 11.10. von 13.15 bis 13.30 Uhr, Management Forum (Forum Rot)
360° Zertifikatsmanagement
(Gemeinschaftsvortrag mit Partner SwissSign)

Sick of ancient permissions?

Quest
Access Management

- Transparente Berechtigungsverwaltung für Fileserver, SharePoint und Drittsysteme
- Monitoring & Autokorrektur nicht autorisierter Veränderungen
- Auditsichere Protokollierung der Berechtigungsvergabe
- Self Service für Fachabteilungen ohne IT-Hintergrundwissen
- Vergabe von individuellen On-demand- und Profilberechtigungen
- Intuitiver Prozess zur Rezertifizierung
- User Provisioning für Administratoren
- Entlastung im User Help Desk

Hint: IT-SA 2018
Halle 10.0 / Stand 412

Zugriffsrechte beim Burgherren beantragen - einfach und schnell!

FILESERVER MANAGEMENT SUITE

Die zuverlässige Lösung für automatisiertes Berechtigungsmanagement

www.fileservermanagementsuite.com

Telefon: +49 (6151) 86 18 - 0
E-Mail: fms@bayoo.net

BAYOONET AKTIENGESELLSCHAFT

SecuPedia

Das Portal für Sicherheits-Informationen

Umfassendes und redaktionell geprüftes Sicherheits-Wissen und aktuelle Sicherheitsinformationen von und für Sicherheits- und IT-Sicherheitsverantwortliche.

Diese Verbände und Unternehmen ermöglichen als Sponsoren die Sicherheitsplattform:

ZVEI: Die Elektroindustrie · ASW Bundesverband · VdS · BDSW · BDGW · BHE · security essen · it sa · VSW · ASW Norddeutschland

dormakaba · GEUTEBRÜCK · tenable · NTT Security · ESSER by Honeywell · SALTO inspired access · WISAG

Neue IT-Sicherheitsstrategien

Von außen und von innen schützen

IT-Infrastrukturen bieten immer mehr Angriffsflächen, die durch klassische Firewalls nicht mehr geschützt werden können. Vor allem für „Internet of Things"-Anwendungen und hochsichere Schutzbereiche brauchen Unternehmen neue IT-Sicherheitsstrategien. Die Trennung der Netze und Security by Design sind dafür die entscheidenden Ansätze.

Von Thomas Günther, INFODAS GmbH

Spätestens seit den Enthüllungen von Edward Snowden ist bekannt, dass sich auch Hardware-Systeme im Inneren einer IT-Infrastruktur unbemerkt manipulieren lassen. Das gleiche gilt für Angriffe auf Elemente im Internet of Things (IoT). Unternehmen brauchen daher völlig neue Sicherheitsstrategien, um solche Angriffe abzuwehren. Verbindet man einen solchen Schutz „von innen" mit neuen Strategien für den äußeren Schutz, entstehen wirksame Sicherheitsmechanismen.

Netz physisch trennen

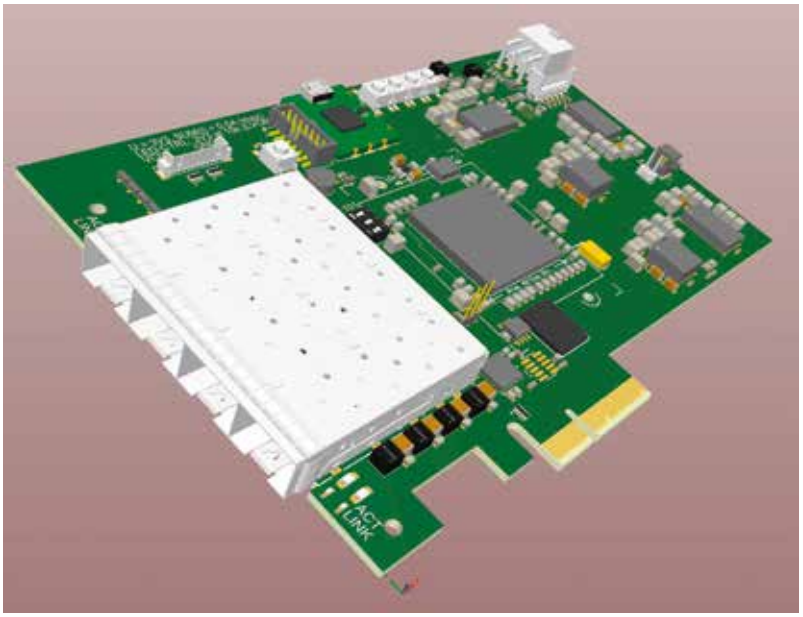
So unterliegen zum Beispiel sensible militärische Informationen ganz besonderen Sicherheitsvorgaben: Sie müssen in einem eigens dafür eingerichteten Netz verarbeitet werden. Dieses sogenannte rote Netz wird vom weniger sensiblen schwarzen Netz streng getrennt. Eine solche Netztrennung nutzen mittlerweile auch immer mehr Großkonzerne, mittelständische Technologieunternehmen sowie Betreiber kritischer Infrastrukturen. Denn auch Baupläne von Prototypen, brisante Strategiepapiere und Steuerungsprogramme von Kraftwerken müssen genau wie militärische Geheiminformationen geschützt werden. Das ist insgesamt eine Frage der unternehmerischen Existenz und im Fall von kritischen Infrastrukturen auch eine Frage des Schutzes der Gesellschaft.

Zusätzliche Sicherheit sollte aber nicht die Effizienz der unternehmensinternen Prozesse verringern. Das war jedoch lange der Fall, da eine Trennung der Netze zum Beispiel die Kommunikation erheblich erschwert. Bisher gab es nur einen Weg, um Informationen aus geheimen Netzen in niedriger eingestuften Netzen verfügbar zu machen: Die manuelle Prüfung via „Drehstuhlschnittstelle" unter Einsatz von USB-Sticks oder CDs – ein langsames, personalintensives und vor allem fehleranfälliges Vorgehen.

Große Datenmengen schnell übertragen

Die Lösung des Problems sind spezielle Torwächter-Systeme, die erkennen, ob eine Information zwar aus einem geheim eingestuften Netz stammt, selbst jedoch nicht vertraulich ist. Mit herkömmlichen Firewalls ist eine solche Differenzierung der Inhalte nicht möglich. Hingegen prüfen speziell entwickelte Sicherheits-Gateways den Inhalt der Dateien vor der Weitergabe genau. Befinden sich in einer Datei geheime oder besonders schützenswerte Informationen, darf sie nicht den Torwächter des höher eingestuften Netzes passieren.

Aber woher weiß das Gateway, ob eine Information geheim ist oder nicht? Strukturierte Daten – beispielsweise XML-Dateien, aber auch viele militärische Datenformate – lassen sich mittels eines Regelwerkes filtern. Um ein solches



Die Funktionalität einer sicheren Netzwerkkarte wird komplett in nicht-manipulierbarer Hardware umgesetzt.

zu definieren, muss im Vorfeld die Struktur der Information bekannt sein. Das Gateway prüft anhand des Regelwerks, ob die Information durch darf oder nicht. Das SDoT Security Gateway der INFODAS GmbH ist ein solcher Torwächter. Es hat die Zulassung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für die Nutzung bis GEHEIM erhalten. Damit ist es für den Einsatz im Hochsicherheitsbereich zugelassen und erfüllt den höchstmöglichen Sicherheitsstandard.

IoT mit "Security by Design"

Des Weiteren stellt die zunehmende Vernetzung von Geräten im Zuge des „Internet of Things" (IoT) Unternehmen vor eine völlig neue Herausforderung. IoT-Systeme nutzen meist moderne Betriebssysteme, wie sie auf Servern, Arbeitsplatzrechnern und Smartphones verbreitet sind. Das Problem: Diese Betriebssysteme basieren auf Millionen von Codezeilen. Fehler und Sicherheitslücken sind deshalb praktisch nicht vermeidbar. Ein weiteres Kernproblem der Betriebssysteme ist die monolithische Struktur: Der wesentliche und größte Teil des Betriebssystems versteht sich als eine Einheit und verfügt über umfangreiche Zugriffsrechte auf Prozessor, Arbeitsspeicher und Peripherie. Wird eine Teilkomponente gehackt, ist meist das gesamte Betriebssystem kompromittiert. Monolithische Betriebssysteme sind daher prinzipiell unsicher.

Auch in diesem Fall sind Firewalls machtlos. Die Gefahr muss stattdessen im Inneren der Systeme beseitigt werden. Möglich ist das mithilfe von „Security by Design"-Ansätzen. Bei diesem Vorgehen berücksichtigen Entwickler die Sicherheitsanforderungen bereits während der Konzeption der IT-Systeme. Das Ergebnis sind Produkte, denen die Sicherheit nicht im Nachhinein „übergestülpt" werden muss, sondern die stattdessen bereits über eine eigene sichere Architektur verfügen.

Kleiner Kern schafft Sicherheit

Ein sicheres Betriebssystem verfügt über einen Mikrokern, in dem nur unbedingt notwendige Funktionen im sogenannten privilegierten Modus laufen. Diese Funktionen erhalten damit Vollzugriff auf alle Hardware-Komponenten. Alle weiteren Funktionen, die für ein Betriebssystem notwendig sind, erhalten nur eingeschränkte Rechte. Damit lässt sich die problematische monolithische Struktur aufheben.

Ein weiterer Vorteil des Mikro-Kernels: Eine lückenlose und intensive Kontrolle aller Funktionen des Betriebssystems ist möglich. Das ist die Voraussetzung für eine Evaluierung, wie sie für einen Zertifizierungsprozess beispielsweise nach Common Criteria notwendig ist. Die INFODAS GmbH hat für seine SDoT-Produktfamilie ein solches Betriebssystem entwickelt, das auf einem Open-Source-Mikrokern L4 basiert.

Eine ebenfalls neue Herausforderung für Unternehmen stellt der Schutz von Hardwaresystemen dar. Edward Snowden machte erstmals bekannt, dass insbesondere Netzwerkkarten verbreitete Angriffsziele sind. Das Problem: Die Firmware einer Netzwerkkarte kann so verändert werden, dass sie den Hauptspeicher eines Servers ausliest und unbemerkt an einen beliebigen Kontrollrechner verschickt. Auch das Einschalten eines heruntergefahrenen Rechners, die Annahme von interaktiven Kommandos sowie das Injizieren von beliebigem Schadcode ist möglich – und zwar ohne dass die Schutzmechanismen eines Betriebssystems oder ein Administrator etwas dagegen unternehmen könnten.

Lösen lässt sich auch dieses Problem ebenfalls mit Security by Design. Dabei wird auf Prozessoren sowie Firmware verzichtet. Die Funktionalität wird stattdessen komplett in nichtmanipulierbarer Hardware umgesetzt. Dadurch entfallen sämtliche externen sowie internen Angriffsvektoren. Das Design setzt hierbei auf einen speziellen Chip, eine sogenannte Feld-programmierbare Gatter-Anordnung (FPGA). Dieser wird nach der Stromzufuhr über einen unveränderlichen Speicherbaustein (ROM) konfiguriert. Der zur Laufzeit veränderliche Konfigurationsmechanismus des FPGAs hingegen wird durch elektrische Maßnahmen unterbunden.

Die INFODAS GmbH hat eine solche Netzwerkkarte entwickelt, die sogar die hohen Geheim-Anforderungen des BSI erfüllt. Ein erster Prototyp wird auf der diesjährigen it-sa präsentiert. Die Karte kann sowohl innerhalb eines herkömmlichen Arbeitsplatzrechners als auch innerhalb eines Servers verwendet werden. Mit einer sicheren Ablaufplattform und einer kontrollierbaren Netzwerkschnittstelle hat Infodas nicht nur für die eigene SDoT-Produktfamilie Lösungen parat, die gänzlich nach dem „Security by Design"-Ansatz entwickelt wurden.

Fazit

Je größer die Angriffsflächen für Hacker werden, desto wichtiger werden neue IT-Sicherheitskonzepte. Lösungen, die den Geheimschutzanforderungen genügen, können Teil einer solchen Sicherheitsstrategie sein. Entweder weil sie vom Kern her so entwickelt wurden, dass sie nicht angreifbar sind, oder indem eine physische Trennung die Daten vor Angreifern schützt. Mit den richtigen Werkzeugen lassen sich beide Konzepte realisieren, damit Unternehmen ihre Geschäftsmodelle sicher und effizient umsetzen können. ■

Messestand: Halle 9, Stand 9-315

IT-Sicherheit

Schützen Sie Ihr Unternehmen gegen:

Systemausfälle | **Datenverluste** | **Datenmanipulation** | **Sabotage** | **Lizenzverstöße**

Penetrationstest:
Statusaufnahme der Sicherheit Ihrer IT-Infrastruktur

Sie erhalten:

- Eine Einschätzung der Sicherheit Ihrer Unternehmensdaten und Darstellung des Gefahrenpotentials des penetrierten Umfeldes aus der Sicht eines Hackers
- eine Erhöhung der Sensibilität zur Sicherheit Ihrer technischen Systeme und Infrastruktur
- eine Bestätigung der IT-Sicherheit durch einen externen Dritten

Weitere Prüffelder:

- Prüfen der Netzwerkstrukturen
- Lücken im Lizenzmanagement
- Datenbankprüfung
- Betriebssystemprüfung
- Prüfen der Telekommunikation
- Prüfung BCM
- Applikationsprüfung

Beratung

- Unterstützung der IT-Organisation bei
  - der Erstellung oder Bewertung von Richt- und Leitlinien
  - dem Aufbau oder Prüfung eines Informationsmanagementsystems (ISMS)
  - Themen wie Outsourcing und/oder Service-Level Agreements
- Unterstützung des IT-Sicherheitsbeauftragten/ Informationssicherheitsbeauftragten

Besuchen Sie uns auf der it-sa – Fachmesse für IT-Security!
09.10.-11.10.2018, Messezentrum Nürnberg, Halle 9 , Stand 244

IBS Schreiber GmbH • Zirkusweg 1 • 20359 Hamburg
Fon: +49 40 69 69 85-0 • **www.ibs-schreiber.de** • **seminare@ibs-schreiber.de**

Medienpartner
<kes>
Die Zeitschrift für Informations-Sicherheit

IT-Sicherheit für die Produktion

Risikomanagement und Früherkennung mit IRMA

Betreiber kritischer Infrastrukturen (KRITIS) müssen ab einer bestimmten Unternehmensgröße rechtliche Vorgaben erfüllen, beispielsweise zum Stand der Technik. Anhand des KRITIS-Sektors Wasser/Abwasser wird in diesem Artikel aufgezeigt, wie dafür nötige Maßnahmen umsetzbar sind.

Von Dieter Barelmann, VIDEC Data Engineering GmbH

Der Gesetzgeber hat mit dem IT Sicherheitsgesetz bereits im Jahr 2015 den rechtlichen Rahmen zur Erhöhung der IT-Sicherheit für die unterschiedlichen Branchen vorgegeben. Laut der Zeitschrift Wirtschaftswoche plant das Bundesinnenministerium (BMI) im Rahmen des sogenannten IT-Sicherheitsgesetzes 2.0 die Meldepflicht von Unternehmen bei Angriffen auf ihre IT-Infrastruktur Ende 2019 zu verschärfen. Beispielsweise soll die Meldepflicht für erhebliche IT-Sicherheitsvorfälle auf weitere Unternehmen, bis in den Mittelstand hinein, übertragen werden. Diese Pflicht gilt bereits aktuell für Betreiber kritischer Infrastrukturen, wie zum Beispiel im Energie-, Wasser- und Gesundheitssektor.

So wurde am 1. August 2017 der Branchenstandard für die Wasser- und Abwasserwirtschaft als erster IT-Sicherheitsstandard vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für einen KRITIS-Sektor anerkannt. In der Wasser-Abwasser-Branche wurde daraufhin vom Deutschen Verein des Gas- und Wasserfaches (DVGW) und der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DWA) der erste branchenspezifische Sicherheitsstandard (B3S) entwickelt. Allen Betreibern von Anlagen der Trinkwasserver- und Abwasserentsorgung wird empfohlen, diesen Branchenstandard umzusetzen, da die Betreiber jederzeit in der Lage sein müssen, den Nachweis eines sicheren Betriebs zu erbringen.

Denn Betreiber kritischer Infrastrukturen sind nach dem BSI-Gesetz dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten und Prozesse nach Stand der Technik zu treffen und das auch gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durch Prüfungen oder Zertifizierungen aktiv nachzuweisen.

Die Branchenverbände DWA und DVGW stellen dazu allen Betreibern (nicht nur den KRITIS-Unternehmen) von Anlagen der Trinkwasserver- und Abwasserentsorgung den praktischen Handlungsrahmen als Mindeststandard mit dem Merkblatt W 1060/M1060 und dem IT-Sicherheitsleitfaden zur Verfügung.

Branchenstandard

Der branchenspezifische Sicherheitsstandard beschreibt verbindliche Rahmenanforderungen, die eine Vorgehensweise zur Risikoanalyse und -behandlung enthält (siehe Abbildung 2). Der Leitfaden beinhaltet eine Sammlung von Sicherheitsmaßnahmen zur Erreichung des im IT-Sicherheitsgesetz geforderten Stands der Technik für den Betrieb der eingesetzten IT-Systeme. Die darin beschriebenen Mindestvorgaben (A-Maßnahmen) sollten von allen Anlagenbetreibern umgesetzt werden – unabhängig davon, ob eine Anlage bereits heute eine kritische Infrastruktur ist oder nicht.

Das bedeutet wiederum, dass sich nahezu jeder Betreiber um diese Thematik zu kümmern hat. Dabei sind Aussagen wie „Uns betrifft das nicht“ oder „Wir sind nicht im Internet, wir haben eine Insellösung“ in keinem Fall ausreichend, denn es reicht schon eine Fernwartung oder der direkte Zugriff über einen kompromittierten Laptop eines Dienstleisters.

IRMA

Ein effektives Informationssicherheits-Managementsystem basiert immer auf den drei Säulen organisatorische, technische und personelle Maßnahmen. Damit scheint die Umsetzung des Sicher-

heitsstandards auf den ersten Blick jedoch problematisch, da häufig die Budgets sowie die Fachkräfte fehlen, um ein durchgängiges Sicherheitsniveau und den im IT-Sicherheitsgesetz geforderten Stand der Technik umzusetzen.

An diesem Punkt hat das Unternehmen VIDEC angesetzt: Die Security-Appliance „Industrie Risiko Management Automatisierung" (IRMA) ist ein Industrie-Computer-System, das kontinuierlich vernetzte Produktionsanlagen überwacht, Informationen zu Cyberangriffen liefert und die Analyse und intelligente Alarmierung mittels einer übersichtlichen Management-Konsole ermöglicht. Cyberangriffe oder Ausfälle sind sofort sichtbar und können detailliert untersucht werden. Zusätzlich bietet das Produkt eine erhebliche Unterstützung und somit Kosteneinsparung bei der Umsetzung von IT-Richtlinien.

B3S und IRMA

Der in IRMA integrierte „B3S-Wasser" entspricht dem praktischen Handlungsrahmen, der im Merkblatt W 1060/M 1060 und dem IT-Sicherheitsleitfaden zur Verfügung gestellt wird. Anhand der Auswahl und Behandlung der Anlagentypen, der Anwendungsfälle, dem Gefährdungs- und Maßnahmenkatalog lässt sich der Standard mit IRMA anwenden.

So werden durch die Auswahl der Anlagentypen (Kanalisation, Kläranlage, Leitzentrale, Trinkwassergewinnungsanlage, Wasserwerk, Trinkwasseraufbereitungsanlage oder Wasserverteilsysteme) die notwendigen Anwendungsfälle zur Risikoanalyse zur Verfügung gestellt. Die relevanten Bedrohungskategorien/Gefährdungen werden angezeigt und die jeweiligen Maßnahmen für die betroffenen Abteilungen Organisation, Personal, Hard- und Software sowie Notfallvorsorge behandelt. Das besondere ist, dass diese Maßnahmen direkt zu den passenden Systemen/Assets behandelt und dokumentiert werden. Der Umsetzungsstatus ist dabei jederzeit sichtbar. Wie im Standard gefordert, besteht hier auch die Möglichkeit, direkt einen zugehörigen Eintrag im Modul „Risiko Management" individuell zu erstellen.

IRMA enthält bereits in der Basisversion die vier Kernfunktionen:

_____ die automatische Erkennung der Assets (Teilnehmer) im Netzwerk. Diese Funktion ist passiv, bedeutet, dass kein Teilnehmer aktiv angefragt wird. Ein wichtiger Aspekt, da viele alte Geräte auf solche Abfragen sehr sensibel reagieren und neue Teilnehmer dadurch automatisch erkannt werden.

_____ Das Risikomanagement unterstützt die Mitarbeiter (IT und Automatisierer) bei der Bewertung eines jeden Assets und ermöglicht die standardkonforme Dokumentation für das Security-Management.

_____ die grafische Darstellung des gesamten Netzwerkes mit allen Querverbindungen in der Kommunikation sowie die Auswertungen zu jedem einzelnen Teilnehmer.

_____ Alarmierung von Anomalien, Änderungen und somit möglichen Angriffen automatisiert über direkte Verbindung (z. B. potenzialfreier Kontakt, SMTP) oder über ein Alarmierungssystem (z. B. AIP).

IT- und Betriebsverantwortliche sparen mit der Appliance IRMA bei der Aufnahme und Inventarisierung der IT-Assets Zeit und haben wenig Beratungsaufwand. Auch hilft ein integrierter Netzplan dabei, eine schnelle Übersicht der Anlage zu gewährleisten. Weitere Vorteile von IRMA sind:

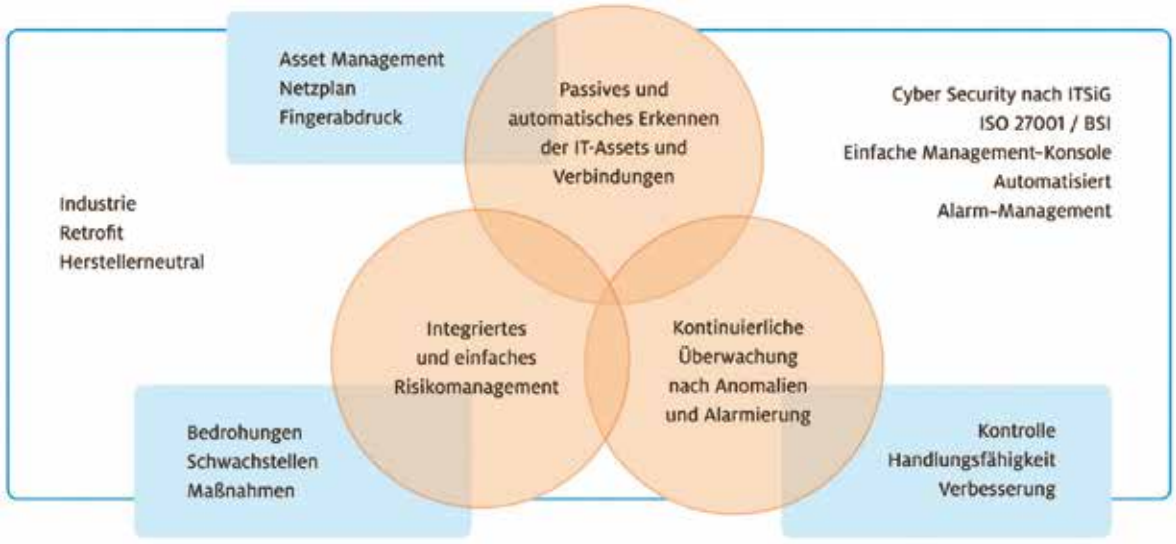


Abbildung 1: Aufbau von IRMA

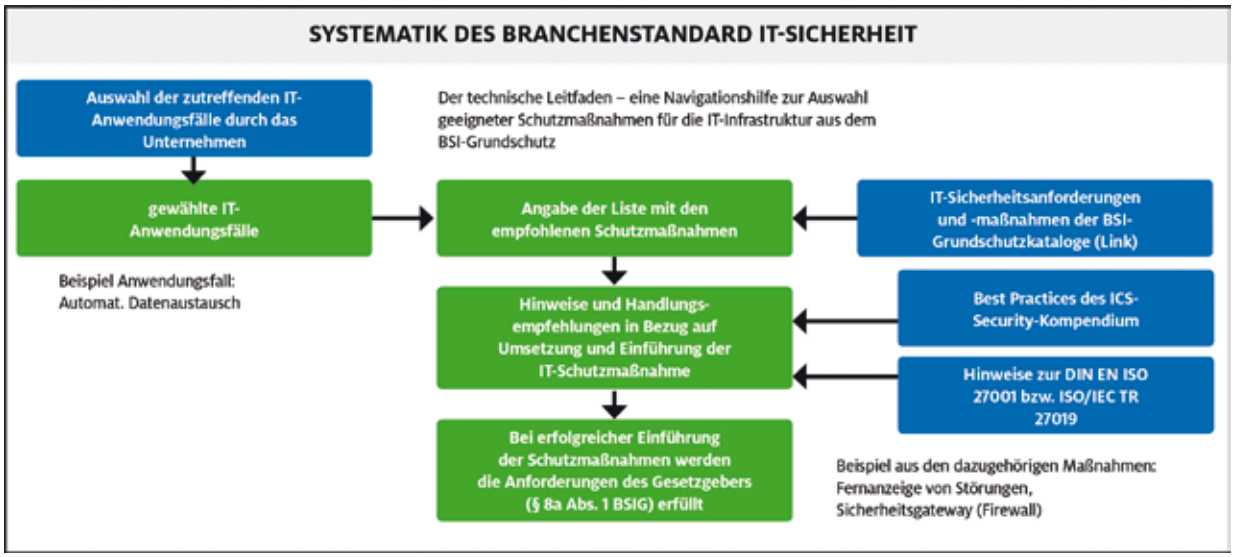


Abbildung 2: Systematik des Branchenstandards DVGW und DWA – M1060/W1060 (Bild: Deutscher Verein des Gas- und Wasserfaches e.V.)

_____ Integriertes Risikomanagement mit strukturierter und immer aktueller Auflistung der Risiken und festgelegten Maßnahmen je IT-Asset für den jeweiligen Anlagenverantwortlichen als Checkliste.

_____ Erfüllen der ITSiG-Meldevorgaben: Erkennen von Sicherheitsvorfällen durch die kontinuierliche Beobachtung der IT-Infrastruktur. Die Alarmierung erfolgt automatisiert.

_____ Angriffserkennung und somit unmittelbare, direkte Handlungsfähigkeit für die Betriebsleitung

_____ Schnelle Ursachen- und Datenerfassung für eine unkomplizierte Meldung

_____ Kontinuierliche Aktualisierung aller Assets mit Netzplan in verschiedenen Sichten

Fazit

Der Schutz vor Cyber-Attacken, die Auswirkungen des IT-Sicherheitsgesetzes oder die unternehmerische Verantwortung für die Verfügbarkeit von echtzeitfähigen Produktionsanlagen (Automatisierungen) sind mehr denn je die aktuellen Anforderungen an die Betriebsleitung und Geschäftsführung. IRMA trägt dazu bei, die IT-Sicherheit in Unternehmen zu erhöhen und unterstützt bei der Umsetzung von Brachenstandards.

Für interessierte Unternehmen gibt es die Möglichkeit, einen Demo-Testlauf für ihre Anlage durchzuführen. Nach kurzer Einrichtung des Systems kann der Anwender bereits die ersten Ergebnisse seiner Anlage im Rahmen eines Workshops sichten. Bei sehr vielen dieser Testinstallationen offenbarten sich einige Überraschungen im Netzwerk. Offene Serviceschnittstellen oder sogar unbekannte Geräte im Netzwerk waren keine Seltenheit. ■

Messestand: Halle 9, Stand 9-506

Impressum

DATAKONTEXT GmbH

Augustinusstraße 9d, 50226 Frechen (DE)
Tel.: +49 2234 98949-30,
Fax: +49 2234 98949-32
redaktion@datakontext.com,
www.datakontext.com

Geschäftsführer: Hans-Günter Böse, Dr. Karl Ulrich

Handelsregister:
Amtsgericht Köln, HRB 82299

Bankverbindung: Landesbank München,
IBAN: DE06 7005 0000 0004 3870 28

Zurzeit gültige Anzeigenpreisliste:
Nr. 35 vom 02. Januar 2017

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel.: +49 6728 289003, anzeigen@kes.de

Media-Daten: Unsere Media-Daten finden Sie online auf www.kes.info/media/.

Vertrieb: Jürgen Weiß,
weiss@datakontext.com,
Tel.: +49 2334 98949-71, Fax: -32

Satz: BLACK ART Werbestudio
Stromberger Straße 43a, 55413 Weiler

Druck: BWH GmbH,
Beckstraße 10, 30457 Hannover

Titelbild und Seite 4: NürnbergMesse/
Thomas Geiger

Wir bedanken uns bei den Mitherausgebern dieser Ausgabe

itsa 2018
Die IT-Security Messe und Kongress
The IT Security Expo and Congress
Halle 9 | Stand 405

noris cloud on openstack

CLOUD MADE IN GERMANY

MEHR LEISTUNG ALS STANDARD

- Cloud Transition aus einer Hand
- Volle Interoperabilität dank Open-Source-Technologie
- Höchste Datensicherheit
- Flexibles Pay-as-you-grow-Abrechnungsmodell

noris.de