OKTOBER 2019

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

MADE IN GERMANY

Powered by:

SecurITy made in Germany

TeleTrusT Quality Seal

VOGEL IT MEDIEN

Eine Publikation von IT-BUSINESS SECURITY INSIDER


G DATA
TRUST IN
GERMAN
SICHERHEIT
Kaffee geholt.
Daten weg.
Desktop sperren rettet
Unternehmen.
Schaffen Sie IT-Sicherheitsbewusstsein
gdata.de/awareness-training
itsa 2019
Die IT-Security Messe und Kongress
Erleben Sie die Gefahr ungeschulter Mitarbeiter
in einem interaktiven Live-Hacking.
Wir freuen uns auf Ihren Besuch – **Halle 9, Stand 520**.

"Secure Platform" – eine aktuelle Herausforderung

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


Bild: TeleTrusT

Liebe Leserinnen und Leser,
die Sicherheit von IT-Systemen kann kaum verlässlich eingeschätzt werden, meist auch nicht von Experten. Oft sind es schwer durchdringbare und komplexe Gebilde aus Hard- und Software.
Ein gravierendes Risiko kann es bei der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme geben. Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) hat mit seinem neu gegründeten Arbeitskreis "Secure Platform" die Zielsetzung formuliert, zu digitaler Souveränität und einem sicheren IT-Ökosystem in Deutschland, aber auch in der ganzen EU, beizutragen.
In diesem Zusammenhang sei auch auf die TeleTrusT-Handreichung "Stand der Technik" des gleichnamigen Arbeitskreises verwiesen, die fortwährend aktualisiert wird und mittlerweile in zwei weitere Sprachen übersetzt wurde.
Die produzierende Wirtschaft, die Verwaltung sowie private Anwender sind mehr denn je auf sichere und vertrauenswürdige Informationsinfrastrukturen angewiesen.
Dabei ist der Staat in der Pflicht, IT-Sicherheit als gesamtgesellschaftliche Aufgabe zu begreifen. Insbesondere vertrauenswürdigere, robuste IT-Systeme, die die Probleme "Softwaresicherheit" und "Malwarebefall" adressieren, sollten gefördert werden. IT-Sicherheitslösungen sollten auf starker Kryptographie basieren und im Kern der IT-Systeme verankert sein.
Proaktive IT-Sicherheitslösungen für "Industrie 4.0" sollen direkt umgesetzt werden, damit Deutschland eine weltweite Vorreiterrolle in IT-Sicherheit und Vertrauenswürdigkeit in Bezug auf die Leitindustrien übernehmen kann.
Die Nutzung von IT-Sicherheitstechnologie "made in Germany" muss bei Staat, kritischen Infrastrukturen und volkswirtschaftlich wichtigen Produktionsunternehmen Präferenz haben.
"IT Security made in Germany" ist Qualitätsmerkmal, ein schlagendes Verkaufsargument und strahlt dabei weit über die Landesgrenzen hinaus.
Diese Sonderpublikation informiert Sie über generelle Lösungsvorschläge, die von deutschen Unternehmen im Bereich der IT-Sicherheit entwickelt worden sind. Ebenfalls die rechtlichen Seiten werden mit einem Blick auf die DSGVO beleuchtet.
Gemeinsam mit den TeleTrusT-Mitgliedern wünsche ich Ihnen eine spannende und informative Lektüre und hoffe dabei, dass Sie nicht nur neue Aspekte für Ihr Unternehmen, sondern auch für sich selbst und Ihr privates Umfeld mitnehmen können. □

Titelbild: © orelphoto/Aha-Soft - stock.adobe.com (M) Carin Boehm

TeleTrusT-Initiative "IT Security made in Germany"

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

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

Was tun Sie bei einem Hackerangriff?

Entspannt bleiben – denn mit secunet sind Daten und Infrastruktur premiumsicher.

Wo Daten und IT-Infrastrukturen vor Cyberangriffen geschützt werden müssen, steht secunet bereit. Als IT-Sicherheitspartner der Bundesrepublik Deutschland bieten wir Behörden und Unternehmen Expertenberatung und premiumsichere Lösungen zum Schutz von Kommunikation und Daten.

secunet – Ihr Partner für IT-Premiumsicherheit.

secunet

Vertrauen hat einen Namen

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

Von Dr. Holger Mühlbauer und Jürgen Paukner

Träger des Vertrauenszeichens "IT Security made in Germany" (Stand 12.09.2019)

- 1984not Security GmbH
- abl social federation GmbH
- Accellence Technologies GmbH
- achelos GmbH
- Achtwerk GmbH & Co. KG
- ads-tec GmbH
- akquinet enterprise solutions gmbH
- Allgeier IT Solutions GmbH
- ANMATHO AG
- Antago GmbH
- apsec Applied Security GmbH
- ASOFTNET
- ATIS systems GmbH
- aumass GmbH & Co. KG
- ausecus GmbH
- Avira GmbH & Co. KG
- Backes SRT GmbH
- Bank-Verlag GmbH
- bc digital GmbH
- BCC Unternehmensberatung GmbH
- Bechtle GmbH & Co. KG
- Beta Systems IAM Software AG
- Biteno GmbH
- Blue Frost Security GmbH
- bowbridge Software GmbH
- Brabbler Secure Message and Data Exchange AG
- Build38 GmbH
- Bundesdruckerei GmbH
- CBT Training & Consulting GmbH
- CCVOSSEL GmbH
- certgate GmbH
- CERTIX IT-Security GmbH
- CGM Deutschland AG
- CHIFFRY GmbH
- C-IAM GmbH
- CoCoNet Computer-Communication Networks GmbH
- Cognitec Systems GmbH
- cognitix GmbH
- Cognitum Software GmbH
- COMback Holding GmbH
- comcrypto GmbH
- comforte AG
- comtime GmbH
- Condition-ALPHA Digital Broadcast Technology Consulting
- consistec Engineering & Consulting GmbH
- Consultix GmbH
- CONTURN Analytical Intelligence Group GmbH
- Crashtest Security GmbH
- CryptoMagic GmbH
- Cryptshare AG
- cv cryptovision GmbH
- dacoso data communication solutions GmbH
- dal33t GmbH
- Daniel Aßmann - Datenschutz & QM
- DATAKOM GmbH
- datenschutzklinik
- DATUS AG
- DERMALOG Identification Systems GmbH
- Detack GmbH
- DeviceLock Europe GmbH
- DFN-CERT Services GmbH
- dhpg IT-Services GmbH Wirtschaftsprüfungsgesellschaft
- digitalDefense Information Systems GmbH
- digitronic computersysteme GmbH
- DIGITTRADE GmbH
- ditis Systeme Niederlassung der JMV GmbH & Co.
- DocRAID(R) - professional data privacy protection
- DoctorBox GmbH
- DriveLock SE
- e-ito Technology Services GmbH
- eCom Service IT GmbH
- ecsec GmbH
- eperi GmbH
- esatus AG
- essendi it GmbH
- exceet Secure Solutions AG
- Fiducia & GAD IT AG
- floragunn GmbH
- FSP GmbH
- FZI Forschungszentrum Informatik
- G Data Software AG
- GBS Europa GmbH
- genua GmbH
- Giegerich & Partner GmbH
- glacier advisory & coaching
- grouptime GmbH
- HiScout GmbH
- Hornetsecurity GmbH
- Huf Secure Mobile GmbH
- Identos GmbH
- ifAsec GmbH
- if(is) - Institut für Internet-Sicherheit
- Infineon Technologies AG
- INFODAS GmbH
- Inlab Networks GmbH

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

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

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

- innovaphone AG
- IS4IT Kritis GmbH
- isits AG International School of IT Security
- ITConcepts Professional GmbH
- IT-Sitter GmbH Deutschland
- ISL Internet Sicherheitslösungen GmbH
- itWatch GmbH
- keepbit SOLUTION GmbH
- KeyIdentity GmbH
- Keyp GmbH
- KikuSema GmbH
- KIWI.KI GmbH
- KORAMIS GmbH
- LANCOM Systems GmbH
- Lanz Services GmbH
- limes datentechnik gmbh
- Link11 GmbH
- Linogate GmbH
- maincubes one GmbH
- MaskTech GmbH
- MATESO GmbH
- Matrix42 AG
- MB Connect Line GmbH Fernwartungssysteme
- Mentana Claimsoft GmbH
- metafinanz Informationssysteme GmbH
- M&H IT-Security GmbH
- MTG AG
- NETZWERK Software GmbH
- NCP engineering GmbH
- Net at Work GmbH
- netfiles GmbH
- NEOX NETWORKS GmbH
- Nexis GmbH
- nicos AG
- Nimbus Technologieberatung GmbH
- OctoGate IT Security Systems GmbH
- ondeso GmbH
- OPTIMA Business Information Technology GmbH
- OTARIS Interactive Services GmbH
- P-ACS UG
- PFALZKOM GmbH
- PHOENIX CONTACT Cyber Security AG
- Pix Software GmbH
- PPI Cyber GmbH
- PRESENSE Technologies GmbH
- procilon IT-Solutions GmbH
- PROSTEP AG
- Protforce GmbH
- PSW GROUP GmbH & Co. KG
- Pyramid Computer GmbH
- QGroup GmbH
- QiTEC GmbH
- QuoScient GmbH
- RED Medical Systems GmbH
- retarus GmbH
- Rhebo GmbH
- Rohde & Schwarz Cybersecurity GmbH
- r-tec IT Security GmbH
- SAMA PARTNERS Business Solutions GmbH
- sayTEC AG
- Schönhofer Sales and Engineering GmbH
- SC-Networks GmbH
- Secomba GmbH
- secrypt GmbH
- secucloud GmbH
- SECUDOS GmbH
- secunet Security Networks AG
- Secure Service Provision GmbH
- Securepoint GmbH
- SerNet GmbH
- signotec GmbH
- Softline AG
- SoSafe GmbH
- Steen Harbach AG
- Steganos Software GmbH
- Symlink GmbH
- syracom consulting AG
- T-Systems International GmbH
- TDT AG
- Tenzir GmbH
- TESIS SYSware Software Entwicklung GmbH
- TE-SYSTEMS GmbH
- THREATINT GmbH & Co. KG
- TÜV Informationstechnik GmbH
- Uniki GmbH
- Uniscon GmbH
- Utimaco IS GmbH
- VegaSystems GmbH & Co. KG
- Veronym Holding GmbH
- virtual solution AG
- Vulidity GmbH
- WhosApp GmbH
- WMC Wüpper Management Consulting GmbH
- Würzburger Versorgungs- und Verkehrs GmbH
- XignSys GmbH
- Zertificon Solutions GmbH

Unternehmen gemeinsam gegen Cybercrime verteidigen

Umfassende IT-Sicherheit bedeutet heute nicht nur den Einsatz einer leistungsfähigen Sicherheitslösung und die Umsetzung weiterer technischer Maßnahmen – auch Mitarbeiter gehören mit dazu. Sie machen den Unterschied, denn ein falscher Klick kann im schlimmsten Fall den Ausfall der gesamten Firmen-IT bedeuten. Auf der it-sa 2019 präsentiert G DATA erstmals live seine Security Awareness Trainings. Im Rahmen eines Live-Hacking werden zudem aktuelle Angriffe demonstriert – und neue Möglichkeiten, diese mit innovativen Technologien wie DeepRay oder BEAST abzuwehren.

G DATA TRUST IN GERMAN SICHERHEIT

87 Prozent der Unternehmen sehen ungeschulte Mitarbeiter als größte Schwachstelle für Cyberattacken (Quelle: ESI ThoughtLab). Durch die G DATA Security Awareness Trainings erhalten die Mitarbeiter das nötige Rüstzeug, um Cybergefahren zu erkennen und aktiv abzuwenden. In mehr als 35 einzelnen E-Learning-Einheiten lernen die Angestellten alles, was sie dazu benötigen. Abgedeckt sind alle wichtigen Themen, die für den Arbeitsalltag wichtig sind, zum Beispiel Arbeiten in der Cloud, Social Engineering oder Phishing.

Bedarfsgerechte Schulung

Bevor die Trainings starten, können IT- und Personalverantwortliche einen Wissenstest bei den Mitarbeitern durchführen. So wird schnell klar, wo die größten Probleme sind. Auf Grundlage dieser Ergebnisse lässt sich die Reihenfolge der Trainings festlegen. Nach und nach absolvieren die Angestellten alle Trainings, um ihr Wissen über IT-Sicherheit zu vervollständigen und alle Risiken beim Umgang mit den IT-Systemen zu kennen.

G DATA „Live-Hacking meets Mitarbeiter Awareness“ beim Congress @ it-sa

Erstmals ist G DATA beim Congress @ it-sa dabei. Am 08. und 09.10.2019 zeigt das Cyber Defense-Unternehmen bei einem interaktiven Live Hacking, wie schlecht geschulte Mitarbeiter Cyberattacken begünstigen und

so zu einem Sicherheitsrisiko werden. Fachbesucher können sich hier über eine Abstimmungs- und Feedbackmöglichkeit per Mobilgerät aktiv beteiligen. Beim Live-Hacking zeigen die G DATA-Experten zudem, wie Unternehmen heute angegriffen werden und wie sie sich dagegen schützen können. Dabei wird auch der Nutzen innovativer Technologien auf Basis von KI oder Graphen in der Abwehr von Malwareangriffen demonstriert.


Auf der it-sa 2019 präsentiert G DATA erstmals live seine Security Awareness Trainings.

Bild: G DATA

it-sa Premiere: BEAST – Das volle Bild durch graphenbasierte Sicherheit

Onlinekriminelle entwickeln Schadprogramme und Angriffsmuster ständig weiter und stellen Hersteller von Sicherheitslösungen vor neue Herausforderungen, weil sie versuchen, eine Erkennung zu verhindern. G DATA präsentiert in Nürnberg BEAST. Die neue graphenbasierte Security-Technologie „Made in Germany“ spürt bisher unbekannten Schadcode durch bösartiges Verhalten auf und geht dabei einen anderen Weg als herkömmliche Erkennungsverfahren: Alle Prozesse werden in einer Graphendatenbank nachgezeichnet, wodurch eine sichere und schnelle Erkennung von Schadprogrammen gewährleistet ist, ohne dass Fehlalarme auftreten. Die neue Technologie wird Teil aller G DATA Sicherheitslösungen für Windows-Betriebssysteme.

G DATA – IT-Security „Made in Germany“

G DATA ist Vorreiter in puncto vertrauenswürdiger IT-Sicherheit und hat bereits im Jahr 2011 im Rahmen der TeleTrusT-Selbstverpflichtung „IT Security made in Germany“ den Einbau von Backdoors kategorisch ausgeschlossen. Hierdurch verpflichtet sich G DATA, keine Lücken für Nachrichtendienste oder andere staatliche Behörden offen zu lassen oder Daten weiterzugeben – nur so kann eine umfassende IT-Sicherheit gewährleistet werden. Darüber hinaus werden die G DATA Sicherheitslösungen in Deutschland entwickelt und unterstehen so den strengen deutschen Datenschutzgesetzten und der EU-Datenschutzgrundverordnung. ■

Neben dem Live-Hacking ist G DATA mit Fachvorträgen zu BEAST und „Kaffee geholt – Daten weg“ am 08. und 09.10.2019 in den Foren der it-sa vertreten.

Messebesucher finden G DATA auf der it-sa in Halle 9, Stand 520.

Mehr Informationen zum G DATA-Messeprogramm unter www.gdata.de/it-sa

Neue Wege für mehr Sicherheit

Herkömmliche IT-Sicherheitsverfahren greifen zu kurz, um die wachsende Zahl an Cyberattacken abzuwehren. Erfolgreicher sind innovative Lösungen, welche die Systeme ganz abschotten oder die Daten an einem sicheren Ort ablegen. Selbst im Falle eines Angriffs kann dann kein Schaden entstehen.

Von Daniel Heck, Rohde & Schwarz Cybersecurity

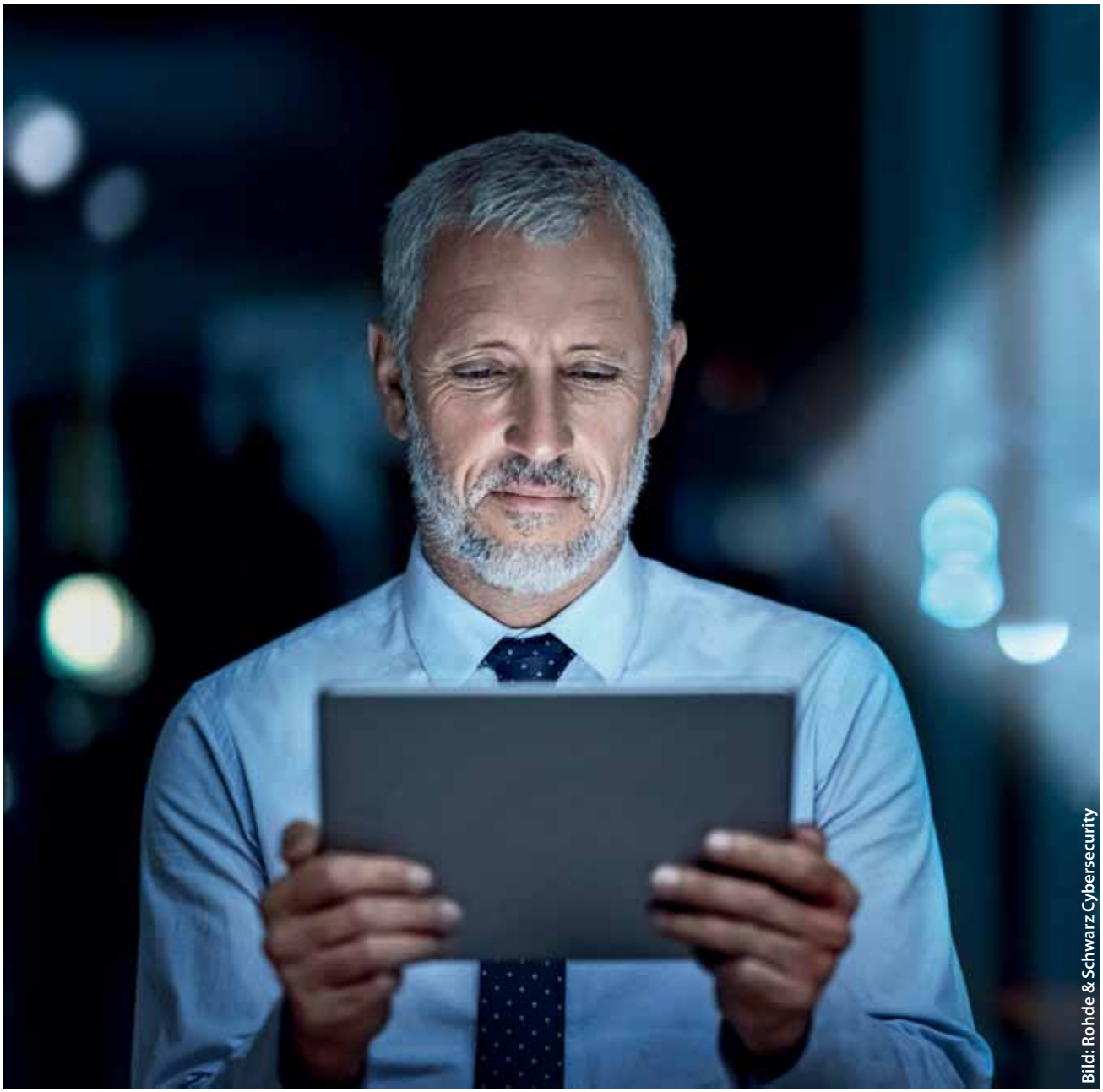


Bild: Rohde & Schwarz Cybersecurity

Angesichts der wachsenden Zahl an Cyberangriffen und der zunehmenden Angriffspunkte in digitalisierten Unternehmen ist es illusorisch geworden, jeden Angriff einzeln aufzuspüren. Diesen Ansatz verfolgen allerdings die meisten herkömmlichen Sicherheitstechnologien. Daten liegen zudem nicht mehr allein im Firmennetzwerk ab – sie werden stattdessen auf cloud-basierte Collaboration-Tools hochgeladen und geteilt oder an Remote-Geräte übertragen. Eine Perimetersicherheit ist hier nutzlos. Das Zeitalter der Digitalisierung braucht neue schlagkräftige IT-Sicherheitstechnologien. Ein Wechsel von reaktiven hin zu proaktiven Ansätzen ist notwendig.

Solche neuen Ansätze lassen sich mittels Separierung und Virtualisierung in der IT-Architektur umsetzen. Die Angriffsfläche der IT-Systeme wird dabei auf das funktional notwendige Maß reduziert. Anstatt immer neuer Malware mit Antivirenprogrammen hinterherzujagen, erfolgt eine systematische Trennung zwischen Internet und Intranet.

Virtualisierte Browser

Ergebnis eines solchen Separierungsansatzes ist der virtualisierte Browser. Er ist von allen anderen Anwendungen und den sensitiven Daten hermetisch getrennt. Es wird eine virtualisierte „Surfumgebung“ geschaffen. Alle potenziell gefährlichen Aktivitäten werden in einem geschlossenen virtualisierten Browser isoliert, bevor sie überhaupt zur Ausführung kommen.

Virtualisierte Browser haben einen weiteren Vorteil: Sie verhindern den Abfluss von Telemetriedaten aus Microsoft Office und Windows 10. Mit einem virtualisierten Browser lassen sich die Telemetriedienste proaktiv blockieren. Durch die Internet-Intranet-Trennung erreichen die für den Versand von Telemetriedaten zuständigen Microsoft-Dienste ihre Gegenstellen im Internet nicht mehr. Sollten Microsoft oder andere Hersteller neue Dienste, neue URL oder ähnliches einführen, bleiben sensible Unternehmens- und Behördendaten allein im eigenen Netzwerk.

Daten absichern in der Cloud

IT-Sicherheitslösungen für die Cloud müssen in der Lage sein, die Daten unabhängig von ihrem Speicherort vor dem Zugriff Dritter zu schützen. Technisch umsetzen lässt sich das mit einem datenzentrischen Sicherheitsansatz: Dabei werden die Daten verschlüsselt, fragmentiert und regulatorisch konform gespeichert. Daten, die Europa nicht verlassen dürfen, werden z. B. logisch-rechtlich in verschiedenen europäischen Rechenzentren sicher verschlüsselt und verteilt abgelegt. In der globalen Cloud liegen ausschließlich virtuelle Dateien ohne Dateninhalt, die aber dafür sorgen, dass von allen autorisierten Nutzern alltägliche Arbeitsabläufe in der Cloud wie gewohnt genutzt werden können. Egal, wo ein Angreifer Zugriff erlangt: Er kann keinen Schaden mehr anrichten. Diese Art der Speicherung ist nicht nur besonders sicher, sie entspricht auch den strengen Datenschutz- und Sicherheitsvorgaben der EU-DSGVO.

Effiziente IT-Sicherheit

IT-Sicherheit muss wirtschaftlich realisierbar sein – auch für kleine und mittelständische Unternehmen. Auch kleine Teams sollten die IT-Sicherheitsanwendungen bedienen können. Zudem dürfen die Lösungen nicht zu viel interne Rechenleistung belegen, da dies hohe Kosten verursachen kann. Besonders effizient sind Software as a Service-Lösungen (SaaS). Unternehmen können sich mit solchen Anwendungen schützen, ohne die gesamte erforderliche Backend-Infrastruktur verwalten und neue Fähigkeiten erlernen zu müssen. Eine solche IT-Security aus der Cloud ist besonders nutzerfreundlich und skalierbar: Je nach Bedarf lassen sich Features an die Bedürfnisse eines Unternehmens anpassen. Entscheidend dabei ⇨

ist allerdings, dass die Daten innerhalb der EU gespeichert und so die europäischen Datenschutzvorschriften erfüllt werden.

Neue Sicherheitssysteme bieten sogar die Möglichkeit, Elemente einer IT-Sicherheitslösung abhängig von deren Sicherheitsbedarf entweder „on-premise“ oder in der Cloud abzulegen. Auf diese Weise lassen sich die Vorteile der Cloud nutzen, ohne auf Sicherheit verzichten zu müssen. Eine solche Skalierung der Sicherheit wird möglich durch „Containering“. Bei diesem Architekturmodell kommen kleinste Softwareeinheiten – sogenannte Microservices – zum Einsatz, die sich unabhängig voneinander steuern lassen. Microservices für sensible Elemente, wie beispielsweise dem Key- und Administrationsserver, können dann auf der eigenen Hardware abgelegt werden. Falls eine solche nicht vorhanden ist, kann eine Cloud genutzt werden mit einem höheren Sicherheitsniveau. Kryptografisch weniger kritische Abläufe lassen sich auf andere Clouds auslagern. Lösungen mit Microservices eignen sich auch für global agierende Firmen mit komplexen Strukturen. So gestaltete Lösungen lassen sich flexibel an die unterschiedlichen Bedingungen anpassen, wie etwa Zeitverschiebung und Betriebsgröße.

Höchste Sicherheit für den Fernzugriff

Damit Mitarbeiter im Home-Office, bei Fortbildungen oder auf Geschäftsreisen stets erreichbar sind und auf Daten und Anwendungen zugreifen können, nutzen sie einen Fernzugriff auf das Unternehmensnetzwerk über das Internet. Kommen Remote-Endgeräte zum Einsatz, ist der Schutz der Daten allerdings komplex.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nennt als wichtigste Maßnahmen die erfolgreiche Authentifizierung des Benutzers, die Verschlüsselung der Daten auf dem Endgerät sowie den Einsatz eines kryptografisch gesicherten VPN, um die Kommunikationsverbindung zwischen dem Endgerät und dem Netz des Unternehmens vor unbefugten Mitlesern zu schützen.

Am effizientesten lässt sich ein solches Bündel an Anforderungen anhand modularer und softwarebasierter Sicherheitslösungen umsetzen. Mit einer solchen Lösung sind keine speziellen und oft teuren Zusatzgeräte notwendig. Stattdessen wird ein sicherer VPN-Client installiert, der die Netzwerkkommunikation des Endgerätes über das Internet schützt. Eine zusätzliche Festplattenvollverschlüsselung sorgt dafür, dass das Endgerät lokale Daten sicher speichert. Wird die Lösung durch einen virtualisierten Browser ergänzt, dann sind die Endgeräte auch vor Angriffen aus dem Internet geschützt.

IT-Sicherheit Made in Germany

Unternehmen sollten darauf achten, dass sie europäische IT-Sicherheitstechnik nutzen. Sie bietet im weltweiten Vergleich hoch innovativen Schutz – und genießt das höchste Vertrauen. Darüber hinaus existiert in Deutschland keine Verpflichtung, Hintertüren für den Staat einzubauen – im Gegensatz zu anderen Staaten. Und mit der EU-DSGVO wurde der Schutz der Daten sogar europaweit gesetzlich verankert. Das ist sowohl ein Vorteil für Bürger und Unternehmen als auch Verpflichtung für Unternehmen, sich selbst im Datenschutz und bei der IT-Sicherheit sicher aufzustellen. □

Der Autor


Bild: Rohde & Schwarz

Daniel Heck ist Vice President Marketing bei Rohde & Schwarz Cybersecurity. Das IT-Sicherheitsunternehmen schützt Unternehmen und öffentliche Institutionen weltweit vor Cyberangriffen.

Wie wird 5G sicher?

Dr. Kai Martius, CTO der secunet Security Networks AG, über das richtige Sicherheitskonzept für den neuen Mobilfunkstandard.

Die Diskussion um den neuen Mobilfunkstandard 5G entzündet sich immer wieder an der Frage nach dessen Sicherheit. Bei genauerer Betrachtung geht es dabei allerdings weniger um konkret erkannte Sicherheitslücken. Vor allem besteht ein Vertrauensproblem, das von einer geopolitischen Angst herrührt. Dauerhaft lässt sich dieses Problem nur beseitigen, wenn Deutschland und Europa wieder stärker in eigene technologische Kompetenz investieren und dadurch die Abhängigkeit von globalen Akteuren verringern. Das kann durchaus gelingen, wenn eine zielgerichtete Standardisierung den Rahmen vorgibt. Gute Ansätze sind vorhanden. Doch eines ist klar: Ein solcher Kompetenzausbau vollzieht sich nicht über Nacht.

Dr. Kai Martius ist CTO der secunet Security Networks AG.

Die gute Nachricht ist, dass auch kurzfristig Maßnahmen verfügbar sind, um 5G abzusichern. Dabei handelt sich um bewährte Konzepte aus der klassischen IT-Welt. Denn 5G bietet als erster Mobilfunkstandard die Möglichkeit, kryptographische Sicherheitsmechanismen Ende-zu-Ende einzusetzen. Das liegt daran, dass 5G faktisch kein reines Funknetz ist. Vielmehr besteht die Technik aus Minirechenzentren, die an ein IP-Netz mit einer Funkschnittstelle angebunden sind. Verschlüsselungstechnologien können hier sehr gut ein Abhören von Nutzdaten verhindern und auch die Verfügbarkeit stärken.

Dennoch bleibt ein Restrisiko: Es ist durchaus vorstellbar, dass nicht vertrauenswürdige Netzwerkkomponenten einen „Kill Switch“ enthalten, der die Verfügbarkeit gefährdet. Daher wäre es sinnvoll, 5G durch ein stärker geschütztes und überwachtes Netz zu ergänzen, das für kritische Infrastrukturen wie Energienetze vorgesehen ist. Im Krisenfall, etwa bei einem Ausfall des 5G-Netzes, könnte diese Infrastruktur eine Kommunikations-Grundversorgung von Industrie und Bevölkerung gewährleisten.

Solche Sicherheitskonzepte lassen sich mit vorhandener Technologie gut umsetzen. Dennoch zeigt die Debatte rund um 5G: Langfristig ist es für Deutschland und Europa wichtig, digitale Souveränität zurückzuerlangen – zumal sich bei künftigen Digitalisierungsprojekten wieder ähnliche Herausforderungen stellen werden.

secunet.com ■

Sichere Kommunikations-lösungen für Mobility, IIoT und Cloud

Seit der Firmengründung vor mehr als 30 Jahren ist es erklärtes Ziel von NCP, Inbetriebnahme, Nutzung und Management eines Remote Access-Netzwerkes für Unternehmen und Anwender so einfach und übersichtlich wie möglich zu gestalten.

NCP
SECURE COMMUNICATIONS

Über die klassische Anbindung der Endgeräte von Mitarbeitern hinaus haben sich die Anforderungen im Laufe der Zeit stark gewandelt. Heute sind Unternehmen weltweit mit Standorten bis in die Produktion zu einzelnen Maschinen, Geräten und Sensoren vernetzt. Datenkommunikation ist längst nicht mehr nur ein Thema der Mitarbeiter.

Hochsichere Maschinen-Kommunikation

Industrie 4.0 bedeutet die Digitalisierung aller Prozesse entlang der gesamten Wertschöpfungskette, von Bestellungen bis hin zur Produktion und die Vernetzung aller darin enthaltenen Akteure, sowie darüber hinaus die Verzahnung der klassischen Unternehmens-IT, wie z. B. ERP-Systeme mit den operationalen Netzen der Produktion, der sogenannten OT. NCP hat für die verschiedensten Industrial Internet of Things (IIoT)-Szenarien Software-Komponenten für den sicheren Datenaustausch und deren Überwachung entwickelt.

Fernwartung – gezielte sichere Ansprache einzelner Systeme

Zugänge zur Fernwartung von Maschinen und Systemen erfordern Flexibilität und Verfügbarkeit bei gleichzeitiger Sicherheit. Sowohl die Absicherung der Verbindungen selbst als auch Maßnahmen zum Schutz vor möglicherweise kompromittierten Netzen und Endgeräten der Hersteller stehen im Fokus.

Identisch konfigurierte Netze stellen in der Fernwartung ein Problem bei der Identifizierung von Zielsystemen dar. Eine gezielte Ansprache bis hin zum richtigen Endpunkt ist mit den NCP-Komponenten möglich und bereits technisch gelöst – durch eindeutige temporäre IP-Adressen und Authentisierungsmerkmale der Gateways und Clients (hardware- oder softwarebasiert).

Professioneller Remote Access

Die langjährige Erfahrung im Remote Access-Umfeld bildet bei NCP die Basis für die klassische ganzheitliche VPN-Lösung – abgestimmt auf die Belange von Anwendern, IT-Administratoren und Controllern.
Die NCP Enterprise-Lösung ist modular aufgebaut und bietet gemanagte VPN Clients für verschiedene mobile Endgeräte, ein zentrales Remote Access Management-System sowie VPN Gateways als Software-Komponente oder virtuelle Appliance. Das Management-System bildet auch gleichzeitig die Brücke zu den IIoT-Komponenten von NCP.

VPN out oft he Cloud

Cloud Provider haben mit NCP die freie Wahl, welche Architektur sie ihren Kunden anbieten möchten. Ob als reine Cloud-Lösung, virtuell, VPN as a Service oder auch als eine Kombination der genannten Architekturen. Neukunden können sofort angeschlossen werden, egal ob zunächst nur im Pilotbetrieb für eine Handvoll oder flächendeckend für eine Vielzahl von Usern.

Made in Germany als Grundstein der IT-Sicherheitslösung

Mit Sicherheitslösungen „Made in Germany“ von NCP gehen Unternehmen heute ein deutlich geringeres Risiko ein. Sie müssen keine Hintertüren fürchten und können von einem voll funktionsfähigen Produkt mit optimaler Schutzwirkung ausgehen. ■

Besuchen Sie NCP auf der it-sa:
Halle 10, Stand 120

Das volle Bild durch graphenbasierte Sicherheit

Cybercrime ist ein Milliardengeschäft. Ob durch Erpressung mit sogenannter Ransomware, Datenspionage und -hehlerei oder Manipulationen im digitalen Zahlungsverkehr.

Von Hauke Gierow und Thomas Siebert, G DATA Software

Malware-Autoren arbeiten konsequent daran, einer Erkennung durch Antiviren-Lösungen zu entgehen. Dazu benutzen die Kriminellen Untergrund-Dienste, die regelmäßig automatisiert prüfen, ob ihre Schadsoftware von einem Sicherheitshersteller erkannt wird. Ist das der Fall, wird der Schadcode automatisch verändert, bis die Erkennung ausbleibt. Um mit der zunehmenden Geschwindigkeit Schritt zu halten, setzen immer mehr Hersteller auf KI-Technologien, um neu verpackte Malware-Samples schnell und effektiv aufspüren zu können.

Doch nur bekannte und immer wieder neu verpackte Schädlinge aufzuspüren, reicht heute nicht mehr aus. Angriffe, gerade gegen Unternehmen, werden immer gezielter. Dabei setzen Kriminelle immer häufiger auch bislang unbekannte Malware oder spezialisierte Schadsoftware ein, von der es nur wenige bekannte Samples gibt. Oder sie führen legitime Tools für eine Angriffskette zusammen, die in ihrer Gesamtwirkung schadhaft ist. Diese Attacken stellen für Antivirenlösungen eine besondere Herausforderung dar.

Eine Abhilfe bietet Verhaltensüberwachung, um schadhafte Prozesse zu erkennen. Diese analysiert das Verhalten von Prozessen auf dem Computer und überwacht dabei etwa Änderungen im Dateisystem und in der Registry, insbesondere an verdächtigen Stellen wie dem Autostart-Ordner.

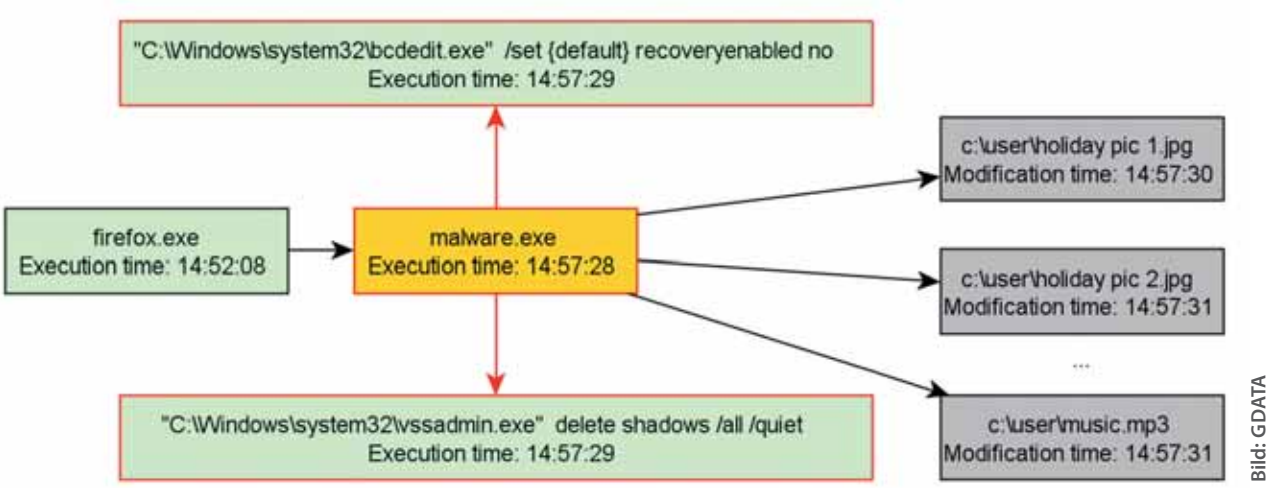
Das Problem der Verhaltensüberwachung

Das Problem: Bestehende verhaltensbasierte Erkennungsansätze versuchen, möglicherweise bedrohliches Verhalten in numerische Werte zu übersetzen – also einen Grad von „Badness“ festzustellen. Bei der Aggregation des numerischen Werts gehen notwendigerweise immer Information verloren, wodurch eine gewisse Unschärfe entsteht – selbst, wenn zum Lernen von Schwellwerten Machine Learning zum Einsatz kommt.

Damit lassen sich zwar durchaus auch unbekannte Malware-Familien aufspüren, die Technologie ist aber für Fehleinschätzungen anfälliger als andere Erkennungsverfahren. Entweder wird der Schwellwert für die Erkennung so hoch angesetzt, dass kaum noch Schadsoftware erkannt wird. Oder der Schwellwert wird so niedrig angesetzt, dass häufig Fehlalarme – sogenannte False-Positives – auftreten.

Verhaltensanalyse mit Graphen

Um dieses Problem zu lösen, hat G DATA „BEAST“ entwickelt. BEAST wählt einen radikal anderen Ansatz als bisherige Technologien



Beispiel eines Graphen: Beim schädlichen Download „malware.exe“ handelt es sich offenbar um eine Ransomware.

zur Verhaltensanalyse. Denn anstatt die verdächtigen Aktionen in einem numerischen Wert zu aggregieren, zeichnet die Technologie die Prozesse in einem Graphen nach. Dazu wurde eigens eine performanceoptimierte Graphdatenbank entwickelt, die lokal auf dem Rechner der Kunden läuft.

Der Vorteil der Graphdatenbank: Sie zeichnet ein vollständiges Bild auf, das Bedrohungen eindeutig erkennen kann. Ein Beispiel findet sich in dem hier dargestellten Graphen. Der Nutzer wurde offenbar von einem Angreifer dazu gebracht, einen schädlichen Download aus dem Webbrowser zu öffnen – oder er wurde Opfer einer Sicherheitslücke, die durch einen sogenannten Exploit ausgenutzt wurde. Beim schädlichen Download „malware.exe“ handelt es sich offenbar um eine Ransomware, die Daten des Nutzers verschlüsselt und für die Entschlüsselung ein Lösegeld fordert. Das zeigt sich darin, dass der Prozess erst eine Instanz des Systemwerkzeugs „bcdedit“ öffnet, um die Wiederherstellungsfunktion von Windows zu deaktivieren. Gleichzeitig deaktiviert ein weiteres Systemwerkzeug „vssadmin“ das Anlegen von sogenannten „Volume Shadow Copies“, die genutzt werden können, um kürzlich versehentlich überschriebene Dateien wiederherstellen zu können. Das ist eine typische Vorbereitungshandlung von Ransomware. Daraufhin beginnt der Schadcode, Dateien im Nutzerverzeichnis zu verschlüsseln.

Nachträgliche System-Bereinigung

Ein weiterer Vorteil der BEAST-Technologie: Da die Informationen über verdächtige Prozesse in der Graphdatenbank für einige Zeit vorgehalten werden, können Aktionen von Malware auch nach einer Infektion zurückgerollt werden. Anders als bei herkömmlicher Verhaltenserkennung überleben die im Graph gespeicherten Informationen auch einen Neustart des Rechners. Das bedeutet: Wird auf dem System Malware installiert, die zu diesem Zeitpunkt noch nicht erkannt wird, kann BEAST die Installation der Malware vollständig zurückrollen. Um dieses sogenannte „Retrospective Removal“ zu ermöglichen, gleicht BEAST Indikatoren aus dem aufgezeichneten Graphen mit anderen Komponenten der G DATA Sicherheitslösung ab.

Dieser Ansatz ist nicht auf infizierte Dateien beschränkt. So können auch andere Indicators of Compromise (IoCs) genutzt werden, um eine nachträgliche Bereinigung eines Systems auszulösen. Das kann neben dem Hashwert einer Datei etwa eine Verbindung zu einem bekannten Command-and-Control-Server sein. □

SICHER. **VERNETZT.**

SecurITy made in Germany

BESUCHEN SIE UNS AUF DER

it sa

Halle 11, Stand 312

NETZWERK UND SECURITY

WACHSEN WEITER ZUSAMMEN

Mit einer am Markt einzigartigen Kombination aus vertrauenswürdiger Netzwerkinfrastruktur und IT-Security „Made in Germany“ präsentiert LANCOM Systems zur it-sa innovative Weiterentwicklungen seiner Netzwerk- und Security-Lösungen. Die **LANCOM Management Cloud (LMC)** ist hierbei die Schaltzentrale für die automatisierte Konfiguration und Pflege der WAN-, LAN-, WLAN- und UTM-Lösungen.

Pünktlich zur it-sa reihen sich nun auch die **LANCOM R&S®Unified Firewalls** in das ganzheitliche Management der LMC ein. Damit ist ab sofort das gesamte Netzwerkportfolio, bestehend aus Routern, Switches, Access Points und Firewalls, auf Wunsch über ein einheitliches, intuitiv bedienbares Cloud-Management-System verwaltbar. Die LANCOM R&S®Unified Firewalls sind somit **„Cloud-ready“** und das Portfolio um eine zentrale Eigenschaft erweitert: **Cybersecurity**. Die einfach zu bedienenden Komplettlösungen sorgen dank state-of-the-art Sicherheitstechnologien und **Unified Threat Management (UTM)** für maximale Sicherheit.

Auf der it-sa präsentiert LANCOM zudem sein weiter ausgebautes SD-WAN-Angebot für noch mehr Sicherheit und Effizienz und zeigt eine Preview seiner künftigen Wi-Fi 6 Access Point-Familie.

www.lancom.de/events/it-sa/

LANCOM Systems

Secure Communications für alle Unternehmensbereiche

Im Zuge der gesamten Digitalisierung und des damit verbundenen, rasanten Fortschritts wachsen nunmehr auch die klassische Unternehmens-IT und die Operative Technologie (OT) mehr und mehr zusammen. Alles trifft sich in der Welt des Industrial Internet of Things (IIoT).

Von Jürgen Hönig, NCP engineering

Aufgrund der Historie und der gewachsenen Strukturen haben aber viele Bereiche einer Wertschöpfungskette, gerade in Produktionsbereichen, in puncto Datensicherheit noch Nachholbedarf. Abhilfe muss hier eine sichere Infrastruktur schaffen, bestenfalls mit einem zentralen Verwaltungspunkt. Dieser baut auf der einen Seite eine Brücke zwischen Produktions- und Informationswelt auf und stellt auf der anderen Seite aber auch sicher, dass Zuverlässigkeit, Transparenz und Datensicherheit gewährleitet werden.

Das Thema Cloud spielt in diesen neu entstehenden Umgebungen wahrlich eine zentrale Rolle. Viele Hersteller, darunter auch Maschinenhersteller, sind zwischenzeitlich dazu übergangen, z. B. ihre Fernwartungsdienste in die Cloud zu integrieren. Hierdurch werden direkte Verbindungen zwischen Hersteller-LAN und Maschine durch Verbindungen mit der Cloud als Endpunkt ersetzt. Die sich aus dieser Architektur ergebenden Vorteile, wie Zentralisierung der Daten, einfache Verwaltbarkeit, globalisierte Hochverfügbarkeit und Skalierbarkeit liegen auf der Hand. Das aufgrund der breitgefächerten Kommunikationsmöglichkeiten entstehende potenzielle Risiko der Datenmanipulation oder eines Datendiebstahls verlangt auch hier eine entsprechende Absicherung der Datenströme mit zusätzlichen Sicherheitsmechanismen wie Authentisierung von Maschinen, z. B. mit Hardware-Zertifikaten.

Lösung für IT und OT

Vor dem Hintergrund des Aufeinandertreffens von IT und OT steigt der Anspruch an Funktionalität und Flexibilität der Produkte, die in den verschiedenen Unternehmensbereichen zum Einsatz kommen. Für den Nürnberger Software-Hersteller NCP, der sich seit vielen Jahren mit der Entwicklung von Lösungen rund um sichere Kommunikation beschäftigt, sind diese Anforderungen mittlerweile Tagesgeschäft. Hier hat man sich neben dem Kerngeschäft, der Entwicklung von ganzheitlichen VPN-Lösungen, bereits sehr früh auch mit speziellen Lösungen wie z. B. für M2M, Car-IT, Digital Signage, ATMs und Fernwartung beschäftigt. Diese heterogenen Welten lassen sich mit einer zentralen Verwaltungskomponente verbinden und bei Bedarf zentral auch in der Cloud verwalten. Die Produkte sind seit Jahren im Einsatz und sichern heute in Tausenden von Umgebungen die Unternehmens-Kommunikation ab.

Zentrale Funktionen sind entscheidend


Bild: NCP

Aufgrund der teils komplexen Umgebungen ist es wichtig, dass die Core-Funktionalität auf der zentralen Seite gegeben ist. Der Anspruch an sichere, zuverlässige Verarbeitung von Massendaten (Big Data) ist ebenso selbstverständlich wie die Mandantenfähigkeit für einen flexiblen Betrieb. So lassen sich unterschiedliche Kunden/Unternehmensbereiche vollkommen getrennt über physikalische oder virtuelle Systeme hinweg bedienen. Durch die hohen Lastanforderungen, die z. B. beim Hosting von vielen Tausend VPN-Tunneln entstehen können, sind Load Balancing und Fail Safe verpflichtend für eine hohe Skalierbarkeit. Eine Management-Konsole, die sowohl mit mehreren Gateways pro Kunde/Unternehmensbereich als auch mit getrennten Mandanten z. B. bei Service Providern zurechtkommt, unterstützt die Abläufe der Anbieter und die Sicherheitsbedürfnisse der Kunden gleichermaßen.

Quality of Service

Unterschiedliche Daten wollen unterschiedlich priorisiert werden. Mithilfe des „Quality of Service“ (QoS) können bestimmte Datenpakete bevorzugt werden. Mit der Priorisierung des Datenstroms können Echtzeit-Anwendungen bei der Zuteilung von Bandbreite begünstigt werden, sodass immer die benötigte Bandbreite für eine qualitativ hochwertige Anwendung ohne Abbrüche oder Verzerrungen bereitgestellt wird. Andere bandbreitenintensive Anwendungen müssen dann warten, bis ausreichend Bandbreite freigegeben ist. Dies äußert sich dann durch langsamere Geschwindigkeiten, die aber bei Nicht-Echtzeit-Programmen wenig kritisch sind. QoS dient dabei als „Bandbreiten-Management“, das keine zusätzliche Bandbreite zur Verfügung stellt, sondern lediglich bestimmte Datenübertragungen bevorzugt.

VPN Clients mit QoS

Für NCP ist es selbstverständlich, dass in der neuesten Softwaregeneration ihrer VPN Clients diese Funktionalität enthalten ist. Somit kann z. B. erreicht werden, dass bei hoher Netzwerklast anstehende VoIP-Pakete bevorzugt versendet werden, um immer eine gute Sprachqualität zu gewährleisten. Ein Herunterladen eines Updates, welches im Hintergrund erfolgt, geschieht entsprechend langsamer. □

Der Autor


Bild: NCP

Jürgen Hönig ist Leiter Marketing bei der NCP engineering GmbH.

Retarus Email Security: Rundumschutz aus deutschen Rechenzentren inklusive Business Continuity

Zusätzlich zur Flut aus Malware- und Spam-Nachrichten sehen sich Unternehmen immer öfter mit komplexen Bedrohungen wie Phishing-Angriffen oder Social Engineering konfrontiert. Traditionelle Sicherheitsmechanismen bieten vor solch perfiden Attacken keinen zureichenden Schutz mehr.

retarus:

Außerdem kursiert Malware in ständig abgewandelten Varianten, die signaturbasierte Virenscanner nicht sofort erkennen und somit nicht sofort herausfiltern können. Ist Schadcode erst einmal unbemerkt im Postfach eines Nutzers gelandet, kann er sich von dort aus nahezu ungehindert in der gesamten IT-Infrastruktur ausbreiten. Retarus Email Security schützt Unternehmen auch vor den Angriffen, gegen die traditionelle Engines meist machtlos sind.

Advanced Threat Protection

Mit Advanced Threat Protection (ATP) hat Retarus ein effektives Paket gegen besonders perfide E-Mail-Angriffe geschnürt. Es enthält unter anderem folgende Mechanismen:

- Sandboxing: Unbekannte, verdächtige E-Mail-Anhänge werden vor der Zustellung in einer abgeschotteten Testumgebung des Retarus-Technologiepartners Palo Alto Networks überprüft, die Retarus in eigenen Rechenzentren in Deutschland betreibt.
- CxO Fraud Detection: Neben einer fortschrittlichen Analyse des E-Mail-Headers entlarven spezielle Algorithmen gegen From- oder Domain-Spoofing gefälschte Absenderadressen als Betrugsversuche. Unternehmen können sich so besser vor finanziellem Schaden durch Social Engineering und „Chefbetrug“ schützen.
- Time-of-Click Protection: Um Phishing-Angriffe zu unterbinden, schreibt Retarus alle Links in eingehenden E-Mails um und prüft sie bei jedem Aufruf erneut. Ist die Zielseite als gefährlich bekannt, wird die

Weiterleitung blockiert und eine Sicherheitswarnung angezeigt.

Forensic SIEM Integration

Retarus Email Security kann forensische Daten, sogenannte Events, in Echtzeit bereitstellen und per API an vorhandene Tools für Security Information and Event Management weiterleiten. So lässt sich der SIEM-Datenstrom unkompliziert mit zusätzlichen Details zur E-Mail-Sicherheit anreichern.

„Detect & React“ mit Patient Zero Detection®

Sollte trotz aller Schutzmaßnahmen dennoch einmal Malware via E-Mail in die Mailboxen von Anwendern gelangen, kommt die von Retarus entwickelte und europaweit patentierte Technologie Patient Zero Detection® zum Einsatz. Diese erzeugt für jeden empfangenen Dateianhang und jede URL einen „digitalen Fingerabdruck“. Falls Retarus Email Security später in einem identischen Anhang Schadcode entdeckt oder eine URL als Phishing-Link identifiziert, werden alle früheren Empfänger und deren Administratoren umgehend informiert. Mit „PZD Real-Time Response“ lassen sich für Microsoft Exchange (On-Premises oder Office 365) automatisierte Reaktionen festlegen, zum Beispiel ein Verschieben oder Löschen von nachträglich als schädlich befundenen Nachrichten.

Email Continuity

100-prozentige Verfügbarkeit ist unbezahlbar. Für den Fall, dass das E-Mail-System beim Kunden komplett ausfällt, sei es durch einen Security-Incident, einen Hardwarefehler oder eine Cloud-Downtime, stellt Retarus übergangsweise vorprovisionierte Webmail-Postfächer zur Verfügung. Signalisiert der Kunde einen Ausfall, kann Retarus das Routing blitzschnell umlenken und die betroffenen Endnutzer können weiter per E-Mail kommunizieren.

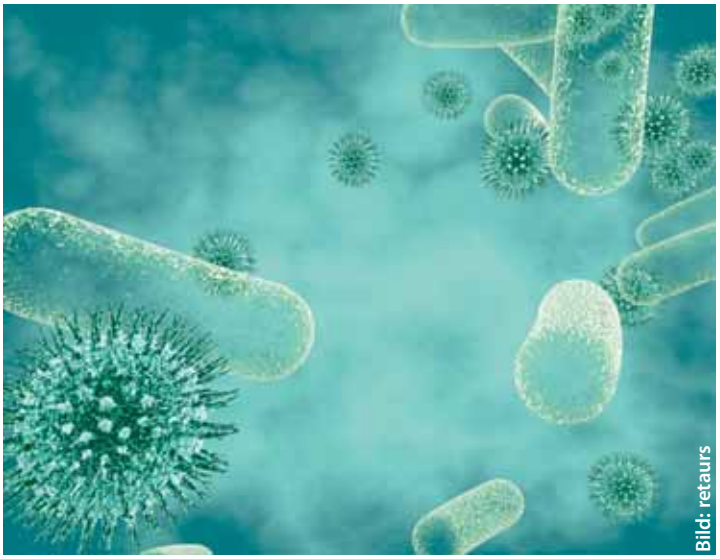


Bild: retaurs

Retarus lenkt Informationsströme auf Enterprise Level, sichert diese mit innovativen und patentierten Technologien ab und sorgt für Business Continuity.

Retarus hat die Erfahrung, Informationsströme auf Enterprise Level zu lenken, abzusichern und für Business Continuity zu sorgen. Nicht zuletzt deshalb haben die Analysten von Gartner Retarus in den „Market Guide for Email Security“ aufgenommen und führt Forrester Research Retarus in der „Wave: Enterprise Email Security, Q2 2019“ als einen der zwölf aktuell wichtigsten Anbieter für E-Mail-Sicherheit weltweit.
Weitere Informationen finden Sie unter www.retarus.de/email-security ■

Retarus auf der it-sa!

Besuchen Sie uns von 8. bis 10. Oktober 2019 in Nürnberg in Halle 11 / Stand 520.

Verschlüsselt Johnny jetzt endlich seine Mails?

Trotz zahlreicher Sicherheitsvorfälle verschlüsseln nach wie vor nur wenige Internet-Nutzer ihre E-Mails. Neue gesetzliche Vorschriften sollen das nun ändern. Damit dies funktioniert, muss der Anwender mehr als bisher im Vordergrund stehen.

Von Klaus Schmeh, cryptovision

Bild: Sashkin/stock.adobe.com

Der Forschungsaufsatz „Why Johnny Can't Encrypt" ist zwar schon 20 Jahre alt, doch Experten halten ihn immer noch für aktuell. In dieser Arbeit von Alma Whitten und J. D. Tygar geht es um die Frage, wie ein Durchschnittsanwender („Johnny") im praxisnahen Test das Verschlüsseln von E-Mails bewältigt. Das Ergebnis ist ernüchternd: Johnny ist mit dem Verschlüsseln schnell überfordert und hat obendrein kein großes Interesse daran.

Mehr Bewusstsein und neue Gesetze

Um das Verschlüsseln von E-Mails endlich populärer zu machen, hat sich inzwischen der Gesetzgeber eingeschaltet. So gibt es die Datenschutz-Grundverordnung (DSGVO) der

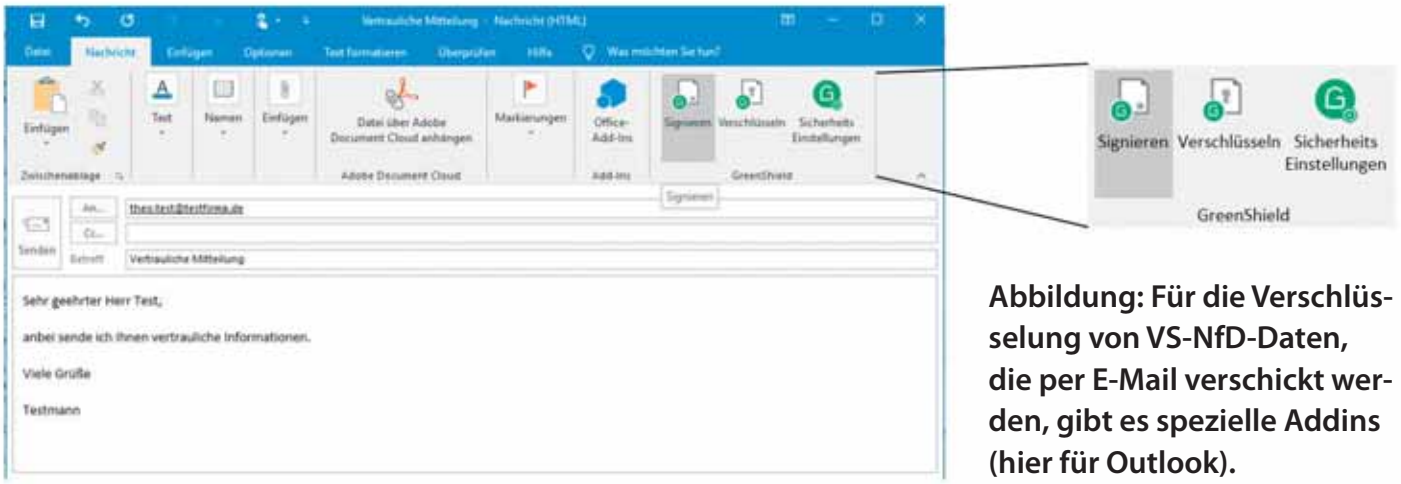


Bild: cryptovision

Abbildung: Für die Verschlüsselung von VS-NfD-Daten, die per E-Mail verschickt werden, gibt es spezielle Addins (hier für Outlook).

EU, die in einigen Bereichen nur durch das Verschlüsseln von E-Mails zu erfüllen ist. Eine Verschlüsselungspflicht besteht außerdem für Rechtsanwälte, Notare und andere Berufsgeheimnisträger – laut dem 2017 neugefassten § 203 des Strafgesetzbuchs. Auch das IT-Sicherheitsgesetz, das eGovernment-Gesetz und das eHealth-Gesetz fordern – direkt oder indirekt – das Verschlüsseln von E-Mails.

Doch Gesetze alleine werden kaum ausreichen, solange Johnny seine E-Mails weder verschlüsseln kann noch will. „Anwender-zentrierte IT-Sicherheit" heißt daher ein wichtiges Stichwort. Experten, wie die deutsche Professorin Angela Sasse von der Ruhruniversität Bochum, empfehlen Schulungen für die Anwender und fordern, dass E-Mail-Verschlüsselungs-Lösungen benutzerfreundlicher werden.

Geheimschutz-Bereich als Vorbild?

Eine Vorreiterrolle in Sachen E-Mail-Verschlüsselung könnten demnächst Behörden und Unternehmen übernehmen, die Geheimschutzanforderungen erfüllen müssen. Diese dürfen Daten bis zur Geheimhaltungsstufe „Verschlusssache – Nur für den Dienstgebrauch" (VS-NfD) verschlüsselt per Mail verschicken, sofern die dazu genutzte Lösung entsprechend zugelassen ist. Bei den von Outlook oder Notes bereitgestellten Verschlüsselungsfunktionen ist dies zwar nicht der Fall, doch es gibt Alternativen, die teilweise zusätzliche Vorteile bieten.

„E-Mail-Verschlüsselung und Datei-Verschlüsselung sollte man heute als Einheit betrachten, da dies die Benutzerfreundlichkeit erhöht", fordert Markus Hoffmeister, Geschäftsführer von cryptovision. „Wenn eine verschlüsselte Datei als Mail verschickt wird, sollte der Client des Empfängers diese als verschlüsselte Mail erkennen."

Eine Lösung, die so arbeitet und außerdem VS-NfD-zugelassen ist, ist das cryptovision-Produkt GreenShield (siehe Abbildung).

Es könnte also durchaus sein, dass sich E-Mail-Verschlüsselung demnächst im Geheimschutz-Segment durchsetzen wird. Es bleibt zu hoffen, dass diese Entwicklung auch auf andere Bereiche überspringt. Wer weiß, vielleicht erscheint dann schon bald eine neue Forschungsarbeit. Möglicher Titel: „Why Johnny Finally Can Encrpypt". □

Der Autor

Bild: cryptovision

Klaus Schmeh ist Berater bei der cv cryptovision GmbH.

E-Mail-Security: Was ist dran am Sandboxing?

Sandboxing wird oftmals als Wunderwaffe in der E-Mail-Security gepriesen. Um echten Mehrwert zu liefern, muss Sandboxing im Kanon mit anderen Technologien eingesetzt werden. In diesem Artikel werden Chancen und Limitationen von Sandboxing erläutert und ein sinnvolles Einsatzszenario beschrieben.

Von Stefan Cink, Net at Work

Bild: natali_mis/stock.adobe.com

Sandboxing wird in verschiedenen Anwendungsfällen mit unterschiedlichen Anforderungen genutzt. In der E-Mail-Security besteht – vereinfacht gesagt – „nur" die Anforderung, eine E-Mail bzw. Anhänge an die Sandbox zu übergeben und möglichst schnell eine positive oder negative Einschätzung zu erhalten. Hat die E-Mail-Security-Infrastruktur eine E-Mail mit Links und/oder Anhängen als verdächtig ausgemacht und beauftragt die Sandbox mit der Prüfung, gaukelt das Sandbox-System dann den Links und Anhängen quasi vor, sie wären dem Empfänger bereits zugestellt, befänden sich jetzt auf dem Client und der Nutzer würde die Anhänge und Links öffnen. Nun wird beobachtet, ob schädliches Verhalten wie beispielsweise das Laden von Schadsoftware auftritt. Geschwindigkeit ist dabei Trumpf, und das Sandboxing muss vollständig automatisiert ablaufen. Sandboxing ist also eine weitere Schutzebene für E-Mail-Sicherheit, die vor allem der Abwehr von Zero-Day-Angriffen, gezielten Angriffen und Advanced Persistent Threats dient.

Limitationen und Schwachstellen von Sandboxing

Im Prinzip eine feine Sache, wären dabei nicht – wie so oft selbst bei sehr komplexen IT-Security-Systemen – die unvermeidlichen Limitationen und Schwachstellen. Die vier wichtigsten Limitationen von Sandboxing in der E-Mail-Security sind:

1. Methoden zur Erkennung einer Sandbox

Professionelle Hacker nutzen einen bunten Strauß an Technologien zur Erkennung traditioneller Sandbox-Umgebungen. Einfache Indikatoren sind das Fehlen verbundener Devices wie Drucker, Unterschiede zwischen physikalischem und virtuellem System (beispielsweise in der Anzahl der Rechenkerne) oder das Fehlen bestimmter Dateien. So nutzte beispielsweise die bekannte Ransomware Locky die Datei run32dll.exe, die in damaligen Sandbox-

Umgebungen nicht verfügbar war. Fehlte die Datei, blieb das schadhafte Verhalten aus und die Prüfung ergab keine Beanstandungen. Auch hier werden die Methoden immer raffinierter: Unlängst wurde die unterschiedliche Laufzeit von Calls zur Windows API ausgenutzt, um eine virtuelle Sandbox-Umgebung zu erkennen.

2. Methoden zum Umgehen einer Sandbox

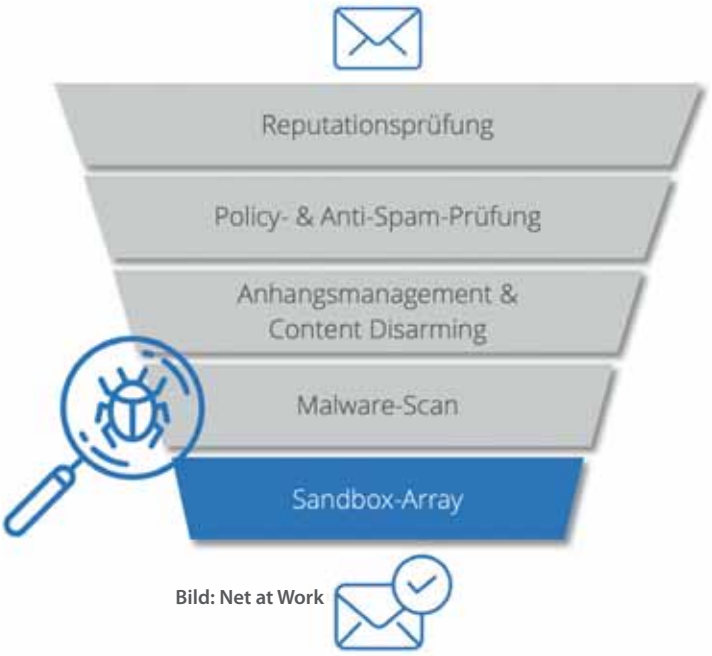
Ein anderer Weg ist die Verhinderung der Prüfung. Ein schlichter Ansatz hierfür ist die Verzögerung der Ausführung des Schadcodes um mehrere Tage oder die Ausführung zu einem bestimmten Zeitpunkt in der Zukunft. Weiterhin wird Verschlüsselung von Code genutzt, um Analysen zu verhindern. Der bekannte Trojaner Emotet wiederum nutzte in einer seiner vielen Ausprägungen die Möglichkeit, Schadcode in File-Formaten zu transportieren, die in der Sandbox nicht ausgeführt werden können, da sie nicht unterstützt werden.

3. Die falsche Sandbox im richtigen Moment

Unterschiedliche Versionen und Ausprägungen von Betriebssystemen, Laufzeitumgebungen, Hilfsprogrammen und Anwendungen sorgen für eine Kombinationsvielfalt von Rechnerumgebungen, die nahezu unendlich ist. Selbst in Organisationen mit striktem Client Management muss die Sandbox-Umgebung ein breites Spektrum an Konfigurationen abbilden, damit sie wirksam prüfen kann. Dabei entsteht prinzipbedingt eine Sicherheitslücke dadurch, dass eine Attacke womöglich gerade die Kombination ausnutzt, die von der aktuellen Sandbox-Umgebung nicht geprüft wird.

4. Aufwand an Zeit und Rechenleistung

Die Prüfung eines E-Mail-Anhangs mit einer Sandbox dauert typischerweise eher Minuten als Sekunden. Beim gängigen E-Mail-Aufkommen selbst in Organisationen mittlerer Größe würde die Sandbox-Prüfung schnell zum Flaschenhals in der Performance der E-Mail-Infrastruktur werden, wenn jedes Attachment bzw. jeder Link mit der Sandbox geprüft werden müsste.



In Kombination mit anderen Mechanismen kann Sandboxing intelligent eingesetzt werden.

Aus den beiden erstgenannten Limitationen wird deutlich, dass auch Sandbox-Hersteller sich ein ständiges Hase-und-Igel-Spiel mit den Angreifern liefern. Sandbox-Ansätze allein können keinen vollständigen Schutz bieten. Dennoch können sie ein wertvoller Baustein in einer gestaffelten Kette von Schutzelementen sein, wenn man sie denn richtig einsetzt.

Net at Work setzt als Technologie für den Einsatz in der E-Mail-Security ein cloudbasiertes Sandbox-Array ein. Die parallele Nutzung von multiplen Sandboxes in der Cloud hilft zum einen dabei, Performance-Engpässe zu vermeiden und bietet gleichzeitig die Möglichkeit, ein breites Spektrum an Konfigurationen parallel zu prüfen. Weiterhin können durch die übergreifende Schwarm-Intelligenz des Cloud-Anbieters Informationen zu neuen Varianten von Schadsoftware schnell über alle Kunden hinweg ausgetauscht werden.

Sinnvoll: Kombination mit anderen Schutzmethoden

Der Schlüssel zum Erfolg beim Sandboxing liegt jedoch in der Kombination mit anderen ⇨

Methoden zum Schutz vor E-Mail-basierter Malware. In einer kaskadierenden Folge kommen so verschiedene Prüfmethoden zum Einsatz. Dabei sollte auf zwei Methoden besonders Wert gelegt werden, weil sie einen sinnvollen und wirksamen Sandbox-Einsatz ermöglichen:

1. Content Disarm & Reconstruction (CDR) sorgt für saubere Anhänge

Mit Funktionen zum Anhangsmanagement werden notorisch als unsicher bekannte Dateiformate wie Word, Excel oder PDF regelbasiert und automatisiert in unkritische PDF-Dateien umgewandelt. Dabei bleibt potenziell vorhandener Schadcode außen vor und dem E-Mail-Empfänger wird so ein garantiert ungefährlicher Anhang zugestellt. Im PDF-Dokument findet sich eine Vorschaltseite, auf der individuelle Hinweise zum Grund der Konvertierung vorhanden sind und – sofern gewünscht – auch ein Link zum Originaldokument, das sich in einer speziellen Quarantäne befindet. So kann sich der User zunächst einen Überblick verschaffen, was der Inhalt der zugesandten Anhänge ist.

2. Konsequente Reputationsbewertung steuert den gesamten Prozess

Diese Methode hat sich als wichtigstes Instrument in der E-Mail-Security herauskristallisiert. Sie basiert auf zwei Säulen: Zunächst werden alle verfügbaren technischen Kriterien für die Reputation eines Absenders genutzt. Als wichtige Stichworte sind hier die mittlerweile robusten – wenn auch leider immer noch sträflich wenig genutzten – Standards SPF, DKIM und DMARC zu nennen. Kombiniert wird dies mit der zweiten Säule: der Auswertung der bisherigen Kommunikationshistorie mit dem Absender. Grob vereinfacht, erkennt das Reputationsmanagement, mit wem in der Vergangenheit bereits kommuniziert wurde. Beide Säulen bieten die Grundlage für ein selbstlernendes Whitelisting mit fundierter Einschätzung zur Seriosität des Absenders. Kombiniert man diese Ansätze nun mit Sandboxing, kann man es wirklich intelligent einsetzen. Dazu werden entsprechende Regeln formuliert und automatisiert umgesetzt. Erreicht beispielsweise eine E-Mail mit Office-Anhängen von einem unbekannten Absender das Secure-Mail-Gateway, wird dem Nutzer über das Anhangsmanagement eine ungefährliche PDF-Version zugestellt. Sollte der Nutzer die Originaldatei anfordern, kann für sie ein Sandboxing angestoßen werden. Die Laufzeit des Sandboxing ist dann unkritisch und so kann eine wirklich gründliche Prüfung erfolgen.

Als weiteres Beispiel können E-Mails mit Anhängen, deren Format in der Sandbox nicht ausgewertet werden kann, bei einem wohlbekannten Absender mit hoher Reputation zugestellt werden, während sie bei Absendern mit niedriger Reputation abgewiesen werden. Eine weitere Regel könnte auffällige E-Mails von an sich vertrauenswürdigen Sendern bewusst dem Sandboxing zuführen.

Den Beispielen gemein ist, dass die Nutzung der zeit- und ressourcenaufwändigen Sandbox-Prüfungen auf eine kleinere Zahl an wirklich sinnvollen bzw. kritischen Fällen fokussiert wird. Für die notwendige fein abgestimmte Steuerung der Schutzfunktionen ist die Qualität der Reputationsbewertung ausschlaggebend. □

Der Autor

Bild: Net at Work

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

INFRASTRUKTUR & AUTOMATISIERUNG

Meet the DC-Experts

Hartwig Bazzanella
VIRZ e.V.

Zukunftsfähige Datacenter-Infrastrukturen für die Smart City

Mark Hlawatschek
ATIX

IT Automation – der Treiber für Innovation

Erik Rylander
Stockholm Exergi

Integrating data centers in the modern sustainable city

Rainer Schwemmer
CERN

Modulare Data Center für Hochenergiephysik

Eine Veranstaltung der VOGEL IT AKADEMIE

DC DATACENTER DAY 2019

22. Oktober, VCC Würzburg

Kostenfreies VIP-Ticket sichern!

www.dc-day.de/vip

Platin-Partner

Premium-Partner

Classic-Partner

Basic-Partner

Medien- & Technologie-Partner

Auf dem Weg in eine neue Galaxie: Ergreifen Sie bei der Migration auf S/4HANA auch die Chance auf ein ganzheitliches Update der Sicherheit und Compliance Ihrer SAP-Systeme.

Bild: akquniet

Ergreifen Sie die Chance!

Warum Sie die S/4HANA-Migration nutzen sollten, um die Sicherheit und Compliance Ihrer SAP-Systeme neu aufzustellen.

Von Bodo Kahl, CEO SAST SOLUTIONS der akquinet AG

Eine der aktuell größten Aufgaben für SAP-Verantwortliche ist die anstehende Migration auf S/4HANA. Dabei werden wichtige Themen oftmals komplett außer Acht gelassen. Ich war ehrlich gesagt erschrocken, als ich hörte, wie wenig Unternehmen sich im Rahmen der Umstellung, die ja jedem bis 2025 bevorsteht, Gedanken um die Sicherheit und Compliance ihrer Systeme machen: nur rund ein Viertel aller Betroffenen. Das ist grob fahrlässig, denn die Unterschiede zwischen SAP ERP und S/4HANA sind deutlich größer als erwartet und keine der bislang getroffenen Sicherheitsmaßnahmen lassen sich einfach auf das neue System übertragen.

Für mich sind zwei Punkte wichtig, die jeder IT-Verantwortliche bei der Migration auf S/4HANA berücksichtigen sollte:

1. Räumen Sie vorher auf!

Es ist wie bei jedem Umzug: Räumen Sie auf, bevor die Möbelpacker vor der Tür stehen und befreien Sie Ihre Systeme von Altlasten. Denn das bestehende Berechtigungskonzept kann zum Beispiel nicht eins zu eins übernommen werden. Auf den

Punkt gebracht ist ohne ein Redesign Ihrer Berechtigungen keine S/4HANA-Migration möglich. Die zweite Baustelle befindet sich im ABAP-Code – ein umfangreiches Projekt, denkt man an durchschnittlich ca. zwei Millionen Zeilen kundeneigenen Codes, von dem etwa 70 % obsolet sind. Unsere Software, die innerhalb kürzester Zeit einsatzfähig und von SAP dreifach zertifiziert ist, sowie unsere erfahrenen SAST-Experten unterstützen Sie gerne dabei.

2. Denken Sie von Anfang an ein umfangreiches Sicherheitskonzept mit!

Das beginnt mit einem initialen Security Audit als ersten wichtigen Schritt zur Härtung des Zielsystems. Hieraus resultiert ein umfangreicher Bericht der gefundenen Schwachstellen mit konkreten Handlungsempfehlungen für die Systemhärtung. Darauf basierend sollten die folgenden Ebenen abgesichert und mittels Echtzeitüberwachung kontinuierlich überprüft werden: Betriebssystem, Netzwerk, Datenbank sowie SAP-Basissystem.

Also: Lassen Sie die Chance nicht verstreichen und nutzen Sie die S/4HANA-Migration für eine Verbesserung Ihrer SAP Security & Compliance, im Idealfall mit einem Partner, der bei Sicherheit & Compliance auf jahrelange Erfahrung zurückblicken kann. ■

Bodo Kahl ist Geschäftsführer SAST SOLUTIONS der akquinet AG. Er arbeitet mit seinem Team für rund 200 Kunden im SAP Security & Compliance-Umfeld.

Bild: akquinet

Die SAST SOLUTIONS bieten eine Portfoliokombination aus Software, Beratung und Service – somit ganzheitliche Lösungen für SAP Security & Compliance

SAST SOLUTIONS / akquinet AG

Paul-Stritter-Weg 5

22297 Hamburg

Telefon: +49 40 88 173-109

E-Mail: sast@akquinet.de

www.sast-solutions.de

www.sast-blog.akquinet.de

@SastSolutions (SAST auf Twitter)

Das SAST SOLUTIONS-Portfolio von akquinet bietet neben der eigenentwickelten Software Suite auch Security & Compliance Consulting sowie Managed Services an. Weltweit vertrauen Unternehmen auf die SAST SOLUTIONS, um ihre SAP ERP- und S4/HANA-Systeme vor Hackerangriffen, Spionage und Datendiebstahl zu schützen. Die gesamte SAST SUITE ist von SAP dreifach zertifiziert für NetWeaver, SAP HANA und S/4HANA.

SAST

Digitale Zertifikate effektiver verwalten

IoT, Industrie 4.0 und Digitalisierung sind Schlüsselbegriffe für die nächste große industrielle Revolution. Die global vernetzte Welt muss zur Sicherheit aller Teilnehmer höchste Ansprüche an den Schutz sensibler Daten und ihrer Infrastruktur im Allgemeinen stellen.

Von Daniel Dyroff, eCom Service IT

Identitätsmanagement auf der Metaebene der Anwender ist ein erster Schritt in Richtung einer sicheren Infrastruktur. Das Verschlüsseln von Geräten als den eigentlich neuralgischen Punkten ist allerdings weitaus elementarer. Genau hier liegt die Herausforderung, da aufgrund der Komplexität bisher gar keine oder nur wenige Anstrengungen für ein adäquates Zertifikatsmanagement unternommen wurden. Auch wenn neue Technologien theoretisch zur Verfügung stehen – Stichwort Blockchain –, werden am Ende weiterhin Schlüssel und Zertifikate in der über Jahre heterogen gewachsenen IT-Infrastruktur der einzelnen Marktteilnehmer eine zentrale Rolle spielen.

Beherrschen komplexer Umgebungen

Für die Administration von Public-Key-Infrastrukturen (PKI) mit einer Vielzahl an Geräten und Usern sind die üblichen Bordmittel nicht ausreichend. Die Auslieferung der Schlüssel und Zertifikate ist aktuell mit einem hohen administrativen Aufwand verbunden. Anforderungen können zum Teil in der Praxis gar nicht umgesetzt werden. Ein PKI-Administrator steht immer wieder vor derselben Frage: „Warum nur hat alles, was mit Zertifikaten zu tun hat, eine so kurze Gültigkeitsdauer?“ Dies äußert sich vor allem immer wieder in SmartCards mit denen sich die Nutzer nicht mehr anmelden können.

Ein Tool mit passendem Service

Der Einsatz von zusätzlicher Software muss sich über eine klar strukturierte, benutzerfreundliche und plattformunabhängige Benutzeroberfläche gestalten. So kann der Workflow des Lebenszyklusmanagements eines Gerätezertifikats deutlich verschlankt werden.
Administrationsprozesse lassen sich intuitiv über assistentengestützte Dialoge durchführen. Zusätzlich sorgt die Möglichkeit, Menüpunkte abhängig von der Verwaltungsrolle auszublenden für mehr Übersicht und damit auch für weniger Bedienungsfehler. Prozesse werden dadurch auf das Notwendige reduziert.
Bisher müssen sich Administratoren im PKI-Bereich immer wieder ärgern über unerwartet abgelaufene Zertifikate, eine Sperrliste, die nicht aktuell ist, oder veraltete Zertifikate, welche immer noch ihre PKI-Systeme und Directorys füllen. Ein weiteres Ärgernis sind Pre-Shared Keys und Serversysteme mit fraglichem Self-Sign-Zertifikat. Aber am schwersten wiegt für PKI-Administratoren, dass der Browser beim administrativen Zugriff auf die Devices eine Sicherheitswarnung ausgibt, welche aktiv umgangen werden muss.

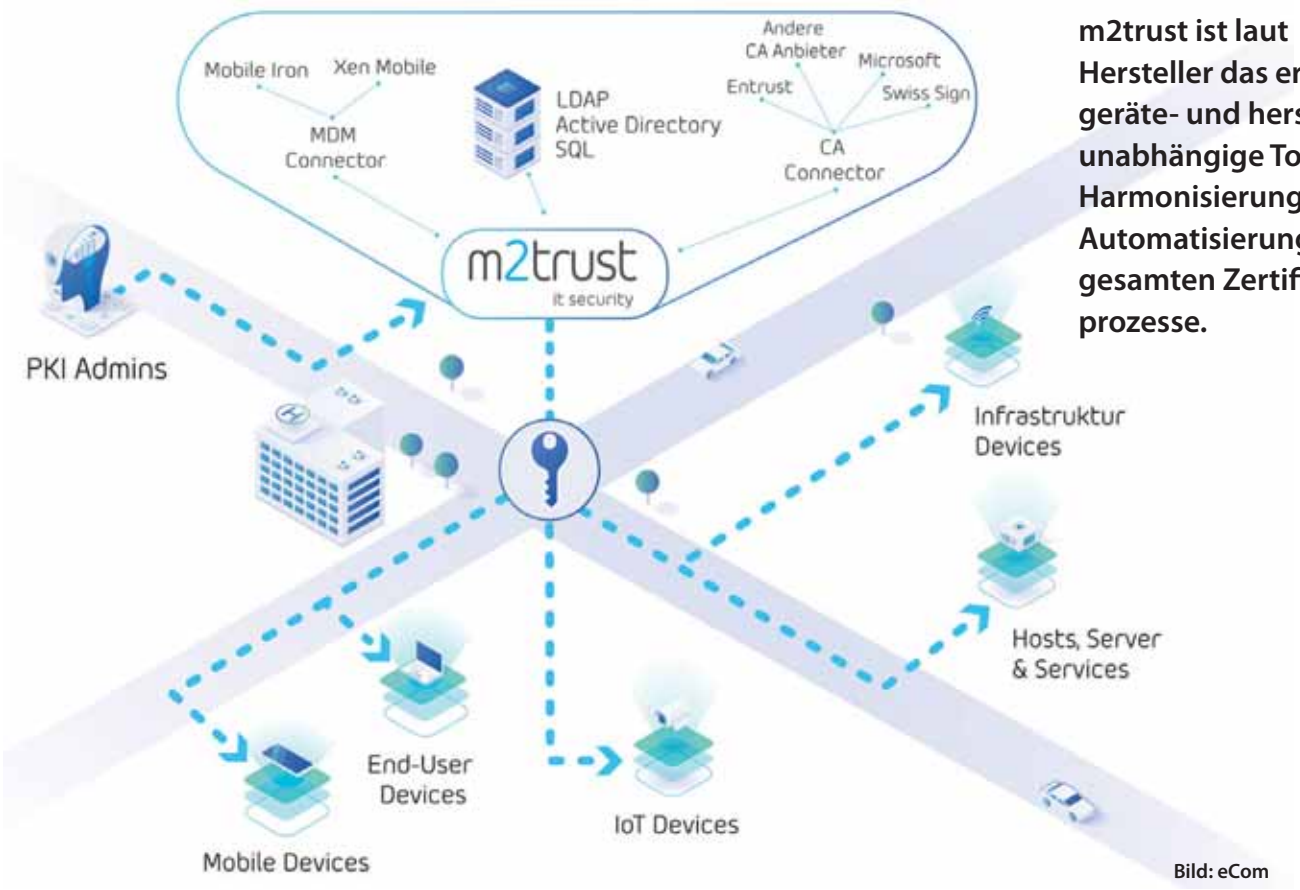


Bild: eCom

m2trust ist laut Hersteller das erste geräte- und hersteller-unabhängige Tool zur Harmonisierung und Automatisierung der gesamten Zertifikats-prozesse.

Durch Funktionen wie die Automatisierung der Zertifikatsverwaltung und die Integration von unterschiedlichen Betriebssystemen über die Certificate Authorities (CA) Connectoren können sämtliche Drittanbieter in die zentrale Zertifikatsverwaltung eingebunden werden. Mit dem MDM Connector wird die Aufbringung und Verwaltung von Zertifikaten auf mobilen Endgeräten automatisierbar. Über eine browserbasierte Benutzeroberfläche lassen sich automatische Aktionen als Folge von definierbaren Ereignissen konfigurieren. Dies und eine Vielzahl von Schnittstellen ermöglichen die Harmonisierung der verschiedenen heterogenen Betriebssysteme.

Vielfältige Anwendungsbereiche

Heutige heterogen gewachsene IT-Landschaften stellen ein effektives Zertifikatsmanagement vor große Herausforderungen. Neben Softwarelösungen von unterschiedlichen Anbietern, muss auch eine Vielzahl unterschiedlicher Geräte und deren Betriebssysteme nahtlos in die unternehmenseigene Public-Key-Infrastruktur eingebunden werden. Ein Beispiel ist hier das Widerrufen von Zertifikaten für mobile Endgeräte bei Verlust oder einem Gesellschaftswechsel durch einen Mitarbeiter. Auch die rechtzeitige Erneuerung des Gerätezertifikats ist über den Mobile Device Management (MDM) Connector automatisch abbildbar.

Automatisierte Lösungen für solche Anwendungsfälle existieren hier im Grunde nicht, weshalb eine konsequente Durchsetzung der Corporate Compliance sowie ein reibungsloser Betrieb oftmals kaum realisierbar ist.

An dieser Stelle muss es über unterschiedlichste Schnittstellen ermöglicht werden, den kompletten Zertifikatslebenszyklus – gerade in solchen IT-Landschaften – automatisch abzubilden. So lässt sich über diverse Connectoren auch Software von Drittherstellern anbinden ⇨

und für das im Unternehmen eingesetzte Zertifikatsmanagement, über ein Webservice-Interface nutzbar, machen.

Über die Zertifikatsverwaltung lassen sich dadurch vollumfänglich Zertifikatsbeantragungen, -erneuerungen und -sperrungen durchführen. Des Weiteren können Schlüssel und Zertifikate sicher wiederhergestellt und Zertifikatsinformationen abgerufen werden. Zertifikatsprofile müssen automatisch abgeglichen und synchronisiert werden. Für eine lückenlose Dokumentation sorgen weitreichende Protokollierungs- und Auditfunktionen.

Prozesse werden vollständig auf Basis von Verzeichnisänderungen automatisiert. Ohne weiteren manuellen Eingriff werden solche Ereignisse erkannt und entsprechende flexibel konfigurierbare Aktionen und Prozesse im Zertifikatsmanagement ausgelöst. Zertifikatsobjekte und Profile, die sich im Verzeichnisdienst und in der Zertifikatsdatenbank befinden, werden effektiv gesäubert und konsistent gehalten. Das bedeutet auf Anwenderseite weniger Aufwand und geringere Supportkosten.

Der bisher hohe Aufwand für das Aufbringen und Verwalten von Zertifikaten auf mobilen Endgeräten wird durch den Einsatz des MDM Connector signifikant reduziert. Durch die Integration des MDM ins Zertifikatsmanagement laufen die Zertifikatslebenszyklusprozesse für mobile Endgeräte selbstständig ab. Die erforderlichen Verzeichniskonten für jedes Endgerät mit provisionierten Zertifikaten werden automatisch erzeugt oder können alternativ auf ein gemeinsames Dienstekonto eingebunden werden.

In der Praxis wird häufig mit heterogenen Systemen gearbeitet. Das hat teilweise historische, teilweise praktische Gründe. Für die Integration dieser heterogenen Systemlandschaften mit ihren unterschiedlichen Endgeräten und Betriebssystemen, kommt wieder ein Connector zum Einsatz, um diese optimal in die Zertifikatsverwaltung einzubinden. Darüber hinaus automatisiert der Connector wichtige Betriebsaufgaben. So lassen sich Zertifikate automatisch für Microsoft, Linux und Macintosh, aber auch für Drucker und IP-Telefone ausstellen, erneuern und sperren.

Zusammenfassung

Digitale Zertifikate sind ein elementarer Bestandteil für die Sicherheit von Unternehmen und deren IT-Infrastruktur in einer vernetzten Welt. Die Zertifikatsverwaltung erfordert ab einer bestimmten Komplexität den Einsatz spezieller Software. Administratoren können nur mit Hilfe von Software das Potenzial der jeweiligen Plattform für das Zertifikatmanagement effektiver nutzen, Prozesse automatisieren und Kosten senken. Darüber hinaus werden sie in die Lage versetzt, unterschiedliche Produkte mit den unterschiedlichsten Betriebssystemen in die Public-Key-Infrastruktur einzubinden und deren Standards zu harmonisieren. Im Ergebnis bedeutet dies weniger Aufwand sowie mehr Sicherheit, Compliance und zufriedenere Nutzer. Langfristig muss ein Service inklusive einer entsprechenden Cloudlösung die Lücke beim Management der Gerätezertifikate in der PKI-Architektur der Unternehmen schließen. Dieser Prozess geht Hand in Hand mit dem allgemeinen Trend zur Cloud und nähert sich dem Traum der „One Click"-Serviceerweiterung zumindest an, auch wenn eine solche Lösung nicht möglich sein wird. □

Der Autor

Daniel Dyroff ist Projektmanager bei der eCom Service IT GmbH.

Bild: eCom

NETFILES

Virtueller Datenraum

Sicherer und Compliance-gerechter Datenaustausch mit Kunden und Geschäftspartnern

Einfach

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

Sicher

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

Bewährt

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

www.netfiles.de

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

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

Worauf man bei der Zertifizierung von IoT-Produkten achten muss

Gerade im Bereich Sicherheit fehlen Anwendern viele Informationen bei Lösungen im Internet of Things. Doch es gibt bereits eine Reihe von Standards und Zertifizierungen für das IoT, weitere werden hinzukommen. Wir geben einen Überblick und sagen, worauf es ankommt.

Von Oliver Schonschek

Sicherheitsstandards sind ein erster Schritt zur IoT-Security, doch damit alleine ist es nicht getan.

Bild: Murrstock/stock.adobe.com

Viele Unternehmen sind nicht in der Lage, Sicherheitsverletzungen an IoT-Geräten zu erkennen. Zu den Top IoT-Sicherheitsbedenken zählen schwache Standard-Anmeldeinformationen, Klartext-HTTP-Kommunikation zu einem Server für Firmware- oder Paket-Updates, Klartext-HTTP-Authentifizierung und die Nutzung veralteter Bibliotheken.

Anwenderunternehmen und Nutzern wäre zweifellos geholfen, wenn es mehr Informationen zur Sicherheit von IoT-Lösungen gäbe, nicht nur über Risiken und Schwachstellen, sondern auch über die tatsächlich vorhandenen Sicherheitseigenschaften. Zusätzlich wäre es nicht nur für den normalen Anwender wichtig, einen Hinweis zu bekommen, ob die verfügbaren Sicherheitsfunktionen bei einem IoT-Produkt ausreichen – und wenn ja, für welchen Schutzbedarf.

Dabei genügt es nicht, die eigenen IoT-Lösungen im Blick zu haben, wie eine Studie des Ponemon Institutes zum Risiko Dritter für das Internet der Dinge zeigt. Ponemon meldet eine dramatische Zunahme von IoT-bezogenen Datenschutzverletzungen, insbesondere aufgrund eines ungesicherten IoT-Geräts oder einer ungesicherten IoT-Anwendung. Waren es 2017 noch 15 Prozent sind es jetzt bereits 26 Prozent. Die wirklichen Ergebnisse sind möglicherweise sogar höher, da die meisten Unternehmen nicht über jedes ungesicherte IoT-Gerät oder jede ungesicherte IoT-Anwendung in ihrer Umgebung oder von Drittanbietern informiert sind.

Viele IoT-Risiken, aber auch viele IoT-Sicherheitsstandards

Neben den vielen Risiken, die es rund um das Internet der Dinge zu beachten gilt, gibt es auch

eine Vielzahl an Empfehlungen und sogar Standards im Bereich IoT-Sicherheit. Einige Beispiele sind:

- Das Deutsche Institut für Normung (DIN) hat mit der DIN SPEC 27072 eine Spezifikation zur Informationssicherheit von IoT-fähigen Geräten veröffentlicht. Konkret fordert die DIN SPEC 27072 u.a. eine sichere Update-Funktionalität, eine im Initialzustand nach Inbetriebnahme verpflichtende Authentisierung vor Zugriffen über eine IP-Schnittstelle und verbietet die Nutzung von Standardpasswörten im Netzwerkbetrieb. Untermauert werden diese Anforderungen durch die verpflichtende Nutzung kryptographischer Verfahren nach dem Stand der Technik.
- Zudem gibt es den „Code of Practice for consumer IoT security“ sowie die Technische Spezifikation „Cyber Security for Consumer Internet of Things“ von der Standardorganisation ETSI.
- Weiterhin haben die Mitglieder des Industrial Internet Consortium (IIC) den „Security Maturity Model (SMM) Practioner's Guide“ entwickelt. Der Leitfaden unterstützt IoT-Betreiber bei der Einschätzung ihres aktuellen und anvisierten Security-Reifegrads.

Sowohl für die Anbieter von IoT-Lösungen als auch für die Anwender ist es entscheidend, dass sich mehr Transparenz im IoT bildet, aber auch bei den Standards und Empfehlungen. Viele verschiedene Spezifikationen erschweren die Vergleichbarkeit und Interpretation der IoT-Sicherheit.

Die EU-Agentur für Cyber-Sicherheit ENISA hat sich IoT-Sicherheitsstandards angesehen und kam zu folgendem Schluss:

- Eine ENISA-Analyse, bei der die bestehenden Standards mit den Anforderungen an Sicherheit und Datenschutz im Bereich des Internet der Dinge abgeglichen wurde, ergab, dass keine signifikante Standardlücke besteht – jede Anforderung kann von einem bestehenden Standard erfüllt werden. Während Standards für viele verschiedene Elemente existieren, um ein Gerät oder einen Dienst sicher zu machen, bezieht sich der Begriff IoT auf ein Ökosystem, das nicht nur Geräte und Dienste umfasst. Darüber hinaus erfordern der Anwendungskontext von IoT, seine hohe Skalierbarkeit und andere Merkmale weitere flexible Ansätze.
- Die Sicherheitslücke bei IoT-Gerätestandards besteht darin, dass die Standards nicht ganzheitlich behandelt werden. Daher ist es möglich, ein Gerät auf den Markt zu bringen, das seinen Benutzer authentifizieren, gesendete und empfangene Daten verschlüsseln und entschlüsseln, den Integritätsnachweis liefern oder verifizieren kann, das jedoch weiterhin unsicher ist und bleibt.

Worauf es bei IoT-Sicherheitszertifizierungen ankommt

Die Sicherung des Internet der Dinge ist mit einem einheitlichen Ansatz nicht möglich – und jede Art von vernetztem Objekt muss individuell bewertet werden. Das IoT erscheint als zu komplex und zu vielschichtig für eine einheitliche Sicherheitsempfehlung und Sicherheitszertifizierung. Dann aber wäre es wichtig, einen Basisschutz für IoT-Geräte zu definieren, was bereits mehrfach erfolgt ist, diesen Basisschutz aber auch auf alle IoT-Geräte anzuwenden, die Einhaltung zu zertifizieren und ganz deutlich zu machen, dass weitere Sicherheitsmaßnahmen je nach IoT-Lösung erforderlich sein können.

Betrachtet man die Schwachstellen und Mängel in der IoT-Sicherheit, sind dies oftmals Punkte, die unter das Thema Basisschutz fallen. Mit Zertifikaten, die diesen nachweisen, wäre also der Transparenz im Internet of Things deutlich geholfen. Die IoT-Sicherheit braucht allerdings je nach Schutzbedarf und konkretem Anwendungsgebiet noch weitere Maßnahmen, also auch weitere Zertifizierungsstufen. □

IT SECURITY ‚MADE IN GERMANY'
NOSPAMPROXY

WWK nutzt NoSpamProxy zur E-Mail-Verschlüsselung und schützt damit Kundendaten im Sinne der EU-DSGVO

Flexible Verschlüsselungslösung sichert die datenschutzkonforme E-Mail-Kommunikation der WWK Versicherungsgruppe mit ihren zahlreichen Partnern. Die weitgehende Automatisierung der Zertifikatsverwaltung erleichtert den Roll-Out sowie den Betrieb.

WWK
Eine starke Gemeinschaft

Datenschutz als Basis für Vertrauen

Vertrauen ist das Fundament einer jeden Geschäftsbeziehung in der Versicherungsbranche. Der sichere und vertrauensvolle Umgang mit Daten der Versicherungsnehmer und Partner ist somit eine unumgängliche Grundvoraussetzung. Auch die WWK Versicherungsgruppe fühlt sich diesem Grundsatz verpflichtet. Vor diesem Hintergrund war die Umsetzung der EU-Datenschutzgrundverordnung (EU-DSGVO) für die WWK selbstverständlich.
Da immer mehr Daten mit Geschäftspartnern über E-Mail-Kommunikation ausgetauscht werden, entschied sich die WWK für die umfassende Einführung von E-Mail-Verschlüsselung, um eine datenschutzkonforme E-Mail-Kommunikation umzusetzen.

NoSpamProxy unterstützt auch Kommunikationspartner ohne eigene Verschlüsselungstechnik

Heute schützt NoSpamProxy nicht nur die E-Mail-Kommunikation der 3.000 internen Nutzer, sondern steht auch den über 10.000 Vertriebspartnern zur Verfügung. Dies erfordert eine

hohe Flexibilität bezüglich der unterschiedlichen Infrastrukturen bei den Kommunikationspartnern. Dazu bietet NoSpamProxy für die Verschlüsselung verschiedene Verfahren je nach Reifegrad der Infrastruktur auf der Empfängerseite. Hat der Empfänger keine Infrastruktur zur E-Mail-Verschlüsselung, können E-Mails auch automatisiert in geschützten Containern als PDF-Mail verpackt bereitgestellt werden, die vom Empfänger freigeschaltet werden können. Dieses Verfahren ist narrensicher und erfordert keinerlei Administrationsaufwand auf Seiten der WWK. Letzteres ist vor allem mit Blick auf die Menge der externen Kommunikationspartner unerlässlich.

Integration mit GlobalSign Managed PKI automatisiert die Zertifikatsverwaltung

Die Integration der GlobalSign Managed PKI mit NoSpamProxy automatisiert die Zertifikatsverwaltung und hält so den Administrationsaufwand minimal. Die Zertifikate der einzelnen User werden bei Bedarf durch NoSpamProxy über eine API-Anbindung an GlobalSign angefordert und sofort ausgestellt. Alle Zertifikate und Schlüssel werden zentral verwaltet, so dass es clientseitig keine Administrationsaufwände gibt. Aus diesem Ansatz ergab sich auch die äußerst zügige Umsetzung des Projektes:
Nach Einrichtung und Testen der Komponenten erfolgte der Roll-Out der neuen Lösung an die rund 3.000 Nutzer und Gruppenpostfächer innerhalb von nur 14 Tagen.

> „Mit NoSpamProxy konnten wir die Anforderungen der EU-DSGVO an eine datenschutzkonforme E-Mail-Kommunikation einfach umsetzen. Der Aufwand im Roll-Out und in der laufenden Administration reduzierte sich auf ein Minimum. Der Support ist hervorragend und auch unsere Sonderwünsche wurden zügig umgesetzt

Marcus Bethmann, IT-Systemadministrator Groupware & Identity Services bei der WWK Versicherungsgruppe

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

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

Die Videoüberwachung bleibt weiterhin ein Brennpunkt beim Thema Datenschutz.

Bild: Production Perig/stock.adobe.com

Videoüberwachung nach DSGVO

Die Anwendung des neuen Datenschutzrechts auf Datenschutz-Klassiker wie die Videoüberwachung fällt Unternehmen schwer. Orientierungshilfen der Aufsichtsbehörden und neue Gerichtsurteile zeigen den Weg, der Blick in das deutsche Bundesdatenschutzgesetz (BDSG-neu) jedoch nicht. Unternehmen sollten sich hier nicht verwirren lassen, sonst kann es zu Fehlern im Datenschutz kommen.

Von Oliver Schonschek

Auf weiterhin sehr hohem Niveau liegt die Anzahl der Petitionen zur Videoüberwachung, so der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern in seinem 14. Tätigkeitsbericht, der im Mai 2019 veröffentlicht wurde. Oft werde nicht bedacht, dass eine Videoüberwachung öffentlich zugänglicher Räume nur unter bestimmten Voraussetzungen zulässig ist. Daran habe sich mit der Europäischen Datenschutz-Grundverordnung (DSGVO/GDPR) nicht viel geändert.

Ein berechtigtes Interesse an Videoüberwachung kann grundsätzlich angenommen werden, wenn der Zweck im Schutz vor Einbrüchen, Vandalismus oder Diebstählen besteht, sofern eine tatsächliche Gefahrenlage nachgewiesen wurde. Bei Webcams gibt es sogar noch mehr zu beachten: Webcams, die Live-Aufnahmen ins Internet übertragen, werden immer häufiger eingesetzt, so der Landesdatenschutzbeauftragte. Die Aufnahmen dieser Kameras sind einer unbestimmten Zahl von Personen

weltweit zugänglich. Sie sind daher nur dann zulässig, wenn auf den Bildern keine Personen identifizierbar sind.

Videoüberwachung durch Unternehmen

Wenn ein Unternehmen nach den Vorgaben zur Videoüberwachung sucht, hilft scheinbar die Datenschutz-Grundverordnung nicht weiter. Man findet dort keine spezifischen Regeln, wie man sie aus dem alten Bundesdatenschutzgesetz (BDSG-alt) kannte. Doch zur Freude vieler Unternehmen findet sich im neuen Bundesdatenschutzgesetz (BDSG-neu) doch wieder ein Paragraph zur „Videoüberwachung öffentlich zugänglicher Räume“ (§ 4 BDSG-neu).

Unter anderem steht dort: Bei der Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs gilt der Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein besonders wichtiges Interesse.

Sprich: Die Interessenabwägung, die vor dem Einsatz der Videoüberwachung durchzuführen ist, wird in diesen Fällen eher dazu führen, dass die Videoüberwachung erlaubt ist.

Nun muss man aber aufpassen, wann die Interessenabwägung zum Beispiel zur Wahrung des Hausrechts zum Ergebnis kommen kann, dass eine Videoüberwachung zulässig ist. Ja mehr noch, man muss zuerst einmal prüfen, ob überhaupt die Vorgaben des BDSG-neu Anwendung finden dürfen.

Videoüberwachung von privaten Stellen nur nach DSGVO

In den letzten Monaten wurde gemeldet, dass sich das Bundesverwaltungsgericht zur Anwendung der Vorgaben aus dem BDSG-neu für die Videoüberwachung durch private Stellen geäußert hat (https://www.bverwg.de/270319U6C2.18.0). Das Bundesverwaltungsgericht hatte deutlich gemacht, dass die Videoüberwachung durch private Stellen ausschließlich am europäischen Datenschutzrecht zu messen ist.

Nach Auffassung des Bundesverwaltungsgerichts regelt die Europäische Datenschutz-Grundverordnung die Videoüberwachung durch Private abschließend. Folglich ist die nationale Bestimmung in § 4 Abs. 1 S. 1 BDSG europarechtswidrig und im Ergebnis unanwendbar. Private Videokameras können daher im Ergebnis nur auf der Rechtsgrundlage des Art. 6 Abs. 1 Buchstabe f DSGVO betrieben werden. Die danach zu erfolgende Güterabwägung ist nicht durch nationales Recht modifizierbar.

Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, erklärte hierzu: „Das Vorhaben, mit dem Videoüberwachungsverbesserungsgesetz privat betriebene Videoüberwachung an öffentlichen Orten durch den Zweck der Terrorabwehr und die öffentliche Sicherheit zu legitimieren, wurde anlässlich des damaligen Gesetzgebungsprozesses aus datenschutzrechtlichen, verfassungsrechtlichen und europarechtlichen Gründen kritisiert. Das wurde nun im Ergebnis durch das Bundesverwaltungsgericht bestätigt. Die Aufgabe der Videoüberwachung zum Schutz der öffentlichen Sicherheit kann nicht auf private Betreiber übertragen werden, sondern bleibt eine Aufgabe der zur Ausübung öffentlicher Gewalt befugten staatlichen Behörden.“

Videoüberwachung erneut überprüfen

„Auch in Zukunft können nach Maßgabe der Europäischen Datenschutz-Grundverordnung private Betreiber die Schutzinteressen von dritten Personen bei der Datenverarbeitung ⇨

berücksichtigen – allerdings nicht im Rahmen einer nationalen Vorrang- und Verstärkerklausel zum Schutz der öffentlichen Sicherheit durch private Videoüberwachungsanlagen", so der Hamburger Datenschutzbeauftragte weiter.

Nach DSGVO sind die berechtigten Interessen des Kamerabetreibers oder eines Dritten mit dem Interesse bzw. den Grundrechten und Grundfreiheiten der betroffenen Personen abzuwägen. Zudem müssen die einzelnen Videokameras für die Wahrung der berechtigten Interessen des Verantwortlichen auch erforderlich sein.

Dr. Lutz Hasse, Thüringer Landesbeauftragter für den Datenschutz, kommentierte: „Bis zu dem jetzigen Urteil wurde heftig über die Anwendbarkeit des § 4 BDSG-neu diskutiert. Daher ist das Urteil sehr begrüßenswert. Es schafft nunmehr Rechtsklarheit auf nationaler Ebene im Bereich der datenschutzrechtlichen Zulässigkeit von Videoüberwachungen durch Private."

Wenn ein Unternehmen also seine Videoüberwachung gegenwärtig auf die Vorgaben des neuen Bundesdatenschutzgesetzes stützt, sollte die Interessenabwägung nochmals auf Basis der DSGVO wiederholt werden, um wirklich die datenschutzrechtlichen Voraussetzungen für eine Videoüberwachung zu erfüllen.


Bild: HmbBfDI

Prof. Dr. Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit: „Die Aufgabe der Videoüberwachung zum Schutz der öffentlichen Sicherheit kann nicht auf private Betreiber übertragen werden, sondern bleibt eine Aufgabe der zur Ausübung öffentlicher Gewalt befugten staatlichen Behörden."

Aufsichtsbehörden geben Orientierung

In den letzten Monaten haben die Aufsichtsbehörden für den Datenschutz eine Reihe von Orientierungshilfen veröffentlicht, die in aller Regel bei der jeweils zuständigen Aufsichtsbehörde im Informationsbereich zu finden sind. Solche Orientierungshilfen sind wichtige Hilfsmittel bei der Anwendung der Datenschutz-Grundverordnung.

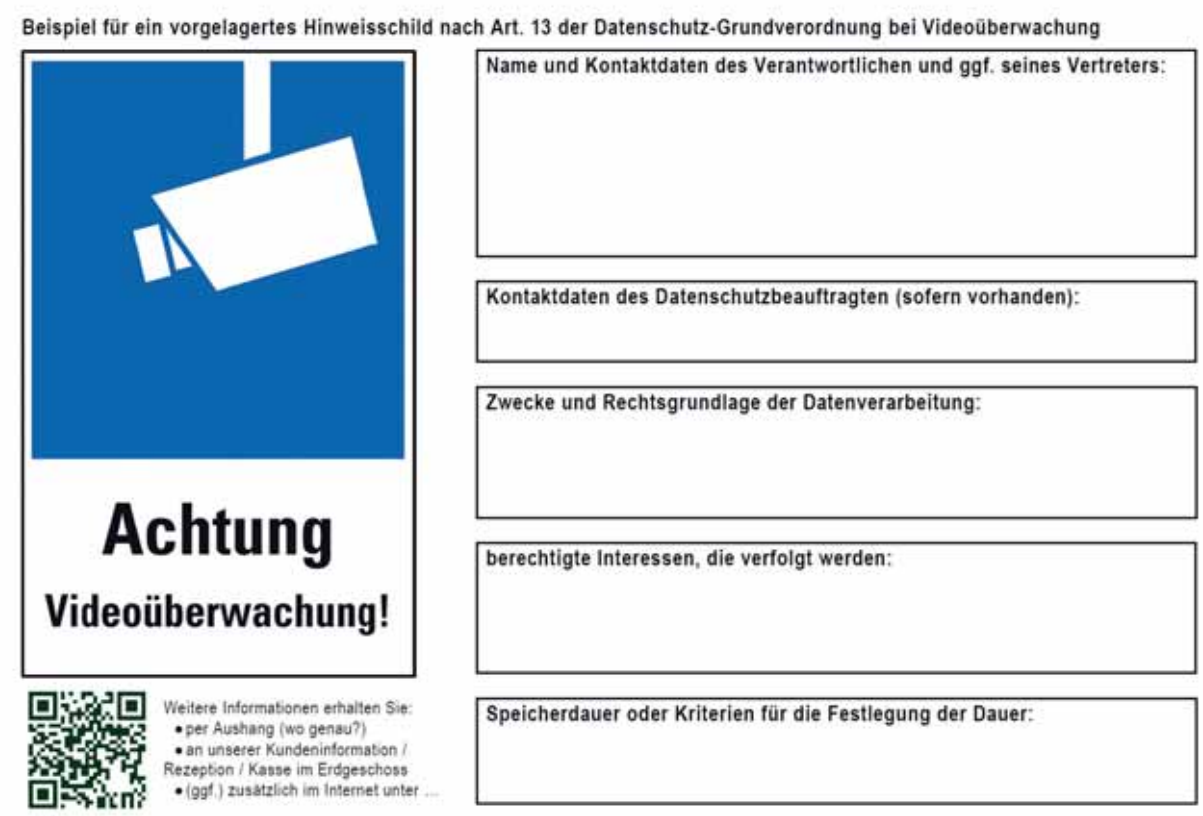
Zum Thema Videoüberwachung zu nennen wären insbesondere die Orientierungshilfen:

- Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen
- Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)
- Orientierungshilfe der Datenschutzaufsichtsbehörden zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen

Grundsätzlich muss man bei der Prüfung einer geplanten Videoüberwachung folgendes beachten:

Für die Prüfung der Rechtmäßigkeit der Videoüberwachung durch nichtöffentliche Stellen muss zunächst die „Generalklausel" in Art. 6 Abs. 1 S. 1 lit. f DSGVO beachtet werden. Danach ist die Verarbeitung rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Soll eine Videoüberwachung auf eine Einwilligung im Sinne des Artikels 7 DSGVO gestützt werden, dürften die Voraussetzungen dieser Vorschrift allerdings nur in seltenen Einzel-



Beispiel für ein Hinweisschild. Die Informationen sind unentgeltlich in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitzustellen. Sie können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden (vgl. Art. 12 DSGVO). Um Lesbarkeit zu erreichen, sollte der Ausdruck mindestens in DIN A4 erfolgen.

fällen erfüllt sein, so die Aufsichtsbehörden. Insbesondere ist das Betreten des gekennzeichneten Erfassungsbereichs einer Videokamera nicht als „eindeutig bestätigende Handlung" und auch nicht als informierte Einwilligung nach Artikel 4 Nr. 11 DSGVO zu werten.

Zudem muss die Videoüberwachung auch wirklich erforderlich sein zur Wahrung des geplanten Zweckes und der Interessen des Unternehmens als verantwortliche Stelle. Ebenso muss an die Hinweisbeschilderung, die Begrenzung der Speicherdauer, die Datensicherheit und die Prüfung, ob eine Datenschutzfolgenabschätzung für die Videoüberwachung gemacht werden muss, gedacht werden. Es zeigt sich: Videoüberwachung bleibt ein Brennpunkt im Datenschutz, die Umsetzung der DSGVO dabei ist zwingend und durchaus anspruchsvoll. Aber die Aufsichtsbehörden haben entsprechend auch viele Informationen dazu veröffentlicht. Hilfreich sind dabei auch das „Muster für ein Hinweisschild zur Videoüberwachung nach Datenschutz-Grundverordnung" sowie das „Muster für ein Informationsblatt zur Videoüberwachung". Die Muster können beispielsweise beim Landesbeauftragten für den Datenschutz Niedersachsen heruntergeladen werden. (www.lfd.niedersachsen.de/startseite/dsgvo/transparenzanforderungen-und-hinweisbeschilderung-bei-einer-videoueberwachung-nach-der-ds-gvo-158959.html) □

SECUREPOINT

NextGen UTM-Firewalls

- **Eingebettet in das Unified Security-Konzept**
- High-End Content-Filter und Zero-Hour-Protection
- Threat Intelligent Feed und Angriffserkennungen
- Schützt vor Ransomware und Cyber-Angriffen
- Single License Modell

Auch als monatliches **Firewall as a Service Mietmodell** erhältlich!

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 04131/2401-0 • E-Mail: info@securepoint.de
www.securepoint.de

SecurITy made in Germany

EU DS-GVO *ready*

Highlight auf der it-sa:
Neue Funktionen für Securepoint Mobile Security

Mit Mobile Security können IT-Verantwortliche private Android- und iOS-Geräte für die Verwendung im professionellen Umfeld vollständig managen und umfassend steuern. Wir präsentieren die von Google zertifizierte Umsetzung auf der diesjährigen it-sa.

Securepoint Mobile Security bedeutet:

- Android Enterprise Mobility Management (EMM)
- Work Profile Management für Android
- Cloud-Firewall Cluster (VPN, Port-Filter, Content-Filter, Virenschutz)
- Verschlüsselte VPN-Verbindungen
- Mobile Device Management (MDM)
- Einfachste Inbetriebnahme
- KMU-optimierte Sicherheitslösung

Lassen Sie sich von uns auf der it-sa 2019 in Nürnberg vom 08. - 10. Oktober beraten.

Wie das IoT dem Datenschutz helfen kann

Sicherheit und Datenschutz im Internet of Things (IoT) sind nicht nur wichtig, sondern auch lohnend, denn das IoT hat nicht nur Risiken, sondern auch Vorteile für den Datenschutz.

Von Oliver Schonschek

Wenn in der letzten Zeit vermehrt über Datenschutz gesprochen wurde, lag dies in aller Regel an der Datenschutz-Grundverordnung (DSGVO/GDPR) der EU. Auch wenn es einige Veränderungen im Datenschutz durch die DSGVO gegeben hat, so bestanden doch viele Anforderungen bereits in Zeiten des alten Bundesdatenschutzgesetzes (BDSG-alt). Das gilt auch für Datenschutzbereiche, die nun als besonders schwierig empfunden werden. Zum Beispiel waren viele der Rechte der Betroffenen bereits im alten Datenschutzrecht vorhanden. Doch durch die DSGVO sind sie nun stärker ins Bewusstsein gerückt.

Einen vergleichbaren (wenn auch nicht so starken) Effekt kann man bei dem Internet der Dinge (IoT, Internet of Things) sehen, wenn es um die Sicherheitsanforderungen bei der Digitalisierung geht. Zweifellos gibt es Besonderheiten im Datenschutz und in der IT-Sicherheit, wenn es um IoT geht. Auch sind spezielle IT-Sicherheitslösungen für das IoT sinnvoll und wichtig. Trotzdem kann man sagen: Das IoT hat die Sensibilisierung für die notwendige IT-Sicherheit nochmals erhöht. Die Risiken im IoT haben durchaus positive Nebenwirkungen für den Datenschutz und die IT-Sicherheit. Das zeigen auch die folgenden Beispiele.

Bild: LuckyStep/stock.adobe.com

Chance, nicht nur Bedrohung: Die Risiken im IoT haben durchaus positive Nebenwirkungen für den Datenschutz und die IT-Sicherheit.

IoT-Risiken als Teil der IT-Sicherheitsrisiken sehen

Betrachtet man die aktuelle IT-Sicherheitslage, stellt man fest, dass die IoT-Risiken eine immer größere Bedeutung erlangen und Gefahr darstellen. Dabei darf man nicht vergessen, dass die IoT-Bedrohungen immer als Teil der Gesamtbedrohungen verstanden werden sollten. Wenn IoT-Risiken zu einer bestimmten Bedrohung beitragen, gilt es, die Bedrohung auch als Ganzes anzugehen. Die Ergebnisse von internationalen Studien verdeutlichen diesen Zusammenhang:

- Cyberkriminelle nutzen verstärkt IoT-Geräte für DDoS-Angriffe. Davor muss man sich schützen, aber am besten so, dass man sich insgesamt vor DDoS-Attacken besser schützt.
- Sechs der Top-12-Exploits sind auf IoT-Geräte ausgerichtet. Entsprechende Gegenmaßnahmen müssen sich natürlich auch auf alle anderen Kategorien von Exploits ausrichten. Benötigt wird daher eine Security Fabric, die die gesamte Netzwerkumgebung von IoT-Endpunkten bis hin zu Multi-Clouds abdeckt und jedes Sicherheitselement integriert. Nur so können Unternehmen der wachsenden Bedrohungslage von heute gerecht werden und ihre wachsende Angriffsfläche schützen.
- Unternehmen vertreten oft unrealistische Ansichten über den Schutz des Industrial Internet of Things (IIoT), in dem Endpunkte als die verletzlichsten Aspekte betrachtet werden. Dabei besteht eine große Unsicherheit darüber, was überhaupt ein Endpunkt ist. Dabei ist es wichtig, dass sich die Unternehmen nicht nur im IoT und IIoT darüber klar werden, welche Endpunkte sie einsetzen, sondern in der kompletten IT und OT.
- Die drastische Zunahme von privaten Endgeräten und IoT-Devices in Unternehmensnetzwerken sorgt für enorme Sicherheitsrisiken. Das bedeutet, dass Unternehmen nicht nur feststellen sollten, welche IoT-Geräte sie nutzen, sondern auch, welche privaten Geräte und IT-Geräte eingesetzt werden.

Security-Empfehlungen nicht durch Insellösungen umsetzen

Zur IoT-Sicherheit gibt es eine Vielzahl von Empfehlungen, was man angehen sollte. Wie Avira berichtete, einigten sich das Europäische Komitee für Normung, die britische Regierung sowie ein Branchenverband erstmalig auf Sicherheitsstandards für IoT-Geräte. Die 13 Richtlinien im Überblick lauten:

- Keine Standardpasswörter verwenden
- Richtlinie zur Offenlegung von Schwachstellen implementieren
- Software auf dem aktuellen Stand halten
- Zugangsdaten und sicherheitsrelevante Daten sicher speichern
- Sicher kommunizieren
- Angriffsflächen minimieren

⇨

Bild: leowolfert/stock.adobe.com

Mehr Sicherheit und Datenschutz im IoT lohnt sich – nicht nur für das Internet of Things, sondern übergreifend für die gesamte Digitalisierung.

- Software-Integrität gewährleisten
- Schutz von personenbezogenen Daten gewährleisten
- Systeme ausfallsicherer gestalten
- System-Telemetriedaten überwachen
- Verbrauchern die einfache Löschung personenbezogener Daten ermöglichen
- Installation und Wartung von Geräten vereinfachen
- Eingabedaten überprüfen

Diese Richtlinien sollten zweifellos auch außerhalb des IoT eine umfassende Anwendung finden, in allen Bereichen der IT und OT.

Was das für die Unternehmen bedeutet

Unternehmen müssen also mehr für den Datenschutz und die IT-Sicherheit im IoT tun. Die Bemühungen, der Aufwand und die Investitionen für ein sicheres und datenschutzkonformes IoT helfen auch bei der Verbesserung im Datenschutz und der IT-Sicherheit in der ganzen, restlichen IT. Viele der neuen IoT-Sicherheitslösungen adressieren die IT und das (Industrial) IoT gemeinsam. Wenn hier neue, übergreifende Lösungen und Verfahren zum Einsatz kommen und Standards etabliert werden, hilft dies eben nicht nur im Internet der Dinge, sondern in der ganzen IT und damit für die gesamte Digitalisierung.

Mehr Sicherheit und Datenschutz im IoT lohnt sich – nicht nur für das Internet of Things, sondern übergreifend für die Digitalisierung. Das sollte bei den Budgets für IoT-Sicherheit bedacht werden, ebenso bei der Überlegung, ob sich der ganze Aufwand für Datenschutz und Sicherheit für das IoT denn überhaupt (schon) lohnt.

Wer das IoT sicherer und datenschutzgerechter macht, schafft im Idealfall keine Insellösungen, sondern ein übergreifendes System für Datenschutz und IT-Sicherheit. □

Bald kein Datenschutzbeauftragter in Kleinbetrieben mehr nötig

Bei der DSGVO gibt es eine wesentliche Neuerung: Der Bundestag verdoppelte vor wenigen Wochen den Schwellenwert für die Ernennung eines betrieblichen Datenschutzbeauftragten. Damit sollen Kleinbetriebe von der Bürokratie entlastet werden.

Von Heidi Schuster, IT-BUSINESS

Die DSGVO gilt seit mehr als einem Jahr, und nun gibt es eine interessante Änderung bezüglich des Datenschutzbeauftragten (DSB). Ursprünglich hieß es, wenn sich 10 Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, ist ein Datenschutzbeauftragter (DSB) notwendig. Mit dem neuen Gesetzentwurf wurde dieser Schwellenwert auf 20 Mitarbeiter heraufgesetzt. Das soll vor allem kleine Betriebe und Vereine entlasten. Befürworter des neuen Schwellenwerts argumentieren, dass 90 Prozent der Handwerksbetriebe davon profitieren würden und ein massiver Bürokratieabbau möglich sei. Hingegen sehen Kritiker wie der Bundesdatenschutzbeauftragte Ulrich Kelber darin eine „falsche Maßnahme, die die Wahrung des hohen Datenschutzniveaus in Deutschland ernsthaft gefährden könnte".

Datenschutz praxisnah gestalten

„Wünschenswert wäre es, wenn die Regierung die aktuelle Evaluierung der Datenschutzgrundverordnung dafür nutzt, den Datenschutz möglichst praxisnah und risikogerecht zu gestalten", meint Patrycja Tulinska, IT-Sicherheitsexpertin und Geschäftsführerin der PSW Group Consulting. Tulinska führt weiter aus: „Als ständig beschäftigt gilt für den Gesetzgeber derjenige, der permanent für die Kunden- oder Personalverwaltung zuständig ist. Personen, die beispielsweise als Handwerker oder Mitarbeiter in der Produktion lediglich mit Namen und Adressen von Kunden umgehen, beschäftigen sich nicht ständig damit. Die automatisierte Verarbeitung von Daten meint das Erheben, Verarbeiten sowie Nutzen personenbezogener Daten mithilfe von Datenverarbeitungsanlagen. Das können also Computer, Smartphones oder Server, aber auch ein Kopierer sein, wenn er mit einem Speichermedium arbeitet."

Ausnahmen

Allerdings: Der neue Schwellenwert gilt nicht für Unternehmen, die personenbezogene Daten verarbeiten, die zur Bewertung der Persönlichkeit des Betroffenen, seiner Leistungen oder seines Verhaltens beitragen. „Das beträfe beispielsweise einen Hörgeräteakustiker oder auch einen Orthopädiemechaniker. Personenbezogene Daten werden von ihnen verarbeitet und zur Bewertung des Betroffenen genutzt. Dementsprechend müssen sie auch dann einen Datenschutzbeauftragten ernennen, wenn sie unter dem Schwellenwert liegen", ergänzt Tulinska. Dasselbe gilt für Betriebe, die hoheitliche Aufgaben verfolgen, etwa den Schornsteinfeger. □

Impressum

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

IT-BUSINESS

Redaktion: Wilfried Platten/pl (-106) – Chefredakteur, Dr. Andreas Bergler/ab (-141) – CvD/ltd. Redakteur

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

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

SECURITY-INSIDER.DE

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

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

Key Account Management: Brigitte Bonasera (-142)

Anzeigendisposition: Dagmar Schauer (-202)

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

EBV: Carin Böhm, Brigitte Krimmer

Anzeigen-Layout: Johannes Rath

Adressänderungen/Vertriebskoordination:
Sabine Assum (-194), Fax (-228)
eMail vertrieb@vogel-it.de

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

Geschäftsführer: Werner Nieberle – Geschäftsführer/Publisher

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

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

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

Inserenten

G DATA Software AG	Bochum	https://www.gdata.de/	2, 8, 9
LANCOM Systems GmbH	Würselen	https://www.lancom-systems.de/	18, 19
NCP engineering GmbH	Nürnberg	https://www.ncp-e.com/de/	14, 15, 52
Net at Work GmbH	Paderborn	https://www.netatwork.de	38, 39
netfiles GmbH	Burghausen	https://www.netfiles.de/	35
retarus GmbH	München	https://www.retarus.com/de/	22, 23
SAST SOLUTIONS / akquinet AG	Hambrug	https://www.sast-solutions.de/	30, 31
secunet Security Networks AG	Essen	https://www.secunet.com/	5, 13
Securepoint GmbH	Lüneburg	https://www.securepoint.de/	44, 45
Vogel IT-Akademie	Augsburg	http://www.akademie.vogel-it.com/	29, 51

SECURITY 2020

CYBERDEFENSE & IDENTITY PROTECTION

TECHCONFERENCE • PEERFORUM • EXHIBITION

9. Juni Hamburg | **16. Juni** Würzburg | **25. Juni** Neuss | **2. Juli** München

Save the date


Keynote


Best Practice

Networking


Sharing Area

Eine Veranstaltung der VOGEL IT AKADEMIE

Jetzt voranmelden: **www.itsecurity-conference.de**

NCP
SECURE COMMUNICATIONS

integrierte Firewall

IIoT Sicherheit

Secure Cloud Connections

Endpoint Security

Quality of Service

mandanten-fähig

zentrales Management

Smart Maintenance

Remote Access

sichere Authentisierung

Die Brücke zwischen Unternehmens-IT und -OT

IT Security für Industrie 4.0
Secure Communications für Ihr Unternehmen.

Secur|Ty made in Germany

INDUSTRIE PREIS 2018 BEST OF

Best of Industry 4.0 Security:
NCP Secure IIoT Solution

www.ncp-e.com