GIT CYBER SECURITY 2018

EIN SPECIAL VON GIT SICHERHEIT + MANAGEMENT

DIE RICHTIGEN SCHUTZMASSNAHMEN GEGEN CYBER-ATTACKEN

Titelthema Seite 12:

MOXA – CYBER SECURITY FÜR DAS IIOT

- **Angriffe auf die Industrie** – und wie effiziente Abwehr aussieht
- **Gebäudesicherheit:** Was Planer und Errichter von Sicherheitssystemen jetzt tun müssen
- **DSGVO vs. Videoüberwachung:** wie man Videotechnik richtig implementiert
- **Vernetzung** von Waren und Systemen – und wer wofür die Verantwortung trägt

Mit Tipps und Cyber-Checks

Event-Partner: it sa 2018

Gefördert von: MOXA Reliable Networks Sincere Service | AXIS COMMUNICATIONS | Dallmeier | ROHDE&SCHWARZ | United Technologies | WatchGuard

WILEY

ORGANISATIONEN INSTITUTIONEN UND UNTERNEHMEN IM HEFT INDEX SCHNELLFINDER

INHALT

CYBERTORIAL

Die Revolution geht weiter

Das **Special GIT Cyber Security** gibt es auch als Microsite, e-Paper und Smart Magazine im responsiven Design. Mehr Infos dazu auf **GIT-SICHERHEIT.de/cybersecurity**

Liebe Leserin, Lieber Leser,

sie gehört zu den meistbesprochenen und geradezu allgegenwärtigen Metathemen unserer Zeit: Die anhaltende digitale Revolutionierung praktisch sämtlicher Lebensbereiche – vor allem aber der Arbeitswelt, unserer Wirtschaft und Industrie. Cyber Security – Thema dieses Specials von GIT SICHERHEIT – ist sozusagen die mitwachsende andere Seite der digitalen Medaille. Das wäre jedenfalls der Idealfall. Freilich gehen Digitalisierung und Vernetzung oft alles andere als Hand in Hand mit der IT-Sicherheit. Ihr Verhältnis zueinander erinnert ein wenig an die Immobilienwirtschaft: Es gibt eben nicht nur Neubauten, sondern einen beträchtlichen Altbestand, der viel nachzuholen hat an Dämmung, energetischer Ertüchtigung und moderner (Smart-Home-) Technik.

Was heißt das übersetzt für industrielle Anlagen? Wie steht es aktuell überhaupt um Cybersicherheit hierzulande? Welche Empfehlungen sind daraus abzuleiten? Antworten liefert zum Beispiel Jens Wiesner vom Bundesamt für Sicherheit in der Informationstechnik in unserem Interview ab Seite 8. Die existenzielle Dringlichkeit dieser Fragen macht eine Umfrage des Verbands Deutscher Maschinen- und Anlagenbauer deutlich (ab Seite 6).

Einen konkreten Eindruck von den Bedrohungen entlang globaler Zuliefer- und Produktionsbeziehungen können Sie sich ab Seite 14 machen. Lukas Linke, Senior Manager Cybersecurity beim ZVEI macht deutlich, wie es am Ende der Lieferkette, bis hin zur Waschmaschine, Smart-Fernseher oder medizintechnischem Gerät, um die Cybersicherheit bestellt ist.

Einen näheren Blick auf Cyber Security in der Sicherheits- und Gebäudetechnik wirft ab Seite 20 Jochen Sauer von Axis im Gespräch mit den Fachberatern, -planern und Errichtern Philipp Rothmann, Benjamin Bäßler und Jens Heil.

Speziell um die Datenschutz-Grundverordnung geht es im Beitrag von Dallmeier ab Seite 17: Welche Folgen hat die derzeit praktisch jedes Unternehmen beschäftigende DSGVO für die Implementierung von Videosicherheitstechnik?

Diese und weitere Artikel in diesem Special sollen Ihnen einen Überblick geben über die aktuellen Risiken – vor allem aber über die richtigen Schutzmaßnahmen in Sachen Cyber Security.

Übrigens: Unser besonderer Event-Partner ist die it-sa – zu Recht bezeichnet sich die Fachmesse für IT-Security-Profis auch als „Home of IT-Security". Auf Seite 26 geben wir Ihnen schon mal eine Vorschau auf das Programm von Messe und Kongress im Messezentrum Nürnberg.

Wir wünschen Ihnen eine interessante Lektüre. Bleiben Sie (nicht nur) cybersicher!

Dr. Heiko Baumgartner
Heiko.Baumgartner@Wiley.com

Steffen Ebert
Steffen.Ebert@Wiley.com

Matthias Erler
Matthias.Erler@Wiley.com

LEITARTIKEL

Keine Digitalisierung ohne Cyber-Sicherheit

Editorial von Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI, Bonn)

Foto: Bundesamt für Sicherheit in der Informationstechnik

Im Januar 2017 hatte Christian Brandstätter, Geschäftsführer des Seehotel Jägerwirt auf der Turracher Höhe in Kärnten, ein Déjà-vu. Denn sein mit 180 Gästen total ausgebuchtes Hotel wurde bereits zum vierten Mal gezielt angegriffen. Die vorigen Angriffe, die über Phishing-Mails kamen, konnten noch abgewehrt werden. Bei dieser Attacke jedoch wurde das gesamte Schlüsselsystem lahmgelegt. Der Angreifer verlangte zur Freigabe zwei Bitcoins. Brandstätter zahlte nicht, informierte die Polizei und handelte: Als Sicherheitsmaßnahme wurde der für die Codeerstellung der Zimmerkarten verwendete PC vom Internet getrennt, Systeme wurden entkoppelt sowie Geräte getauscht.

So passiert in Österreich, aber so oder ähnlich hätte es auch in Deutschland passieren können. Ein scheinbar harmloser Fall? Mitnichten. Eher ein Beleg dafür, was alles möglich ist und wie Systeme, die eigentlich Sicherheit vermitteln sollen, zur Sicherheitslücke werden können.

Einfallstore für Cyber-Angriffe sind vielfältig. Der Angreifer verschafft sich Zugang über eine oder mehrere Schwachstellen, via E-Mail oder über eine Anwendungs- oder Netzwerkschwachstelle und schleust Malware in das Unternehmensnetzwerk ein. Moderne Cyber-Attacken haben nichts mehr mit den vergleichsweise harmlosen Spamming-Wellen früherer Jahre zu tun. Die Angreifer verfügen über leistungsfähige und flexibel einsetzbare Angriffsmittel und verbessern ihre Methoden kontinuierlich. Zurzeit gibt es rund 620 Millionen PC-basierte Schadprogrammvarianten und täglich kommen rund 280.000 neue Varianten hinzu. In den letzten beiden Jahren verursachten Cyber-Angriffe in Deutschland Schäden in zweistelliger Milliardenhöhe.

Nach den Ergebnissen der Cyber-Sicherheits-Umfrage 2017, die das BSI im Rahmen der Allianz für Cyber-Sicherheit durchgeführt hat und an der rund 900 Unternehmen und Institutionen teilnahmen, sind knapp 70 Prozent der Befragten in den letzten beiden Jahren Opfer von Cyber-Angriffen geworden. In knapp der Hälfte der Fälle waren die Angreifer erfolgreich und konnten sich zum Beispiel Zugang zu IT-Systemen verschaffen, die Funktionsweise von IT-Systemen beeinflussen oder Internet-Auftritte von Firmen manipulieren.

Vor allem in der Fabrik- und Prozessautomatisierung sowie in Kritischen Infrastrukturen eingesetzte industrielle Steuerungsanlagen (Industrial Control Systems, ICS) sind potenzielle Ziele. Schon seit einigen Jahren zeichnet sich ab, dass eine oder mehrere Gruppen Schadsoftware entwickeln, die speziell für Angriffe auf Prozesssteuerungsanlagen geeignet ist. Ausfälle oder Störungen haben in der Regel gravierende physische Auswirkungen, beispielsweise in Form von Stromausfällen oder Produktionsunterbrechungen.

Im Mai 2017 drangen unbekannte Hacker in das Netz einer regionalen Tochter des Energieversorgers EnBW ein und hatten für einen Zeitraum von wenigen Minuten Zugriff auf einen geringen Teil des Internetverkehrs. Der Betreiber, meldete den Sicherheitsvorfall beim BSI und bat um Unterstützung. Der Vorfall wurde im Rahmen des Nationalen Cyber-Abwehrzentrums in Zusammenarbeit mit dem betroffenen Unternehmen analysiert und bearbeitet.

Im Dezember 2017 wurde der Angriff auf ein Safety Instrumented System (SIS) einer Industrieanlage im Nahen Osten mit einer „Triton" genannten Schadsoftware gemeldet. Diese Systeme unterliegen besonderen Anforderungen an funktionale Sicherheit. In industriellen Automatisierungssystemen, die auch in Kritischen Infrastrukturen und der Prozessindustrie zum Einsatz kommen, werden sie im Regelfall getrennt vom Leitsystem aufgebaut. Die Angreifer konnten sich auch nur Zugang zu den IT-Servern des Opfers verschaffen und bewegten sich hauptsächlich mit eigenentwickelten Tools durch die Demilitarisierte Zone der Betriebstechnik. Sie wurden erkannt und konnten abgewehrt werden.

Angriffe auf Sicherheitssysteme in der Industrie, in Kritischen Infrastrukturen oder im Dienstleistungsbereich stellen, aufgrund der möglichen Auswirkungen für Mensch und Umwelt, eine ernstzunehmende Bedrohung dar. Natürlich hat ein Angriff auf das Schlüsselsystem eines Hotels eine andere Dimension als einer auf das Safety-System einer Industrieanlage oder die Kommunikations-Infrastruktur einer Region.

Aber: Darauf kommt es nicht an. Wir dürfen keinen dieser Angriffe auf die leichte Schulter nehmen. Wir dürfen auch nicht hinnehmen, dass durch die hohe Innovationsfrequenz und die intensivierte Nutzung von Informations- und Kommunikationstechnologie quasi naturgesetzlich immer neue Sicherheitslücken und Schwachstellen entstehen. Wir brauchen Cyber-Sicherheit von Anfang an, müssen sie bei jeder Produktentwicklung mitdenken, mitgestalten und mitkalkulieren. Und wir dürfen nicht nachlassen, auf die Gefahren aus dem Cyber-Raum hinzuweisen, über Angreifer und Angriffe zu informieren, unsere Abwehrbemühungen zu verstärken, unsere Forschung zu intensivieren und unsere Kooperation auszubauen. Ohne erfolgreiche Cyber-Sicherheit gibt es keine erfolgreiche Digitalisierung. Daher hat der Bund das Bundesamt für Sicherheit in der Informationstechnik zur nationalen Cyber-Sicherheitsbehörde ausgebaut, wodurch die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft erfolgreich gestaltet wird. ■

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bonn
Tel.: +49 228 99 9582 5850
presse@bsi.bund.de
www.bsi.bund.de

Sicherheit komplett

von Wiley

Mit unseren digitalen und gedruckten Medien sind Sie immer bestens informiert – über alle Themen der Sicherheit.

Probeabos, Mediadaten, Kontakt: GIT-GS@wiley.com

WILEY

BETRÜGERISCHE KOMUNIKATION

Millionenschaden durch Cybercrime

Ende 2017 haben mehrere VDMA-Mitglieder unabhängig voneinander von Betrugsfällen mit gefälschten Kontodaten bei Angeboten an internationale Kunden berichtet. Vorsicht ist geboten.

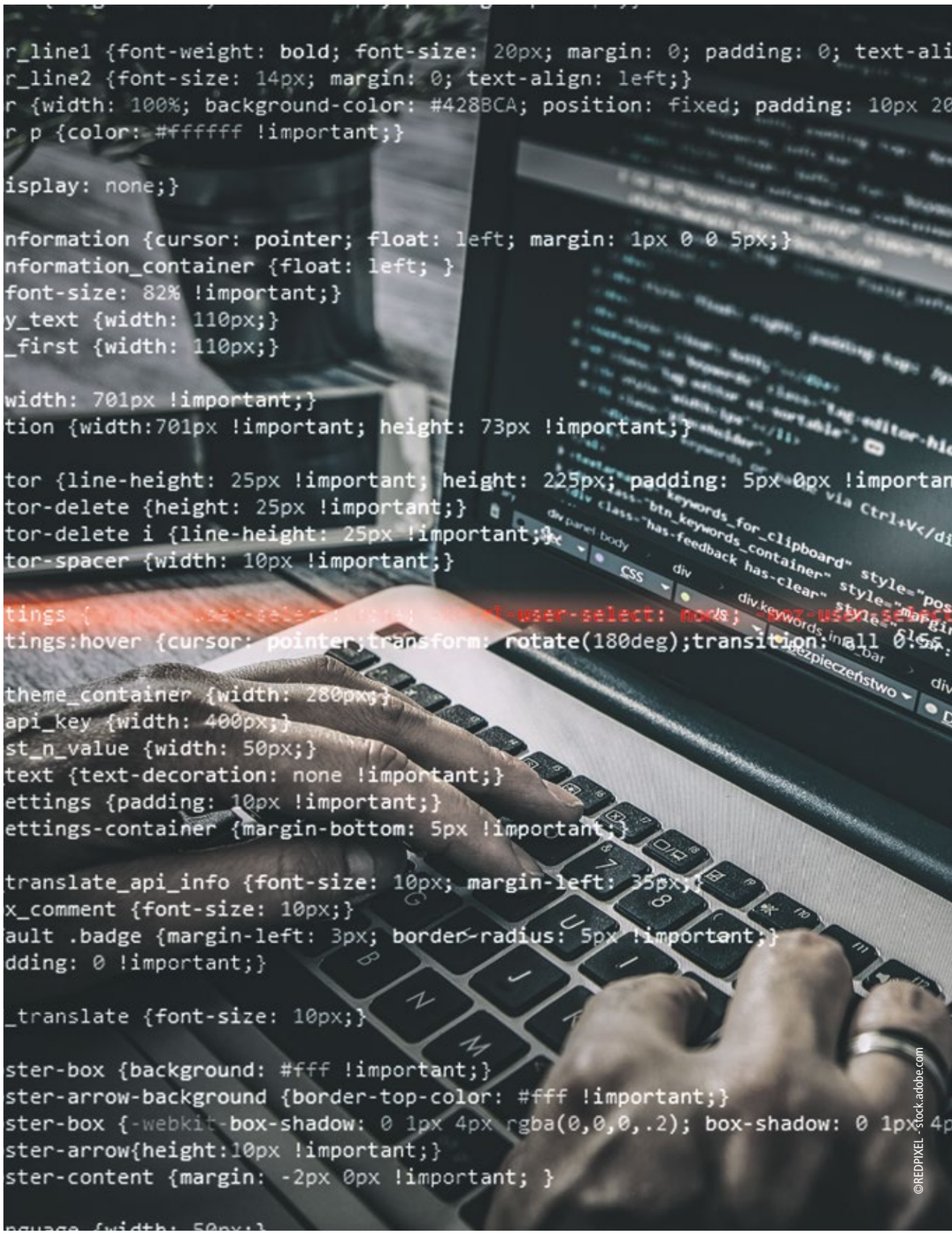
Cyberkriminelle ändern Angebot-E- Mails, tauschen Kontodaten in PDF-Dokumenten aus und bringen Kunden dazu, auf andere Konten Anzahlungen für Maschinen zu überweisen. Der dem VDMA bekannte Schaden geht pro Fall bereits in die Hunderttausende. Die Betrüger sind noch immer aktiv. In allen Fällen zeigt sich, dass sich die Täter in die E-Mail-Kommunikation eingeklinkt haben. Ziel der Betrüger ist es, die Kontodaten für Anzahlungen zu manipulieren. Dadurch werden die Anzahlungen auf andere Konten überwiesen. Dem betroffenen Kunden eines Maschinenbauers entstand dadurch ein großer finanzieller Schaden, darüber hinaus wurden die Geschäftsbeziehungen stark belastet. So berichtet ein Unternehmen aus Nordrhein-Westfalen, dass durch diese Betrugsmasche sowohl die Anzahlung des Kunden von über 400 000 Euro weg sei als auch der Kunde selbst.

E-Mail-Accounts gehackt

Es ist davon auszugehen, dass sich der Angreifer auf illegalem Wege einen Zugang zu einem der E-Mail-Konten des Maschinenbauers verschaffte. Der Angreifer konnte daraufhin über einen längeren Zeitraum alle E-Mails des Betroffenen mitlesen und ist erst

Ansprechstellen

Die zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft finden Interessierte unter dem Unten angegebenem Link, ebenso die Meldestelle against Cybercrime in Österreich.



©REDPIXEL - Stock.adobe.com

Wichtige Internetadressen

- www.bka.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
- bundeskriminalamt.at/306/start.aspx
- industrialsecurity.vdma.org
- sud.vdma.org

aktiv geworden, als ein vielversprechendes Angebot im Postfach landete. Der Maschinenbauer erhielt vom (vermeintlichen) Kunden nun eine E-Mail, in der eine Änderung der E-Mail-Adresse angekündigt wurde. Aufseiten des Kunden ist dies gleichzeitig in ähnlicher Art geschehen. Somit lief ab diesem Zeitpunkt die Kommunikation nur noch über den Angreifer. Diese Art von Angriff ist ein sogenannter „Man-in-the-Middle-Angriff". Die gefälschten E-Mail-Adressen unterscheiden sich oft nur in einem Buchstaben, der im Outlook angezeigte Name des Absenders bleibt jedoch gleich, wie im vorliegenden Fall. Dadurch war es schlussendlich dem Angreifer möglich, die PDF-Angebote unbemerkt zu manipulieren und den Kunden dazu zu bewegen, die Anzahlung auf das falsche Konto zu überweisen.

Betrugsfälle sollten grundsätzlich zur Anzeige gebracht werden, denn nur so können weitere Fälle bei anderen Unternehmen verhindert werden. Jedes Landeskriminalamt (LKA) hat eine Meldestelle für Cybercrime. In Österreich ist die Meldestelle beim Bundeskriminalamt. Bei den genannten Vorfällen sind die jeweiligen Landeskriminalämter gemeinsam mit den betroffenen Unternehmen gegen die Betrüger vorgegangen – bisher leider ohne Ermittlungserfolg.

Telefonischer Direktkontakt bei Zahlungen

Der VDMA empfiehlt, bei Angeboten per E-Mail immer ein Auge auf die E-Mail-Adresse des Geschäftspartners zu haben und nicht nur auf den Anzeigenamen des Absenders. Unternehmen sollten ihre Mitarbeiter und gegebenenfalls Kunden sensibilisieren, stets skeptisch gegenüber angekündigten Änderungen der E-Mail-Adresse zu sein. Auch plötzliche Kontoänderungen in einer laufenden Kommunikation sollten nicht einfach hingenommen werden. Sofern möglich, sollten vor Zahlungen die Kontodaten im telefonischen Direktkontakt bestätigt werden. Technisch ist auch der Passwortschutz für PDF-Dateien mit telefonischer Übermittlung des Passwortes denkbar. Über die Möglichkeit des Abschlusses einer Cyberversicherung können Interessierte mit Thomas Völker von der VDMA in Kontakt treten, dem Versicherungsmakler für den Maschinen- und Anlagenbau. ■

Autor
Steffen Zimmermann,
VDMA Competence Center Industrial Security

Kontakt

VDMA Verband Deutscher Maschinen- und Anlagenbau e.V.
Frankfurt
Tel.: +49 69 6603 0
kommunikation@vdma.org
www.vdma.org

Seit 2013 arbeitet Herr Wiesner im Bundesamt für Sicherheit in der Informationstechnik (BSI) und ist seit Mitte 2016 Leiter des Referats „Cyber-Sicherheit in Industrieanlagen"(ICS). Zusätzlich zu Awareness und praktischen Empfehlungen für Hersteller, Integratoren und Betreiber von ICS ist ein weiterer Aufgabenschwerpunkt seiner Tätigkeit die Nationale und Internationale Zusammenarbeit zur Stärkung der Cyber-Sicherheit von Industrieanlagen

INDUSTRIE

Cybersicherheit in Industrieanlagen

Im Gespräch mit Jens Wiesner, BSI, Bundesamt für Sicherheit in der Informationstechnik

GIT SICHERHEIT: Herr Wiesner, das Thema Cybersicherheit gewinnt zunehmend an Relevanz gerade auch für Industrieanlagen. Wie schätzen Sie die aktuelle Lage diesbezüglich ein?

Jens Wiesner: Die Digitalisierung schreitet voran, gerade die Wirtschaft profitiert an vielen Stellen von mehr Effizienz und Effektivität. Gleichzeitig gibt es viele Bestandsanlagen, die zu einer Zeit gebaut wurden, als IT-Sicherheit noch keine Rolle spielte. Viele Anlagen werden jetzt ertüchtigt und gleichzeitig kommen mit der Vernetzung beispielsweise durch Nutzung von Cloud/Edge und Apps Herausforderungen hinzu, die von vielen noch gar nicht abgeschätzt werden können. Die Mischung aus Aufbruchsstimmung und Unsicherheit darf jedoch nicht zu einer Verweigerungshaltung führen, die dann ein Wettbewerbsnachteil wird. Andererseits müssen die Anlagen zuverlässig produzieren. Um das zu erreichen, nimmt das Bundesamt für Sicherheit in der Informationstechnik seine gestaltende Rolle wahr und unterstützt Hersteller, Errichter und Betreiber bei der Absicherung ihrer Systeme und Anlagen.

Wo liegen nach Ihrer Ansicht die neuen Herausforderungen?

Jens Wiesner: Mit der zunehmenden Digitalisierung nimmt auch die Vernetzung zu. Die klassischen Konzepte der gestaffelten Verteidigung (Defense in depth) werden immer weniger wirksam, wenn die Grenzen zwischen den einzelnen Ebenen - beginnend bei Sensoren und Aktoren über die Steuerung bis zu den Managementsystemen - durch umfassende Anbindung beispielsweise mit Clouddiensten immer weiter verwischen.

Unternehmensübergreifende Infrastrukturen, sichere Identitäten und Kommunikation müssen übergreifend möglich sein – was sind Ihre Empfehlungen und Tipps an die Sicherheitsmanager der Industrie?

Jens Wiesner: Aktuell haben viele einfache Angriffe Erfolg, die mit elementaren, ebenso einfachen Maßnahmen hätten verhindert werden können. Oft dauert es viel zu lange, bis ein Angreifer im Netzwerk bemerkt wird. Dabei sind gerade Produktionsnetzwerke mit ihrer vergleichsweise einfachen und meist statischen Konfiguration prädestiniert dafür, durch Angriffe erzeugte Anomalien zu erkennen. Bei vielen Verantwortlichen ist mittlerweile das Bewusstsein vorhanden, dass etwas getan werden muss, bei der konkreten Umsetzung jedoch gibt es Nachholbedarf. Oft scheitert es an fehlendem Personal, das in der Lage ist, Vorgaben zu machen und durchzusetzen. Die Einführung von Sicherheitsfunktionen macht manche Vorgänge langwieriger und umständlicher und wird daher als lästig oder gar unnötig wahrgenommen. Diese Einstellung ist falsch, denn letztlich ist in Zeiten der Digitalisierung eine Investition in die IT-Sicherheit eine Investition in den Geschäftserfolg. Wichtig ist, dass es nicht eine einzige Lösung gibt, die das System absichert, sondern immer mehrere im Zusammenspiel miteinander wirken. IT-Sicherheit ist ein dauerhafter Prozess, der gelebt werden muss. Das BSI bietet Unternehmen Hilfestellung an, etwa im Rahmen der Allianz für Cyber-Sicherheit (www.allianz-fuer-cybersicherheit.de) oder mit dem modernisierten und praxistauglichen IT-Grundschutz.

Cybersecurity muss zu den jeweiligen Prozessen passen, je nach Produktionsumfeld. Stichwort Industrie 4.0 – Produktion in Losgröße 1: Wie lässt sich da für Cybersicherheit sorgen?

Jens Wiesner: Industrie 4.0 wird mit Unterstützung des BSI auch unter Sicherheitsaspekten entwickelt. Diese müssen bereits in der Designphase der Produkte berücksichtigt werden („Secure by Design") und umfasst die Nutzung sicherer Protokolle und Identitäten genauso wie einen abgesicherten Auslieferungszustand („Secure by Default").

Wo sehen Sie die Herausforderungen im Spannungsfeld Funktionale Sicherheit und Security? Inwieweit ist das Thema Cybersecurity in der Funktionalen Sicherheit angekommen?

Jens Wiesner: 2017 wurde ein Vorfall bekannt, bei dem das Safety-System einer Kritischen Infrastruktur im Mittleren Osten angegriffen wurde. Dieses Vorgehen war gezielt auf die Anlage zugeschnitten und hätte im „Erfolgsfalle" erhebliche Schäden verursachen, möglicherweise sogar Menschenleben kosten können. Viel zu oft sehen wir noch, dass in der Funktionalen Sicherheit die IT-Sicherheit keine große Rolle spielt und das Gefahrenbewusstsein für dieses Risiko noch nicht angemessen ausgeprägt ist.

Welche Warnungen sprechen Sie als BSI derzeit aus? Was sind die größten Gefahren und Angriffsflächen der Hacker?

Jens Wiesner: Wir unterscheiden zwischen gezielten und ungezielten Angriffen. Wannacry und Notpetya, zwei bedeutende Cyber-Angriffe des letzten Jahres, waren ungezielt. Sie hatten nicht eine spezielle Anlage im Fokus, haben aber dennoch in vielen Fällen Produktionsprozesse empfindlich gestört oder lahmgelegt. Es wird weitere Vorkommnisse dieser Art geben, denn Cyber-Angriffe sind ein für die Angreifer lukratives Geschäftsfeld. Zusätzlich werden wir auch weiterhin gezielte Angriffe sehen, bei denen Schwachstellen in Unternehmen mit dem Ziel der Erpressung ausgenutzt werden. Sicherheitsverantwortliche sollten sich auf das Szenario der gezielten Störung von unternehmenskritischen (Produktions-)Prozessen einstellen.

Wie steht es um die Security-Normen für das Produktionsumfeld?

Jens Wiesner: Der modernisierte IT-Grundschutz des BSI beinhaltet jetzt auch sogenannte IND-Bausteine und Umsetzungshinweise für das Produktionsumfeld. Zusätzlich sind diese auch für Funktionale Sicherheit mit der Möglichkeit zur Kommentierung über die BSI-Homepage www.bsi.bund.de verfügbar. Im internationalen Umfeld hat sich ISO/IEC 62443 etabliert, aufgrund des Umfangs von über 1.000 Seiten allerdings eher für Fortgeschrittene zu empfehlen. Die Verbände ZVEI und VDMA bieten kostenlos herunterladbare Einführungen dazu an. ■

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bonn
Tel.: +49 228 99 9582 0
bsi@bsi.bund.de
www.bsi.bund.de

INDUSTRIE

IT ohne Grenzen

Kernelemente des IT-Risikomanagements in der industriellen Fertigung

Die Digitalisierung löst die Grenzen zwischen Büro-IT und Produktions-IT immer weiter auf: Vormals getrennte Netze werden verknüpft, die eingesetzte Technik konvergiert und wird gleichzeitig durch neuartige Elemente, etwa cyber-physische Systeme, ergänzt. Diese Entwicklung verspricht erhebliche Effizienzgewinne und neue Geschäftsmodelle, erhöht aber auch die Anfälligkeit der industriellen Fertigung gegen Hacker, Malware und andere IT-Bedrohungen. Für Unternehmen wird es daher immer dringlicher, die Risiken ihrer Produktions-IT zu kennen und angemessen zu behandeln.

Wegen des großen Handlungsbedarfs wurden in den letzten Jahren verstärkt Normen und Empfehlungen zur IT-Sicherheit im industriellen Kontext publiziert – zu erwähnen sind hier etwa die mehrteilige technische Spezifikation IEC 62443, die VDI/VDE-Richtlinie 2182 und das ICS-Kompendium des Bundesamts für Sicherheit in der Informationstechnik. Auch dass der im Jahr 2017 modernisierte IT-Grundschutz des BSI eigene Bausteine zur Sicherheit der industriellen IT enthält, verweist auf die Dimensionen des Problems.

IT-Sicherheit im Produktionsbereich setzt das Zusammenwirken von Herstellern, Integratoren und Anwendern der IT-gestützten Produktionsanlagen voraus – die Handreichungen der Standards adressieren folglich alle drei Gruppen. Zusätzlich können übliche Methoden zur Analyse, Bewertung und Behandlung von IT-Risiken auch im Produktionsumfeld hilfreich sein, da bei der Umsetzung der Empfehlungen der Standards zu berücksichtigen ist, wie sich die einzelnen organisatorischen und technischen Maßnahmen auf die Geschäftsprozesse auswirken.

©vege - stock.adobe.com

Kernelemente des IT-Risikomanagements

Für ein effizientes Risikomanagement sollten Unternehmen den Fokus auf die kritischen Teile ihrer Produktions-IT richten, also auf Komponenten, die einen hohen Beitrag zur Wertschöpfung leisten und bei denen sich Ausfälle oder Störungen besonders gravierend auswirken können. In der Regel sind dies vollständige technische Systeme, etwa ausgewählte Anlagensteuerungen, Leitsysteme oder Prüfstrecken, aber auch bestimmte Teilaspekte der Produktions-IT beispielsweise Fernwartungsschnittstellen oder Netzkopplungen können im Blickfeld stehen. Diese Komponenten können top-down ausgewählt werden („Welche Anwendungen und Systeme werden in den wichtigen Prozessen des Unternehmens genutzt?"). Einfacher ist oft ein Bottom-up-Vorgehen („Welche Prozesse werden durch die Anwendungen und Systeme unterstützt?"), bei dem das Wissen der IT-Verantwortlichen stärker gefragt ist. In jedem Fall sollten das Wissen und die Einschätzungen der Prozess- wie auch der IT-Verantwortlichen in die Auswahl einfließen, damit sowohl der prozedurale als auch der technische Stellenwert der IT-Komponenten angemessen berücksichtigt werden.

Analyse und Risikoszenarien

Für die als kritisch identifizierten IT-Komponenten ist zu untersuchen, welche Risiken sich aus möglichen Bedrohungen, vorhandenen Schwachstellen und drohenden Schadensauswirkungen ergeben. Dieser Analyse sollten komplexe Risikoszenarien zugrunde gelegt werden, beispielsweise die Gefahr von Hackereinbrüchen aufgrund ungeschützter Fernwartungszugänge, die Anfälligkeit gegen Schadsoftware durch Missbrauch offener USB-Ports oder das Ausspähen vertraulicher Daten bei unverschlüsselter Netzkommunikation. Für die Bewertung eines Risikoszenarios können Faktoren betrachtet werden, die ein mögliches Eintreten positiv oder negativ beeinflussen. Die Wahrscheinlichkeit, dass eine Schwachstelle ausgenutzt wird, ist beispielsweise umso größer, je bekannter sie ist und je zugänglicher ein betroffenes System ist, ferner umso weniger Kenntnisse und Ressourcen für einen erfolgreichen Angriff nötig sind. Umgekehrt sinkt die Wahrscheinlichkeit von Angriffen in der Regel, wenn diese leicht zu entdecken und die Angreifer einfach zu identifizieren sind. Hingegen erhöht der Trend zur Vernetzung der Produktions-IT bei vermehrter Verwendung von Standard-Komponenten die Wahrscheinlichkeit erfolgreicher Angriffe signifikant, da das Wissen um deren Schwachstellen allgemein verbreitet und damit auch Angreifern leicht zugänglich ist.

Bei der Auswahl und dem Zuschnitt von Maßnahmen zur Risikominimierung ist neben deren Wirksamkeit und Wirtschaftlichkeit insbesondere auch deren Eignung im Anwendungskontext zu berücksichtigen. Dieser ist insbesondere durch die folgenden Merkmale charakterisiert:

- Im Unterschied zur Büro-IT, bei der Vertraulichkeit vorrangiges Sicherheitsziel ist, haben im Produktionsumfeld die Verfügbarkeit und das korrekte Funktionieren (die „Integrität") der Systeme die höchste Priorität. Sicherheitsmaßnahmen verbieten sich oft, wenn sie wie ein automatisiertes Patchmanagement oder der Echtzeitbetrieb von Virenscannern die Abläufe auch nur geringfügig zu verzögern drohen.
- Während übliche Büro-IT nur wenige Jahre genutzt wird, haben Produktionsanlagen meistens Laufzeiten von weit über zehn Jahren. Da jede Softwareänderung das Funktionieren einer Anlage gefährdet, können sicherheitsrelevante Aktualisierungen nicht oder nur eingeschränkt eingespielt werden. Haftungsregelungen der Hersteller untersagen zudem oft eigenmächtige Modifikationen. Es kann daher unterstellt werden, dass ein Großteil der IT im Produktionsumfeld hochgradig unsicher ist – ein Risiko, das sich angesichts immer neu entdeckter Software-Schwachstellen stetig verschärft.
- Die Produktions-IT ist ausgesprochen heterogen, was den Administrationsaufwand erhöht und die durchgängige Anwendung von Sicherheitsrichtlinien erschwert. Organisatorische Mängel kommen hinzu: So fehlt es vielfach an Personal, das neben fachlichem Know-how auch solches zur IT-Sicherheit hat. Oft sind auch die Zuständigkeiten unzureichend geregelt, was unter anderem dazu führt, dass Anlagen ohne Berücksichtigung von IT-Sicherheitsaspekten beschafft und in Betrieb genommen werden – IT-Sicherheitsvorfälle sind damit vorprogrammiert.

Breites Spektrum an Maßnahmen

Die erwähnten Standards und Best-Practice-Darstellungen zur Sicherheit industrieller IT zeigen ein breites Spektrum möglicher Maßnahmen auf. Dazu zählen starke Authentisierungsverfahren als Vorbedingung für den Zugriff auf kritische Systeme, die netztechnische Separierung der Systeme oder aber die Deaktivierung von USB-Ports und anderen problematischen Schnittstellen. Zur Verringerung von IT-Risiken tragen neben der gezielten Absicherung und Härtung einzelner Systeme sowie einer am Schutzbedarf orientierten Netzsegmentierung insbesondere aber auch übergreifende organisatorische Maßnahmen bei. Eine große Breitenwirkung kann etwa erzielt werden, wenn

- die mit den Produktionsanlagen verknüpften IT-Komponenten besser dokumentiert werden,
- die betroffenen Mitarbeiter – dies können sowohl Führungskräfte als auch Anlagenbediener sein – für mögliche Gefährdungen und den sicherheitsgerechten Umgang mit IT sensibilisiert und geschult sind und
- durch Vorgaben und Vorabprüfungen vor der Beschaffung dafür gesorgt wird, dass Anlagen gute Sicherheitseigenschaften aufweisen, also etwa nicht mit bereits schon veralteten Betriebssystemen ausgeliefert werden und das Patchmanagement mit den Herstellern verbindlich geregelt ist.

Wichtigste Voraussetzung für ein nachhaltiges IT-Risikomanagement in der industriellen Fertigung ist es jedoch, dass die zugehörigen Aufgaben – dazu gehört auch die kontinuierliche Überwachung der Risiken – im Unternehmen organisatorisch verankert sind. Insbesondere sind spezielle Verantwortlichkeiten für IT-Sicherheit in diesem Bereich zu schaffen und sind deren Zusammenarbeit mit den Anlagen- und Geschäftsprozessverantwortlichen sowie die Schnittstellen zum übergeordneten Risiko- und Informationssicherheitsmanagement des Unternehmens zu regeln. Gut aufgestellte IT-Sicherheitsorganisationen in den Unternehmen geben nicht zuletzt auch Herstellern und Integratoren zusätzliche Impulse zur Entwicklung und Bereitstellung sicherer IT-Systeme in der industriellen Fertigung. ■

Autoren
Mechthild Stöwer,
Abteilungsleiterin Security Management (SMA)

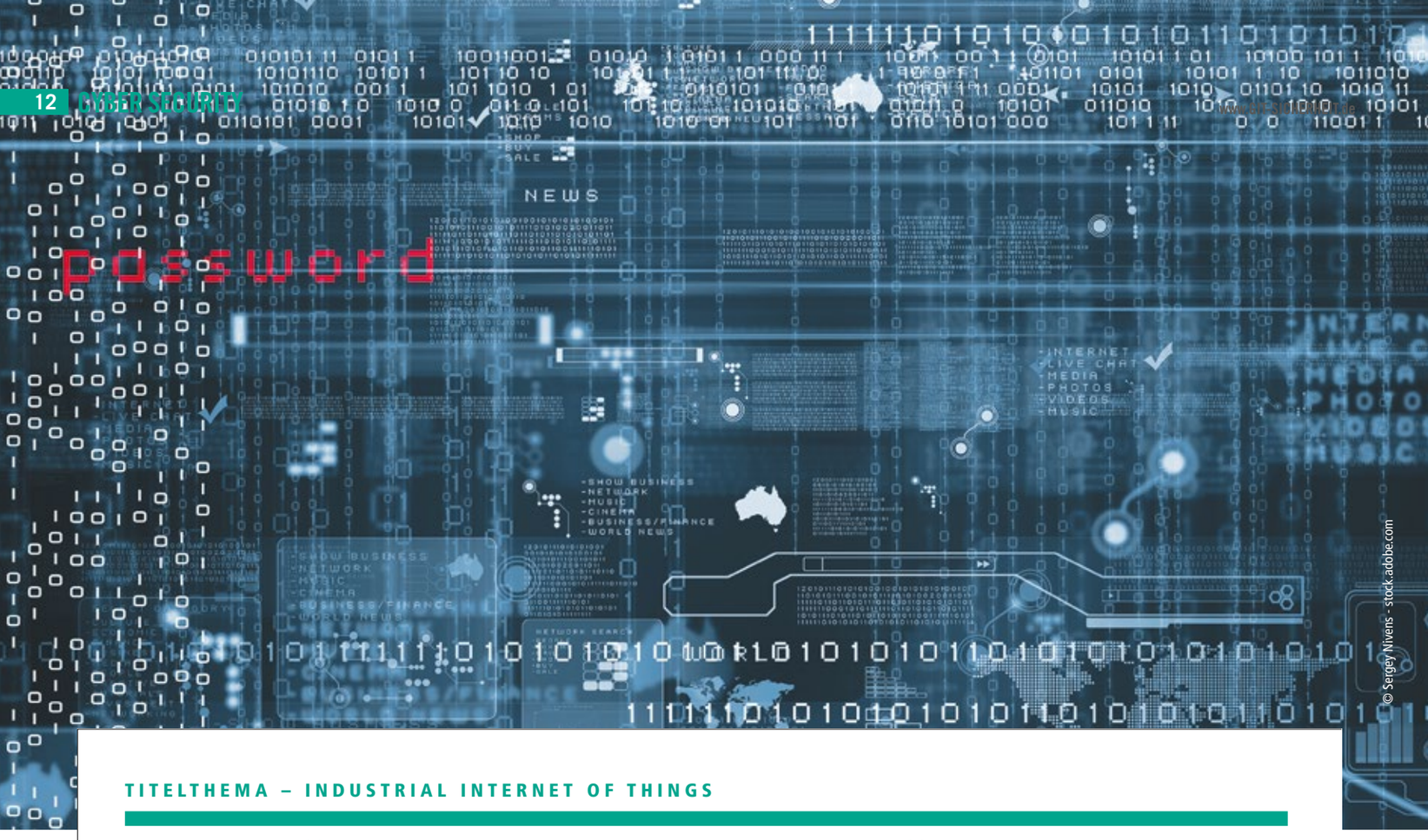
Reiner Kraft,
Wissenschaftlicher Mitarbeiter und Projektleiter am SIT

Der Cyber-Check

- Kritische IT identifizieren
- IT-Risiken analysieren
- IT-Risiken behandeln
- IT-Risiken überwachen

Kontakt

Fraunhofer-Institut für Sichere Informationstechnologie – SIT
Abteilung Security Management
Sankt Augustin
Tel.: +49 2241 14 3272
info@sit.fraunhofer.de
www.sit.fraunhofer.de



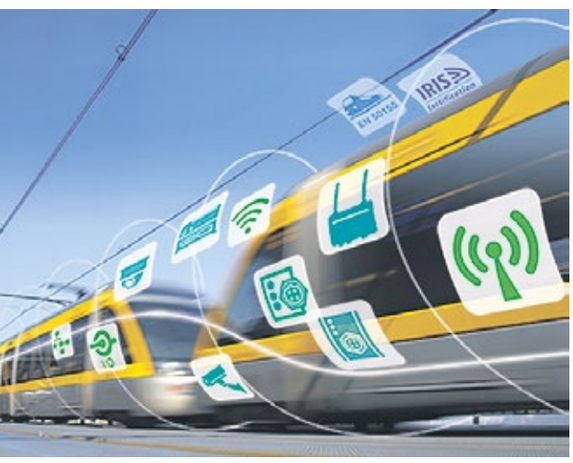
© Sergey Nivens - stock.adobe.com

TITELTHEMA – INDUSTRIAL INTERNET OF THINGS

Der Cybersecurity-Standard, der IIoT-Netzwerke schützt

Netzwerkgeräte mit IEC 62443-4-2 absichern

Die Verbreitung des IIoT, sprich des Industrial Internet of Things, geht mit immer mehr vernetzten Geräten einher. Während dieser Trend die Betriebseffizienz steigert, erhöhen sich gleichzeitig auch die Gefahren durch Cyberangriffe. Doch es gibt Lösungen.



Moxa: Kompetenz in Sachen Cybersecurity für den Schienenverkehr

Die Bedenken von Eignern und Betreibern sind gerechtfertigt – gemäß einschlägiger Erhebungen ist die Anzahl von Cyberattacken insbesondere in der Fertigung gestiegen. Mit den passenden Lösungen lassen sich jedoch in sämtlichen Branchen sichere Systeme für den Betrieb von IIoT-Netzwerken schaffen, auch in so betriebskritischen Bereichen wie zum Beispiel dem Schienenverkehr.

Partnerschaften für den Erfolg im intelligenten Schienentransport – Cybersecurity für Schienenverkehrsnetzwerke

Keine Frage: Die schnelle Urbanisierung steigert auch weiterhin die Nachfrage nach Schienentransportlösungen – nicht nur in Metropolen, sondern auch für länderübergreifende Transportwege. Da ist es interessant zu wissen, dass das Unternehmen Moxa flexible, erweiterbare und sichere IP-Netzwerkinfrastrukturen liefert, die mit der steigenden Anzahl von Fahrgästen mithalten können und dabei die Betriebseffizienz erhalten.

Sichere Geräte und Netzwerke – sicher überwacht und verwaltet

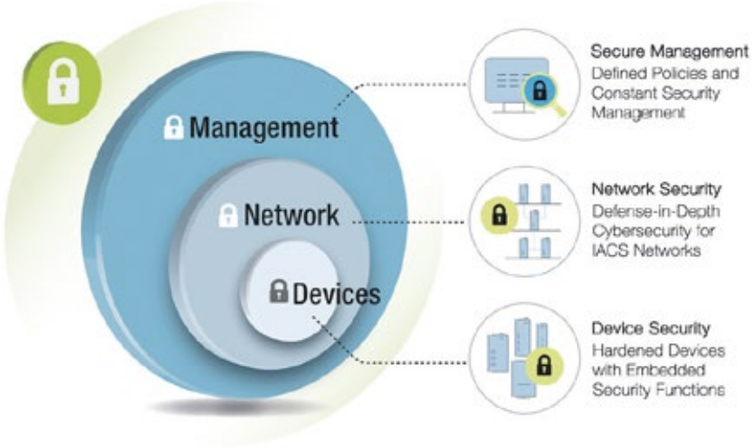
Das Industrial Internet of Things hat auch auf der Schiene seine ganz besonderen Facetten. Die im Rahmen des IIoT immer stärker vernetzten Züge sind anfällig für Cyberattacken. Um Schienenverkehrsnetze abzusichern, sind robuste Netzwerkkommunikation mit erweiterten Sicherheitsfunktionen und einfach zu bedienende Managementsoftware erforderlich. Die effektivste Methode zur Verbesserung der Gerätesicherheit ist es, sicherzustellen, dass sich Einstellungen nicht derart verändern lassen, dass die Geräte und damit letztlich das Netzwerk gefährdet werden.

Cybersecurity-Experten sehen den IEC 62443-Standard als den relevantesten für die Absicherung von Geräten in Industrienetzwerken an. Moxas Industrial Ethernet Switches verfügen mit der Firmware Turbo Pack 3 über den IEC 62443-4-2 Cybersecurity-Standard und unterstützen zusätzlich weitere Sicherheits-Managementfunktionen, wie MAC Address und RADIUS-Authentifizierung, um nicht autorisierten Zugriff, bekannte Sicherheitslücken sowie unvorhersehbare Angriffe auf IIoT-Netzwerke zu verhindern.

Defense-in-Depth

Beim Entwurf eines Netzwerks ist es außerdem eine gute Vorgehensweise, die Defense-in-Depth-Sicherheitsarchitektur zu nutzen, die

Zuverlässige und geprüfte Systeme



Defense-In-Depth Framework

zum Schutz individueller Zonen und Zellen entworfen wurde. Der erste Schritt, den man beim Entwurf eines Defense-in-Depth-Schienenverkehrssystems machen sollte, ist die Segmentierung von Netzwerken, sodass der Verkehr isoliert werden kann, um ihn gegen Cyberattacken oder menschliche Fehler zu schützen. Sind die Netzwerkgeräte und -topologie sicher, muss eine Leitlinie für die Netzwerkverwaltung erstellt werden, so dass Betreiber einen vollständigen Überblick über den Sicherheitsstatus des gesamten Netzwerkes erhalten.

Sicher und effizient im Schienenverkehr

Moxa bietet ein umfangreiches Produktportfolio für Zugbetreiber und Systemintegratoren an, das entsprechend der EN 50155- und IEC 62443-Standards entworfen wurde. Über 500 Netzwerke für CCTV, CBTC, TCMS, Fahrgast-Wi-Fi und Zustandsüberwachung hat Moxa bereits weltweit installiert. Als IRIS rev 0.3-zertifizierter Hersteller erfüllt Moxa auch den ISO/TS 22163:2017 Standard für Qualitäts- und Business-Managementsysteme im Schienenverkehrswesen.

Das Unternehmen entwickelt aktiv innovative Technologien und teilt seine Expertise in den globalen Verbänden des Schienenverkehrswesens, wie dem IEC Technical Committee 9/WG 43, einem Vorreiter in Design und Entwicklung von Schienenverkehrsprodukten der nächsten Generation. Ein gutes Stück Sicherheit also, was da von Moxa geboten wird - Cybersecurity inklusive. ■

Kontakt

Moxa Europe GmbH
Unterschleißheim
Tel.: +49 89 37003990
www.moxa.com

CYBER SECURITY UND DSGVO

Schutz vor Attacken

Tipps von VdS zum Schutz vor Cyber-Attacken und zum Umsetzen der EU-Datenschutzgrundverordnung

© Sergey Nivens/Shutterstock

vds.de/cyber: beide Richtlinien VdS 3473 (Informationssicherheit) und VdS 10010 (Datenschutz) kostenlos zum Download

Die Unternehmenssicherheit mit ihren klassischen Handlungsfeldern Brandschutz, Security (Schutz gegen Einbruch, Diebstahl, Sabotage) und Naturgefahren (z. B. Überschwemmung, Starkregen) muss heute um den Aspekt der Cyber-Security ergänzt werden. Denn: Die Nutzung moderner IT zur Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen in Unternehmen sowie der Anschluss an das Internet sind heute unabdingbare Erfordernisse, um im weltweiten Wettbewerb bestehen zu können. Die Digitalisierung und die Vernetzung bieten allerdings eine breite Angriffsfläche für Cyber-Kriminelle. Hierzu in unserem Interview: Markus Edel, studierter Produktionstechniker und Leiter des Bereichs Cyber-Security bei VdS. Das Institut bietet umfassende Leistungen zur Absicherung speziell von Mittelständlern in den Bereichen Informationssicherheit und Datenschutz.

GIT SICHERHEIT: Herr Edel, unsere Leser berichten, dass ihre IT-Abteilungen gerade vor allem zwei große Themen zu bewältigen haben: Absicherung gegen die immer zahlreicheren digitalen Angriffe sowie die aufwändige Umsetzung der EU-Datenschutzgrundverordnung. Zu beiden Hauptaufgaben bieten Sie kostenlose Richtlinien an. Dann haben Sie für unsere Leser sicher auch ein paar Tipps zur Bewältigung dieser Herausforderungen parat. Doch der Reihe nach: Medienberichte über IT-Attacken nicht nur auf Firmen sind schon so häufiger wie trauriger Standard geworden. Und die Zerstörungskraft der Angriffe steigt immer weiter. Was können, was müssen Unternehmensverantwortliche hier tun? Gibt es typische Schwachstellen, auf die Sicherheitsmanager verstärkt achten sollten?

Markus Edel: Das ganz erhebliche und zudem täglich gravierender werdende Problem sind die „offenen digitalen Scheunentore“ in zu vielen KMU,

um mal die bildhafte Sprache vieler IT-Experten zu zitieren. Gerade die Produktionsmaschinen im Mittelstand sind oft nicht auf dem erforderlichen Sicherheitsniveau – und zwar, leicht paradox, eben wegen der starken Prozessoptimierung in diesen Firmen. Immer wieder hören wir von Fertigungsleitern, dass wichtige Sicherheits-Updates nicht installiert werden können, weil die Zeitspanne zum Einspielen und vor allem der danach oft nötige Neustart der Systeme den durchgetakteten Betriebsablauf zu sehr stören würden. Die Folge: Wertvolles Wissen über industrielle Prozesse, die sogenannten „Kronjuwelen", stehen für digitale Angreifer zu häufig nahezu offen. Und diese Angreifer gibt es in Hülle und Fülle: Dass die Ideen unseres äußerst erfindungsreichen Mittelstandes bekanntermaßen auf der ganzen Welt begehrt sind, macht die 3,6 Millionen deutschen KMU zu einem bevorzugten Ziel sowohl für Spionage als auch für Zerstörung durch Cyber-Aktivitäten, macht Deutschland zu dem weltweit am stärksten von IT-Kriminalität betroffenen Land.

Für diese sehr lukrative kriminelle „Wertschöpfung" sind nicht einmal spezielle IT-Kenntnisse nötig. Unzählige Schadsoftwarevarianten und Angriffstools lassen sich im Darknet – und nicht nur dort – schnell und günstig einkaufen. Oft inklusive: eine Erfolgsgarantie! Verschlüsselungstrojaner sind und bleiben ein hohes Risiko. Unlängst wurde zudem eine gravierende Sicherheitslücke in einigen Prozessorfamilien bekannt, die Zugriff auf fast alle Bereiche der Rechner ermöglicht. Diese Prozessoren wurden in großer Zahl verbaut, also sind gerade Firmen mit moderner Infrastruktur betroffen – diese Lücke ist für Hacker perfekt, um ganz gezielt Exploits einzusetzen. Hinzu kommen die „herkömmlichen" Viren und Malware, die jeden Computer bedrohen – natürlich auch den Laptop des Entwicklungsingenieurs, der dort vielleicht die unersetzlichen Konzepte für den nächsten Patentantrag abgelegt hat. Wannacry übrigens war Experten zufolge eher stümperhaft programmiert, richtete aber trotzdem auf der ganzen Welt Milliardenschäden an. Und natürlich wird seine „Erfolgsgeschichte" zahlreiche Nachahmer auf den Plan rufen.

Gerade Maschinen und Anlagen sind Berichten zufolge gefährdete Ziele...

Markus Edel: ...und auch die VdS-Cyber-Audits bestätigen viel zu häufig: Gerade Automatisierungssysteme, die im 24/7-Betrieb laufen, haben seit Windows XP, in einigen Fällen sogar seit noch längerer Zeit, kein Update mehr gesehen. Die Cyber-Kriminellen dagegen haben ihre Angriffsmechanismen über Jahre hinweg immer weiter verbessert. Das daraus resultierende Spannungsfeld tendiert zu Ungunsten der IT-Anwender – wenn nicht die erforderlichen Gegenmaßnahmen ergriffen werden.

Und täglich gehen zig weitere industrielle Anlagen ins Netz, zwecks der sinnvollen digitalen Fernwartung oder Auslastungsüberwachung per Internet. Das eröffnet Hackern immer mehr und noch mehr Zugriffsmöglichkeiten. Schon jetzt wird unser volkswirtschaftlicher Schaden durch Cyber-Kriminalität auf 55 Milliarden Euro im Jahr geschätzt – heftige 1, 9 % Prozent des Bruttoinlandsprodukts. Tendenz allen Experten zufolge: Sehr stark steigend.

> „Gleich nach Abschluss des Quick-Audits weiß das auditierte Unternehmen, ob die Cyber-Security-Maßnahmen der aktuellen Bedrohungslage angemessen sind – inklusive präziser Hilfestellungen zum Beseitigen möglicher Einfallstore der Kriminellen."

Kostenlose Web-Quick-Checks: Sofortige, individuelle Ermittlung des Cyber-Schutzstatus und des DGSVO-Erfüllungsgrades (auch speziell für die Prozessautomatisierung): vds-quick-check.de

Was können Unternehmensverantwortliche also tun? Jeder weiß, dass digitale Zugänge ins Unternehmensnetz gesichert werden müssen. Nur gilt hier wie für jedes physische Schloss: Kriminelle, die über das nötige Können verfügen und auch genug Zeit zur Verfügung haben, werden viele Sicherheitsmechanismen irgendwann überwinden. Das Können läßt sich äußerst günstig einkaufen – und auch die nötige Zeit haben Hacker fast immer, denn im Schnitt registrieren Unternehmen digitale Angriffe erst nach rund 200 Tagen, wenn überhaupt. Handlungsdruck ist also durchaus gegeben: Wir müssen uns besser und systematisch schützen, und das schnell!

Was sind die Ihrer Meinung nach wichtigen Schritte dort hin?

Markus Edel: Für Informationssicherheit existieren mit der DIN ISO IEC 27001 und dem BSI-Grundschutz zwei wirklich gute Vorlagen. Nur ist die Umsetzung dieser beiden sehr umfassenden Standards für viele Mittelständler personell wie materiell auch beim besten Willen nicht zu leisten. Deswegen hat VdS, wie Sie auch in der GIT berichteten, mit den Richtlinien 3473 „Cyber-Security für kleine und mittlere Unternehmen" den ersten IT-Sicherheitsstandard speziell für den Mittelstand geschaffen. Diese pragmatische Lösung steht bereits unter den Top-3 der implementierten Managementsysteme für Informationssicherheit, wie eine BSI-Studie bestätigt. Einer unserer Anwender nennt die VdS 3473 in einem aktuellen Interview in der Computerwoche „die wohl praktikabelste Umsetzungsmöglichkeit für ein ISMS in kleinen und mittleren Unternehmen". Diesen prämierten Leitfaden – und ebenso die angesprochenen Hilfestellungen zur DSGVO-Umsetzung, auf die ich gleich noch zu sprechen komme – stellen wir im Internet kostenlos zur Verfügung.

Die Richtlinien 3473 sowie 10020 speziell für industrielle Automatisierungstechnik enthalten praxisnahe Vorgaben zur Sicherstellung einer zuverlässigen organisatorischen sowie technischen Umsetzung von Informationssicherheit. Mit 20 % des Aufwandes der ISO- oder BSI-Vorgaben.

Wie steht es um ganz konkrete Tipps?

Markus Edel: Ganz konkrete Tipps aus den VdS 3473 für Ihre Leser: Jedes Unternehmen verfügt über besonders exponierte IT-Systeme und meist

auch über solche, bei denen über das Netzwerk ausnutzbare Schwachstellen vorliegen. Beide sind gemäß Abschnitt 10.3.2 von der restlichen IT-Infrastruktur abzukapseln, indem der Netzwerkverkehr auf das für die Funktionsfähigkeit notwendige Minimum beschränkt wird. Dadurch soll erreicht werden, dass Sicherheitsprobleme an diesen Stellen gar nicht erst entstehen. Sollte ein solches Problem dennoch auftreten, wird durch die Beschränkung des Netzwerkverkehrs verhindert, dass sich die Schadsoftware ungehindert verbreiten kann. Denn die Schadenhöhe hängt natürlich von Art und Menge der betroffenen Unternehmensdaten ab. Eine ganz simple Gegenmaßnahme: Die strukturierte Verwaltung von Zugängen und Zugriffsrechten. In vielen Firmen können Mitarbeiter auf Verzeichnisse zugreifen, die sie für ihre Arbeit gar nicht benötigen, was die zerstörerische Wirkung jedes Schadenprogrammes potenziert. Also: Zugänge nur genehmigen, „wenn sie für die Aufgabenerfüllung des jeweiligen Nutzers oder für die betrieblichen Abläufe des Unternehmens notwendig sind". Und sie bei Beendigung oder Wechsel der Anstellung eines Nutzers „umgehend überprüfen und bei Bedarf anpassen" – was ohne unsere Richtlinien sehr gern und häufig vergessen wird. So verringern wir gemeinsam die Wahrscheinlichkeit, dass über E-Mail-Konten eingeschleppte Malware schwerwiegende Schäden verursacht. Ganz wichtig, sozusagen an erster Stelle stehend, sind auch die umfassenden Vorgaben der VdS 3473 für regelmäßige Backups. Da können sich Locky, Wannacry, Petya, Rapid und ihre ganz sicher kommenden stärkeren Verwandten ruhig austoben – ihre Zerstörung wird in sehr engen Grenzen gehalten.

Oft wird ja der Mensch als „Risikofaktor" genannt...

Markus Edel: ...daher ist weiter die Schulung der Mitarbeiter entscheidend. Informationssicherheit ist eine Managementaufgabe, ist in einen organisatorischen Kontext zu stellen und ganzheitlich umzusetzen. Übrigens adressiert unser Leitfaden zur DSGVO-Umsetzung, den ich noch näher erläutern werde, ebenso wie die VdS 3473 die Geschäftsführung – denn auch Datenschutz ist keinesfalls ein reines IT-Thema, sondern Chefsache. Zurück zur generellen Informationssicherheit: Die VdS 3473 fordern, das betroffene

Markus Edel, Leiter der Zertifizierungsstelle für Managementsysteme von VdS

Personal zielgruppenorientiert über Gefährdungen aufzuklären und im Umgang mit Sicherheitsmaßnahmen zu unterweisen. Diese Schulungen und Sensibilisierungen der Mitarbeiter müssen geplant, gesteuert und stetig verbessert werden. Informationssicherheit funktioniert nur, wenn sie im Unternehmen gelebt wird. Den Kriminellen wird immer etwas Neues einfallen – deshalb ist die ganzheitliche Ausrichtung des VdS-Standards so wichtig. Leider sehen sich viele Unternehmen in diesem wichtigen Punkt schlecht aufgestellt: 29 % der bisher 3.000 Nutzer unseres Web-Quick-Checks, mit dem auf www.vds-quick-check.de schnell und kostenlos der Status der eigenen IT-Sicherheit bestimmt werden kann, bewerten die Ganzheitlichkeit ihrer eigenen Cyber-Security als mangelhaft. Vorteil für Unternehmen, die nach dieser Erkenntnis die VdS 3473 einsetzen: Gerade auf diesem Gebiet kann mit geringen Mitteln viel erreicht werden. Schon sehr kostengünstig und mit minimalem Aufwand umsetzbare Kleinigkeiten erzielen eine große Wirkung. Wichtig sind z. B. eine klare Informationssicherheitsleitlinie, die vom Topmanagement verabschiedet und entsprechend im Unternehmen kommuniziert wird, mit präzisen Vorgaben auch für die private Nutzung der Unternehmens-IT und vor allem für externe Mitarbeiter – beides gravierende Einfallstore bei Cyber-Angriffen, ob bewusst oder unbewusst. Ein kleiner Schritt mit großer Wirkung für die Unternehmenssicherheit ist auch, administrative Zugänge ausschließlich den Administratoren der Firma vorzubehalten und diese Zugänge nach einem festgelegten, regelmäßigen Turnus auf ihre weitere Notwendigkeit hin zu überprüfen. Dies blockt von vorneherein zahlreiche Möglichkeiten der Cyber-Kriminellen, einem Betrieb und damit seinen Angestellten Schaden zuzufügen. Ein weiter Tipp: Für jedes IT-Outsourcing- und Cloud-Computing-Vorhaben die notwendigen Anforderungen an die Sicherheit definieren. Der Vertrag mit jedem Dienstleister hierfür sollte präzise Rechts- und Sicherheitsvorgaben enthalten und zur Erfüllung verpflichten.

Ein wichtiges Sicherheitsinstrument ist das VdS-Quick-Audit direkt im Unternehmen. Ein VdS-Experte analysiert dabei vor Ort sowohl das technische als auch das organisatorische Schutzspektrum. Der umfassende Bericht nach Abschluss der meist eintägigen Untersuchung deckt direkt bestehende Sicherheitslücken auf und bietet präzise Vorschläge zur Verbesserung der individuellen Informationssicherheit.

Das zweite brandaktuelle Thema nicht nur für die IT-Sicherheitsverantwortlichen ist natürlich die EU-Datenschutzgrundverordnung. Studien gehen davon aus, dass 90 % der KMU die 300 Seiten starke Verordnung noch nicht umgesetzt haben, trotz drohender Strafzahlungen in Millionenhöhe seit dem Geltungsstichtag am 25. Mai. VdS hat zur DSGVO-Erfüllung einen Leitfaden entwickelt, über den wir in vergangenen Ausgaben bereits berichtet haben – was genau raten Sie den 90 %?

Markus Edel: Wie GIT SICHERHEIT Leser wissen: Die bedeutsamste Veränderung zur bisherigen Rechtslage ist die sogenannte Rechenschaftspflicht. Konkret fordert diese: Jedes Unternehmen, das personenbezogene Daten verarbeitet, selbst jeder Ein-Mann-Betrieb, und ebenso jede Behörde, muss jederzeit und vollständig nachweisen können, dass sämtliche Vorgaben der DSGVO eingehalten werden. Das können Unternehmen nur auf eine Art leisten, und zwar durch das Einrichten eines Datenschutz-Managementsystems. Dies ist ein Führungssystem, kein technisches Hilfsmittel; es kann allerdings durch ein solches unterstützt werden. Nötig ist seit dem 25. Mai – und die beliebten Abmahnanwälte sind bestimmt schon sehr aktiv – ein Regelrahmenwerk mit klar definierten Leit- und Richtlinien, Prozessen, Rollen und Verantwortlichkeiten sowie Kontrollmechanismen. Dazu kommen die üblichen Anforderungen an prüffähige Dokumentationen und klare Kommunikationsregeln. Um den DSGVO-Umsetzungsprozess speziell für KMU zu erleichtern, haben wir die kompakten Richtlinien VdS 10010 erstellt.

Die junge VdS-Publikation zeigt einen Weg auf, die rechtlichen, organisatorischen und technischen Anforderungen der DSGVO so strukturiert wie möglich und vor allem mit überschaubarem Aufwand umzusetzen. Unsere Richtlinien bündeln die DGSVO-Forderungen auf 32 Seiten, und das auditierungs- und zertifizierungsfähig. Auch im Kompetenzfeld Datenschutz unterstützen wir übrigens mit umfassenden Dienstleistungen rund um die gelungene Umsetzung, z.B. durch die Services VdS-anerkannter Datenschutz-Managementsystem-Berater, mit zahlreichen maßgeschneiderten Bildungsangeboten und auch durch einen ebenfalls kostenlosen Quick-Check zum DSGVO-Erfüllungsgrad nach 26 Fragen. Ein großer Vorteil für die Umsetzungsverantwortlichen ist sicher, dass die VdS 10010 sich an den Richtlinien VdS 3473 zur Cyber-Security orientieren und über weite Strecken gleichartig aufgebaut sind, was erhebliche Synergieeffekte bei diesen wichtigen Themen mit sich bringt. So können die geforderten Leit- und Richtlinien zusammengefasst abgebildet, das Wissensmanagement und vor allem die Sensibilisierung der Mitarbeiter direkt in einem geplant und durchgeführt werden. Denn natürlich stellt die DSGVO ebenso zahlreiche Anforderungen an die Informationssicherheit hinsichtlich des Schutzes der personenbezogenen Daten – welche die VdS 3473 praxisgerecht mit abdecken. Durch die Synergien der VdS 3473 und VdS 10010 sparen die Verantwortlichen im Mittelstand und in Behörden Aufwand und Kosten bei der Implementierung der erforderlichen Maßnahmen sowie auch bei einer möglicherweise gewünschten VdS-Zertifizierung – und können sich so schneller und vor allem ungestört von kriminellen Störenfrieden auf ihre Kern-Erfolgsprozesse konzentrieren.

Herr Edel, wir danken für das Gespräch.

Kontakt

Markus Edel
VdS Schadenverhütung GmbH, Köln
Tel.: +49 221 7766-380
medel@vds.de
www.vds.de

DSGVO VS. VIDEOÜBERWACHUNG

Welche Funktionen sind nötig?

DSGVO-konforme Videosicherheitstechnik einfach implementiert

Das Thema DSGVO ist spätestens seit dem Mai des Jahres 2018 stark strapaziert - und gerade beim Einsatz von Videotechnik herrscht weiterhin viel Unklarheit darüber, welche Anforderungen Unternehmen erfüllen müssen. Unsicherheit herrscht auch darüber, welche Systemfunktionen notwendig sind, um Videosicherheitssysteme auf einfache Weise DSGVO-konform konfigurieren können.

Viele Endanwender stellen fest, dass die neue europäische Datenschutz-Grundverordnung (DSGVO) selbst keine spezifische Regelung zur Videoüberwachung enthält, weshalb sich die DSGVO-konforme Umsetzung für jedes Unternehmen anders darstellt. Zudem ist davon auszugehen, dass neben noch ausstehender Rechtsprechung und damit der tatsächlichen Auslegung in der Praxis auch unternehmensspezifisch – beispielsweise durch unterschiedliche Entscheidungen der Betriebsräte – Unterschiede bezüglich der Videosicherheit zu erwarten sind. Neben dem Datenschutz kommt hierbei nun auch der Datensicherheit ein höherer Stellenwert zugute, da dadurch erhobene Daten vor Verlust oder Manipulation geschützt werden sollen. Somit gilt: Kein Datenschutz ohne Datensicherheit, und Unternehmen müssen die DSGVO in beiden Bereichen erfüllen. Für viele Firmen stellt sich nun die Frage, welche Komponenten notwendig sind, um die Anforderungen konkret erfüllen zu können. Hersteller bieten hier unterschiedliche Ansätze, das Datenschutz- und Datensicherheitsmodul von Dallmeier bietet beispielsweise 14 verschiedene Komponenten.

Datenschutz – Schutz der Rechte der betroffenen Personen

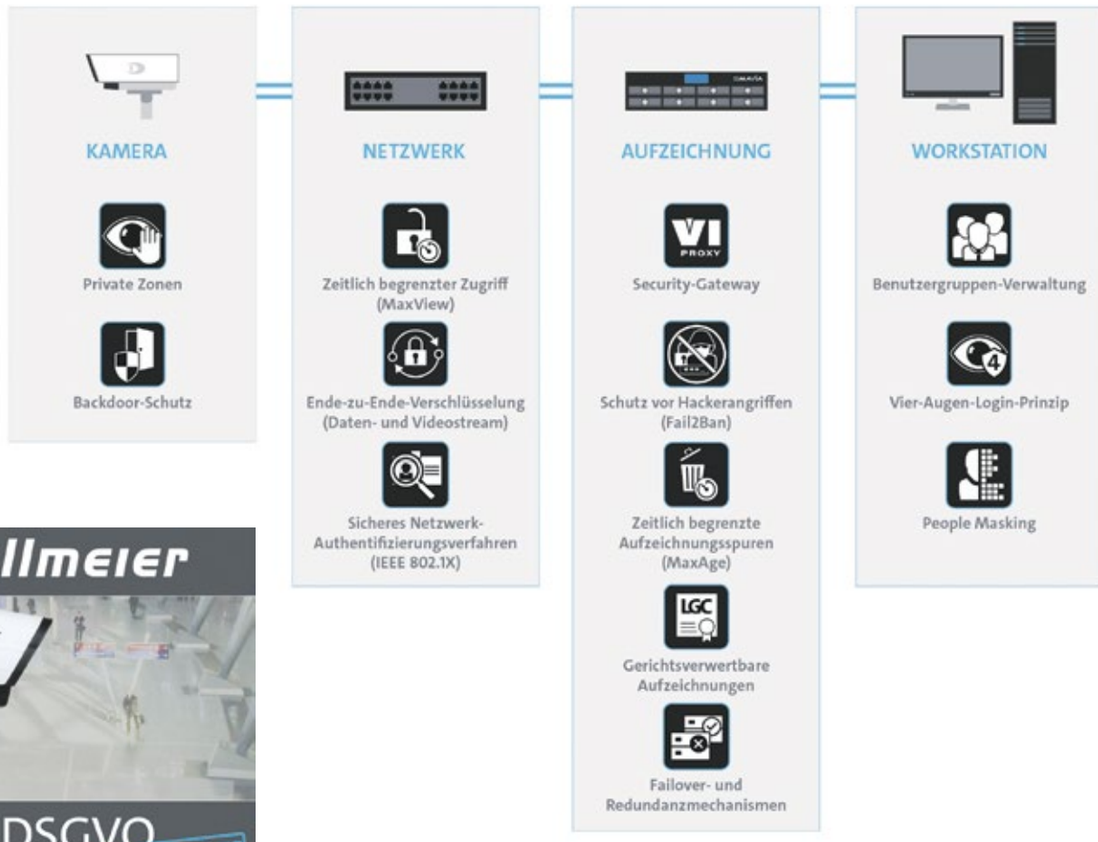
Beim Datenschutz geht es darum, wie in Art. 25 der DSGVO gefordert, geeignete technische und organisatorische Maßnahmen zu treffen, um Datenschutzgrundsätze und die Rechte der betroffenen Personen zu wahren. Im Modul von Dallmeier finden sich dazu vier wesentliche Komponenten:

- Die Verpixelung von ganzen Personen durch „People Masking“, die bei Bedarf rückgängig gemacht werden kann.

Bitte umblättern ▶

Über Dallmeier

Dallmeier verfügt über eine mehr als 30-jährige Erfahrung in der Übertragungs-, Aufzeichnungs- und Bildverarbeitungstechnologie und ist als Pionier und Vorreiter im Bereich von CCTV/IP-Lösungen weltweit anerkannt. Das profunde Wissen wird in der Entwicklung intelligenter Software und der Herstellung qualitativ hochwertiger Recorder- und Kameratechnologie eingesetzt. Das ermöglicht dem Unternehmen Dallmeier, nicht nur Stand-alone Systeme, sondern komplette Netzwerklösungen bis hin zu Großprojekten mit perfekt aufeinander abgestimmten Komponenten anzubieten.



▲ **Überblick: EU-DSGVO Topologie**

Dallmeier-DSGVO-Modul bietet Funktionen zum Schutz vertraulicher oder personenbezogener Daten vor Manipulation, Verlust oder unberechtigtem Zugriff ▼

Fortsetzung von Seite 17 ▶

- Die Einrichtung von „Privaten Zonen" im erfassten Bild, um z.B. öffentliche Bereiche unsichtbar zu machen. Diese Abdeckung kann weder live noch in der Aufzeichnung rückgängig gemacht werden.
- Die Festlegung der Speicherdauer für jede einzelne Kamera bzw. Aufzeichnungsspur, um eine Löschung nach Zweckerfüllung zu garantieren.
- Die Sichtbarmachung von datenschutzrechtlich irrelevanten Bereichen durch detaillierte, virtuelle 3D-Simulation bereits bei der Projektplanung. So lässt sich einerseits feststellen, wo die Bildqualität keine Personenerkennung zulässt und daher keine personenbezogenen Daten entstehen. Anderseits können für datenschutzrelevante Bereiche die Funktionen, wie z. B. People Masking, bereits im Vorfeld maßgeschneidert geplant werden.

Datensicherheit – Schutz der personenbezogenen Daten selbst

Für den Bereich Datensicherheit legt die DSGVO in Art. 32 fest, dass geeignete technische und organisatorische Maßnahmen ergriffen werden, um ein angemessenes Schutzniveau zu gewährleisten, das den Sicherheitsrisiken angemessen ist. Zum Schutz vertraulicher oder personenbezogener Daten vor Manipulation, Verlust oder unberechtigtem Zugriff bietet das Dallmeier-Modul folgende Funktionen:

- Das optionale „Vier-Augen-Prinzip", das beim Zugriff auf Aufzeichnungen zwei Passwörter verlangt.
- Die Benutzergruppenverwaltung über AD/LDAP zur Regelung der Zugriffsrechte.
- Ein sicheres Netzwerk-Authentifizierungsverfahren gemäß IEEE 802.1X zum Schutz des Netzwerks vor unberechtigtem Zugriff.
- Eine Ende-zu-Ende Verschlüsselung mit TLS 1.2 / 256 Bit AES für den Schutz sowohl der Daten- als auch der Videoübertragung zwischen aktuellen Dallmeier-Systemen.
- Die Festlegung der Aufzeichnungszeit für jede Benutzergruppe. Bilder, die älter als der eingestellte Zeitraum sind, können nicht ausgewertet werden.
- Das sichere Erkennen und Verhindern von Verbindungsversuchen durch Hackerangriffe. Werden wiederholte Verbindungsversuche von einer unbekannten IP-Adresse erkannt, wird diese automatisch für längere Zeit blockiert.
- Die Möglichkeit, Aufzeichnungs-Appliances als Security Gateway des Videosystems einzusetzen. Dadurch werden Videonetzwerk und Produktionsnetzwerk voneinander getrennt. Dies verhindert unberechtigten Zugriff z.B. über Kameras im Außenbereich und senkt die Netzwerklast.
- Die Entwicklung sämtlicher Hard-, Soft- und Firmware-Lösungen im eigenen Haus und damit keine versteckten Zugangsmöglichkeiten über Backdoors sowie gehärtete Betriebssysteme.
- Failover- und Redundanzmechanismen gegen Datenverlust.
- LGC-Zertifizierung für eine Beweissicherung, die alle Kriterien für eine gerichtliche Verwertbarkeit erfüllt.

Vorsicht bei DSGVO-„konformen" Datenschutzzertifikaten

Grundsätzlich fördert die EU die Einführung von datenschutzspezifischen Zertifizierungen bzw. Datenschutzsiegeln, da diese die Transparenz erhöhen und Unternehmen den Nachweis über die Einhaltung der DSGVO erleichtern sollen. Jedoch gibt es bei dieser Thematik einige wichtige Punkte zu beachten: Einerseits waren trotz der zweijährigen Übergangsfrist keine gültigen Zertifizierungen vor dem 25. Mai 2018 möglich, die eine Konformität mit den Anforderungen der DSGVO offiziell bestätigen. Anderseits sind keine Zertifizierungen für Produkte oder Dienstleistungen selbst möglich, sondern nur für Datenverarbeitungsvorgänge. Dass beispielsweise eine Überwachungskame-

ra „DSGVO-konform“ ist, ist somit nicht möglich. Des Weiteren ist bei Zertifikaten und Datenschutzsiegeln darauf zu achten, dass sowohl die Zertifizierungsstelle selbst als auch das von ihr angebotene Prüfverfahren für einen Datenverarbeitungsvorgang offiziell nach DSGVO akkreditiert sind. Andernfalls haben diese Zertifikate keinerlei rechtliche Wirkung in Bezug auf die DSGVO. Zu erkennen ist ein „echtes“, akkreditiertes Zertifikat etwa am entsprechenden Logo einer offiziellen nationalen Akkreditierungsstelle – in Deutschland die Deutsche Akkreditierungsstelle, kurz DAkks. Akkreditierungsstellen „prüfen“ die Prüfer, also diejenigen Stellen, die eine Zertifizierung oder ein Datenschutzsiegel ausstellen. Unternehmen sollten also möglichst genau auf eine offizielle Akkreditierung der Zertifikate und Datenschutzsiegel nach DSGVO achten und nicht unnötig Geld für „Scheinzertifikate“ ausgeben.

Fazit: Am besten gut vorbereitet sein

Seit dem 25. Mai 2018 existieren zwar „auf dem Papier“ viele Paragraphen und Artikel zum Datenschutzrecht. Deren finale Auslegung im praktischen Vollzug steht aber noch keinesfalls fest und wird auch über das Jahr 2018 hinaus noch von den nationalen und europäischen Datenschutzaufsichtsbehörden kontrovers diskutiert und definiert werden – einschließlich einer abschließenden Beurteilung durch den Europäischen Gerichtshof bei strittigen Punkten.

Daher bleibt der beste Weg für Unternehmen bei der Videosicherheit: Anstatt auf einzelne, möglicherweise „scheinzertifizierte“ Teile einer Videosicherheitslösung zu vertrauen, ist es oft sinnvoller, im gesamten Prozess der Videodatenverarbeitung über die notwendigen datenschutz- und datensicherheitsrelevanten Techniken und Verfahren zu verfügen, um so flexibel wie möglich auf die zu erwartenden Anforderungen reagieren zu können. ■

Kontakt

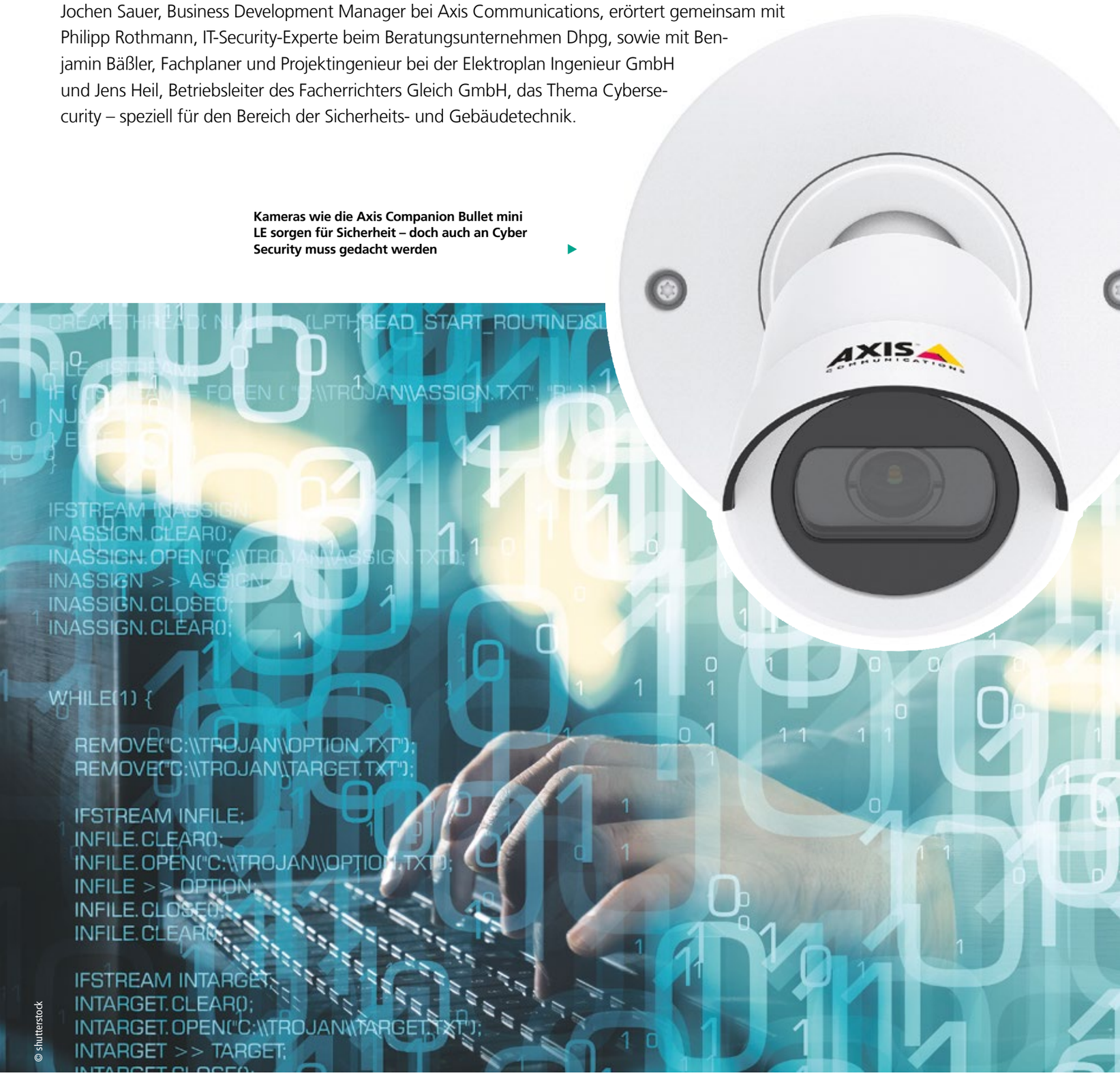
Dallmeier electronic GmbH & Co.KG
Regensburg
Tel.: +49 941 8700 0
info@dallmeier.com
www.dallmeier.com

VIDEOSICHERHEIT – DER AXIS ROUNDTABLE

Fehlerquelle Cybersecurity

Cyberangriffe gegen die Wertschöpfungskette – was tun?

Jochen Sauer, Business Development Manager bei Axis Communications, erörtert gemeinsam mit Philipp Rothmann, IT-Security-Experte beim Beratungsunternehmen Dhpg, sowie mit Benjamin Bäßler, Fachplaner und Projektingenieur bei der Elektroplan Ingenieur GmbH und Jens Heil, Betriebsleiter des Facherrichters Gleich GmbH, das Thema Cybersecurity – speziell für den Bereich der Sicherheits- und Gebäudetechnik.



Kameras wie die Axis Companion Bullet mini LE sorgen für Sicherheit – doch auch an Cyber Security muss gedacht werden ▶

Verfassungsschutz warnt vor Cyberangriffen“ – diese Headline macht Mitte Mai 2018 die Runde in vielen deutschen Medien. Hintergrund: Verfassungsschutzpräsident Hans-Georg Maaßen warnt vor Cyberangriffen auf kritische Infrastrukturen in Deutschland. Der Schutz vor Hackern und ihren Aktivitäten rückt immer mehr in den Fokus einer breiten Öffentlichkeit – und die Frage, wie man sich bestmöglich schützen kann - und wer für den Schutz überhaupt verantwortlich ist.

Ein Bereich, der vielleicht weniger spektakulär als das Wasserwerk oder die Stromversorgung eines Hans-Georg Maaßen anmutet, ist der Hausbau. Egal ob es sich um einen Zweckbau, also Büro, Einkaufszentrum, um ein Krankenhaus oder ein Privatgebäude handelt. Überall wo informationstechnische Systeme zum Einsatz kommen, sollte Cybersicherheit von Anfang an ein essentielles Thema sein. Durch das Internet der Dinge, Industrie 4.0 oder intelligente Geräte im Allgemeinen wächst die potenzielle Gefahr, einem Cyberangriff ausgesetzt zu sein.

Auch Hersteller von Sicherheitssystemen, genauso wie Fachplaner und -errichter sehen sich hier der Herausforderung gegenüber, ihre Kunden kompetent zu beraten. Denn es fehlt an einem allgemeinen Konsens, wie das Thema am besten angepackt werden soll. Wer ist verantwortlich? Bereits der Planer – oder doch der Errichter? Oder obliegt die digitale Sicherheit doch dem Kunden selbst? Im Rahmen eines Roundtables diskutierten die Experten Sauer, Rothmann, Bäßler und Heil speziell diese Fragen.

Kritische Infrastrukur, komplexe Folgen

Cybersecurity, da ist sich die Runde zunächst noch einig, ist ein hochbrisantes Anliegen – das dürfte auch beim letzten IT-Sicherheitsmuffel angekommen sein. Ein bekannter Fall, der Anfang 2016 durch den Blätter- und Pixelwald rauschte, war der Cyberangriff auf das Städtische Krankenhaus Neuss, bei dem sich eine Schadsoftware im Informationssystem der Klinik ausbreitete. Der Computervirus hatte über einen E-Mail-Anhang, den ein Mitarbeiter des Krankenhauses geöffnet hatte, Zugang zum IT-System der Klinik gefunden. Die Schadsoftware hatte die Computersysteme des Krankenhauses für über zehn Tage lahmgelegt, da die Ransomware alle erreichbaren Daten verschlüsselte. Dieser Angriff auf eine kritische Infrastruktur zeigt, wie komplex die Konsequenzen sein können. Und dies werde, so die Roundtable-Experten, keine Ausnahmen bleiben. Weder eine Einrichtung wie ein Krankenhaus als Angriffsziel noch Hackerangriffe auf Netzwerke von Unternehmens seien Einzelfälle.

Die Zahl von Hackerangriffen nimmt zu. Nicht zuletzt durch die steigende Zahl von vernetzten Geräten und IoT-Systemen - die für Hacker über ihre IP-Adressen und Sicherheitslücken attraktive Angriffsziele sind. Prognostizierte der US-Marktforscher Gartner für das Jahr 2017 weltweit noch 8,4 Milliarden vernetzte Geräte, sollen 2020 bereits 20,4 Milliarden Devices über Netzwerke miteinander verbunden sein. Während von der Öffentlichkeit Cyberangriffe und das damit einhergehende Thema Cybersecurity überwiegend in der IT-Branche angesiedelt werde, stelle das Thema die Hersteller, Fachplaner, Facherrichter und Auditoren der Gebäude- und Sicherheitstechnik im Alltag jedoch vor zahlreiche Herausforderungen.

> „Errichtung und Instandhaltung von Sicherheitstechnik gehen Hand in Hand“
>
> **Jens Heil, Betriebsleiter Gleich GmbH, Mitglied der Geschäftsleitung, Errichterbetrieb für Sicherheitstechnik**
>
> **„Als herstellerunabhängiger Facherrichter integrieren wir die Sicherheitskonzepte in die Netzwerke unserer Kunden oder errichten autarke Netzwerke. Wir sind die ersten Ansprechpartner unserer Kunden, wenn beispielsweise eine Netzwerkkamera ein Patch benötigt oder eine Sicherheitslücke entstanden ist. Uns ist es ein großes Anliegen, unsere Kunden in die Lage zu versetzen, eine mündige Entscheidung über ihr Sicherheitssystem treffen zu können. Für unsere Arbeit ist es hilfreich, im Austausch mit Herstellern beispielsweise über die Softwarehärtung informiert zu werden, um dies weiterzugeben bzw. entsprechende Maßnahmen proaktiv zu ergreifen. Unabhängig von der Einrichtung, legen wir unseren Kunden nahe, eine Servicevereinbarung mit deren Errichtern zu schließen, um entstandene Sicherheitslücken frühzeitig zu entdecken und zu eliminieren.“**

Anforderungen an den Fachplaner: Komfort und Sicherheit verknüpfen

„Ein Kunde hat wenig Bewusstsein für Sicherheitslücken, bis er selbst davon betroffen ist“, bringt es Benjamin Bäßler, Projektingenieur Elektroplan Ingenieur GmbH, auf den Punkt. Die Anforderungen des Fachplaners und die Wünsche des Kunden seien nicht immer die gleichen. Denn während der Kunde den Komfort und die Finanzierung im Blick habe, denke der Fachplaner auch an die IT-Sicherheit

> 100-prozentige Sicherheit gibt es nicht“
>
> **Benjamin Bäßler, Projektingenieur bei der Elektroplan Ingenieur GmbH – Fachplanung Elektro mit Schwerpunkt Sicherheitstechnik**
>
> **Ein zunehmender Trend, den wir bei unseren Kunden aus der Industrie und dem gehobenen Privatbau wahrnehmen, bezieht sich auf die geforderten Funktionalitäten in einer Ausschreibung. Kunden und Bauherren fordern immer häufiger einen Endzustand der Anlage, der ihnen eine absolute Sicherheit garantieren soll. Diese Forderung verfehlt die Realität, das Problem tritt insbesondere dann in den Vordergrund, wenn die Ausschreibung auf eine bestehende Anlage aufsetzt, deren technische und konzeptionelle Parameter schon bei der Errichtung nur ungenügend im Sinne der Sicherheit festgelegt wurden.“**

der Systeme sowie ob und wie diese mit anderen Systemen integriert werden sollten. Eine weitere Herausforderung sei hier, auch langfristig zu denken und den End-to-Support des Herstellers im Blick zu haben. Nur weil beispielsweise ein Videoüberwachungssystem bei der Abnahme eines Gebäudes als sicher eingestuft werde, heiße es nicht, dass dieser Status automatisch für die nächsten Jahre gelte. In der Praxis bedeutete dies, dass Gebäudebetreiber und -nutzer die IT-Sicherheit selbst Jahre nach der Inbetriebnahme aufrechterhalten müssten.

Die Angriffspunkte eines Gebäudes reichen beispielsweise von Netzwerk-Druckern bis zu professionellen Zutrittskontrollsystemen. „Die Aufgabe für die gesamte Wertschöpfungskette lautet, die Komplexität beherrschbar zu machen“, erklärt Philipp Rothmann, Senior Manager bei den IT-Beratern und Wirtschafts-

Bitte umblättern ▶

prüfern Dhpg. Eine häufig diskutierte Lösung betreffe die Risiko-Clusterung, wonach Netzwerke für einzelne Zwecke wie beispielsweise die Videoüberwachung, eingerichtet und sogenannte „Insellösungen" geschaffen werden. In einem solchen isolierten System bilden etwa mehrere Computer ein eigenständiges Netzwerk, das nicht direkt mit anderen Netzwerken verbunden und daher schwerer angreifbar sei. Der Nachteil: Diese Systeme können nicht zusammen mit anderen integriert werden.

Doch was bedeutet das für den Fachplaner? Hier sind sich die Roundtable-Teilnehmer einig, dass der Fachplaner langfristig planen und zukünftige Entwicklungen im Blick haben müsse – sowie auch kritisch die Hersteller der einzelnen Komponenten auswählen solle.

Die Einhaltung dieser Punkte sei extrem wichtig – die Praxis jedoch sehe anders aus. Hier sei der Fachplaner oft im Zwiespalt zwischen den Anforderungen an eine Sicherheitsanlage seitens seiner Kunden sowie den Lösungen, die technisch die meisten Vorteile versprechen. Die Herausforderung für den Fachplaner lautete daher, das Bewusstsein beim Endnutzer dafür zu wecken, dass Komfort oftmals zweitrangig sei – dafür aber die Sicherheit eines Systems von hoher Priorität.

IT und Gebäudetechnik nähern sich an: Herausforderung für den Facherrichter

Ebenso wie der Fachplaner müsse auch der Facherrichter für die Sensibilisierung pro Cybersecurity beim Endkunden sorgen. Schließlich sei der Sicherheitsprofi nicht nur für die Errichtung der Anlagen zuständig, sondern eben auch für die Instandhaltung.

Hinzu komme, dass Sicherheit heutzutage umfassender geworden sei: Befand sich beispielsweise früher eine Patentschrift in einem Tresor, der durch einen Bewegungsmelder und Videoanlagen gesichert wurde, liege diese Patentschrift eines Unternehmens heute auf einem Server, der eine andere Angriffsabwehr erfordere. Wobei IT-Sicherheit hier mit physischer Sicherheit verbunden sein müsse. Denn eine unüberwindbare Firewall helfe wenig, wenn das Bürogebäude unverschlossen und ohne eine Zutrittskontrolllösung für Unberechtigte sperrangelweit offenstehe.

Viele Unternehmen besäßen eine IT-Abteilung, die als wichtiger Bestandteil im Unternehmen die Netzwerksysteme für Videosicherheitsanlagen und das produktive Netz sichere. Durch die immer stärker werdende IP-Ausrichtung der Sicherheitstechnik seien Kunden inzwischen stärker involviert als vielleicht noch vor zehn, fünfzehn Jahren. Wenn die Videoüberwachungsanlage eines Kunden beispielsweise mit dem Internet verbunden sei, sichern sich Facherrichter oftmals durch Haftungsausschlüsse ab. Denn durch einen ungesicherten Zugang zum Internet wachse die Gefahr eines Cyberangriffs. Die Konsequenz: Viele Facherrichter verlören lieber einen Auftrag als ihre Reputation, indem sie darauf verzichteten, unsichere Netzwerksysteme zu errichten. Um dieses Dilemma aufzulösen, werde es in der Folge zunehmend wichtiger, dass alle Vertreter der Wertschöpfungskette zusammenarbeiteten.

Axis-Roundtable zum Thema Cyber Security: Jochen Sauer, Philipp Rothmann, Moderatorin Silke Stumvoll, Benjamin Bäßler und Jens Heil

Wer hat Schuld an der Sicherheitslücke?

Auditoren würden meist dann in Unternehmen gerufen, wenn die Vermutung auf eine Sicherheitslücke bestehe - und die Gefahr eines Angriffs drohe. Dabei kämen oftmals Sicherheitslösungen zutage, die zwar für die Mitarbeiter komfortabel seien, aber keine ganzheitliche Sicherheit böten. Beispiel: Ein Unternehmen verknüpfe die Funktion einer Zutrittskarte mit RFID-Chip mit der Abholung von Druckunterlagen. Doch der Mitarbeiter verliert die Zutrittskarte in der Mittagspause und merkt dann im Büro, dass auch bereits gedruckte Unterlagen verschwunden seien. Dies sei, nicht nur in Zeiten der Datenschutz-Grundverordnung, ein schwerwiegendes Problem. In diesem konkreten Fall führte das Unternehmen einen zusätzlichen Pin zur Abholung von Druckaufträgen ein.

Der Endanwender habe das Thema Cybersecurity oftmals nicht im Blick und sei sich der Gefahr oftmals nicht bewusst. Die Roundtable-Experten diskutieren lange, wessen Aufgabe es eigentlich sei, den Kunden ausreichend zu informieren und zu schulen. Fazit: Es könne nur ein gemeinsames Unterfangen sein, egal ob Fachplaner oder -errichter. Zudem seien auch die Hersteller in der Pflicht, um beispielsweise langfristig Updates oder etwa einen Long-Term Support (LTS) für Produkte zur Verfügung zu stellen.

Zertifikate als Sicherheit für den Endnutzer

Als Endanwender, also Inhaber eines Gebäudes, sei man gut beraten, schon bei der Auswahl eines Fachplaners und -errichters auch den Aspekt Cybersecurity zu beachten. Denn werde hier eine kompetente Kraft ausgewählt, sei der erste wichtige Schritt bereits getan: Sensibilisierung für das Thema Cybersicherheit. Hilfreich seien hier Schulungszertifikate sowie Sicherheitsstandards, nach denen sich der Nutzer richten kann. Doch während im Bereich Brandmeldetechnik eine sehr gute und auch transparente Normierung bestehe, fehle dem Verbraucher im Bereich Cyber-Sicherheitstechnik verbindliche Zertifikate. Hier gebe es definitiv Handlungsbedarf.

„Seitens der Wertschöpfungskette fällt es aufgrund der sich schnell ändernden Erkenntnisse über Sicherheitslücken schwer, entsprechende Zertifikate zu generieren" sagt Fachplaner Benjamin Bäßler, Projektingenieur der Elektroplan Ingenieur GmbH. Hersteller hätten etwa die Möglichkeit, sich ihr Information Security Management System durch eine unabhängige Prüfung ISO 27001 zertifizieren zu lassen. Diese Zertifizierung sei unter anderem Bestandteil des IT-Sicherheitsgesetzes, welches für die Betreiber von kritischen Infrastrukturen („Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen") verpflichtend sei.

Wissen teilen – Sicherheit schaffen

Zertifikate, die als Orientierung für den Endanwender bei der Suche nach dem passenden Fachplaner und –errichter dienten, sind das eine. Doch auch Planer und Errichter benötigten kompetente Partner an ihrer Seite, die ebenso langfristig denken. So sei es essentiell, dass die Hersteller der einzelnen Komponenten, egal ob dies eine Sicherheitskamera, eine Türsprechanlage oder eine Schranke sei, ebenfalls bewusst ausgewählt werden. Auch hier gebe es unterschiedliche Hilfestellungen wie Normen oder Standards.

In der Diskussionsrunde wies Jochen Sauer von Axis Communications auf die Verantwortung der Hersteller selbst hin. Denn Cybersecurity fange beim Produkt selbst an. „In unserem Hardening Guide zeigen wir Möglichkeiten, wie unsere Produkte gehärtet werden können – also gegen Hackerangriffe gesichert werden. Zudem bieten wir Webinare und informieren über Sicherheitspatches", so der Experte für Sicherheitsanlagen.

Herausforderungen für die Wertschöpfungskette

Die Diskussion zeigte, dass die Anfänge einer übergreifenden Zusammenarbeit vorhanden und sich Fachplaner sowie Facherrichter einig sind, dass Cybersecurity nur gemeinsam und in Zusammenarbeit mit den Herstellern erreicht werden könne. Doch dürfen auch die Herausforderungen für die einzelnen Parteien nicht ignoriert werden: Der Fachkräftemangel sowie eine abweichende Gewichtung auf Seiten des Endkunden.

Der Fachkräftemangel betreffe nicht nur das Handwerk in Deutschland, sondern auch die Gebäudetechnik: So hätten auch Facherrichter echte Schwierigkeiten, passendes

Transparenz schafft Sicherheit“

Jochen Sauer, Business Development Manager A&E bei Axis Communications

„Als Hersteller von IP-basierten Netzwerk-Kameras ist Sicherheit unser Kerngeschäft. Bei der Entwicklung von Hard- und Software achten wir bereits von Anfang an darauf, dass die Systeme so frei von Schwachstellen wie möglich und so unempfindlich gegen Angriffe wie möglich konzipiert werden und verfolgen durch lückenlose Tests die Qualität unserer Produkte. Darüber hinaus setzten wir als Unternehmen auf ein transparentes Informationsmanagement, wodurch bekanntgewordene Schwachstellen offen kommuniziert werden. Nur regelmäßige Sicherheitsupdates und eine offene Kommunikation aller Beteiligten über den kompletten Lebenszyklus erschaffen erst ein sicheres System.

Cyberangriffe werden durch das Internet der Dinge zunehmen“

Philipp Rothmann, Senior Manager beim IT-Berater und Auditor Dhpg

„Als IT-Beratungsgesellschaft treten unsere Kunden meistens erst mit uns in Kontakt, wenn es bereits eine Sicherheitslücke in ihrem Netzwerk gab oder der entsprechende Verdacht besteht. Die anschließend aufgedeckten Schwachstellen beruhen größtenteils auf fehlerhafter Planung und dem Vorzug von Komfort bei der Handhabung gegenüber Sicherheit. Abhilfe schaffen würden verpflichtende Penetrationstests nach der finalen Einrichtung eines Sicherheitssystems, das dem Betreiber Auskunft über mögliche Schwachstellen liefert, Risiken aufzeigt und somit bei einem möglichen Angriff, eine schnelle Reaktion durch alle Beteiligten ermöglicht.“

Personal zu finden. Hinzu komme, dass die Fachplanung komplexer geworden sei: statt eines singulären Systems seien mehrere Sicherheitssysteme parallel im Einsatz. Hier ändern sich die technischen Anforderungen in kurzen Abständen. Ideal wäre die Schaffung einer neuen Expertenposition, beispielsweise die eines speziellen Systemintegrators. Dieser prüfe das System auf seine Vernetzung mit den verschiedenen Gewerken und ihre Kompatibilität – und habe auch die Cybersicherheit im Blick.

Ein weiterer Punkt sei der Wunsch von Endnutzern nach absoluter Sicherheit. Da Nutzer interagieren wollen und sich nicht alle Systeme voneinander trennen ließen, wäre eine Lösung auf eine „offene Kommunikation“ der einzelnen Geräte zu setzen: Das hieße, transparent nachzuverfolgen wie die verschiedenen vernetzten Geräte, ohne proprietäre Protokolle, miteinander arbeiten. Außerdem solle gezielt festgelegt werden, was die Devices austauschen dürfen. Für diese Aufgabe seien entsprechendes Wissen sowie Integratoren notwendig, die zusätzlich zu ihrem Fachwissen zur Standardisierung der Einrichtung auch Experten im Bereich Cybersecurity seien.

Security by Design: Sichere Passwörter

Am Beispiel des Neusser Krankenhauses zeigt sich, dass Mitarbeiter beim Thema Sicherheit ein elementarer Bestandteil des Sicherheitskonzepts seien und entsprechend geschult werden müssen. So verfügte das Krankenhaus zum Zeitpunkt des Cyberangriffs beispielsweise nur über ein Single-Sign-On, über das ein Mitarbeiter durch eine einmalige Authentifizierung am Arbeitsplatz auf alle Dienste zugreifen konnte.

„Dieses Beispiel zeigt, dass sichere Passwörter und die Passwortverwaltung, im Hinblick auf das Thema Security by Design, unerlässlich sind“ so Jochen Sauer von Axis Communications. Dabei gelte es zu beachten, dass Passwörter schwer zu erraten sein müssen. Die Empfehlung, besonders komplexe Passwörter zu verwenden, die häufig gewechselt werden, ist allerdings nur schwer praktikabel. Auch Philipp Rothmann von der Dhpg prognostiziert, dass Passwörter auch in der unmittelbaren Zukunft wichtig bleiben würden, aber es einen zusätzlichen Faktor geben muss.

„Risiko erkannt, Risiko gebannt“

Ein intelligenter Ansatz zur Risikominimierung sei der sogenannte Penetrationstest. Also das aktive Testen der Anlagen in Hinblick auf Sicherheitslücken. Dabei werde zwischen zeitpunktbezogenen oder zeitraumbezogenen Zertifizierungen unterschieden. So kann beispielsweise eine Wirtschaftsprüfungsgesellschaft eine Zeitpunktbetrachtung des Sicherheitszustandes erstellen. Damit werde das Risiko eines Angriffs eingeschätzt und Risikolücken aufgezeigt.

Arbeiteten alle beteiligten Parteien zusammen und seien sie offen für eine konstruktive Fehlerkultur, könnten Risiken frühzeitig erkannt und auf Gefahren reagiert werden, bevor sie zu Bedrohungen würden. Werde ein obligatorischer Penetrationstest als Bestandteil der Ausschreibung aufgenommen, böte dies für Fachplaner und Facherrichter die Möglichkeit, per Vertrag aus der Haftung genommen zu werden.

Wartung als Maßnahme zur Sicherheitsvorsorge

Habe der Hersteller seine Systeme bestmöglich gehärtet, der Fachplaner alle möglichen Sicherheitsrisiken bedacht, sei das Sicherheitssystem optimal konstruiert – und habe der Facherrichter das Sicherheitssystem aufgesetzt, getestet und fehlerfrei abgenommen, bedeute eine sichere Lösung jedoch nicht selbstverständlich, dass sie dies auch am folgenden Tag noch sei.

Während regelmäßige Wartungen in der Brandmeldetechnik verpflichtend seien, so seien Wartungsverträge und instandhaltungsorientiertes Betreibungsmanagement in der Videotechnik bisher selten. „Ursächlich für das Verhalten ist das Fehlen einer rechtlichen Vorschrift oder eine negative Erfahrung wie die eines Cyberangriffs, die Notwendigkeit etwas zu verändern und Gelder bereitzustellen“, berichtet Jens Heil vom Facherrichter Gleich GmbH.

Zugleich gebe es Unterschiede zwischen industriellen und privaten Nutzern von intelligenten Gebäuden. Während Unternehmen häufiger bereit seien, einen Wartungsvertrag mit Facherrichtern abzuschließen, treffe dies auf Privatnutzer nur bedingt zu. Zugleich sähen sich letztere häufig nicht in der Lage, ihre Sicherheitssysteme selbständig zu prüfen.

Fazit: Wertschöpfungskette stolpert über sich selbst

Die zunehmende Komplexität in der Sicherheits- und Gebäudetechnik erfordere die Zusammenarbeit aller Beteiligten der Wertschöpfungskette. Auch wenn Vertreter der verschiedenen Gewerke die Vorteile der Zusammenarbeit klar definierten, finde der Austausch noch nicht flächendeckend statt. Durch fehlende Transparenz der Arbeitsprozesse, der Wertschöpfungskette, Zeit- und Kostendruck, sowie die Tendenz der Nutzer, komfortable Lösungen den sicheren vorzuziehen, seien Sicherheitslücken die Realität. Darüber hinaus fehle in der breiten Öffentlichkeit das Bewusstsein für die Komplexität von Cybersecurity. So werde etwa Gebäudesicherheit als Thema wahrgenommen, es fehle jedoch das Verständnis der Verknüpfung einzelner Komponenten miteinander. So schließe beispielsweise so mancher Mitarbeiter sein Smartphone zum Laden an den Computer an – und böte bereits damit potenziellen Angreifern einen Eintrittspunkt für das unternehmensweite Netzwerk.

Hersteller trügen unter anderem durch eine intelligente Gerätehärtung zu einer besseren Sicherheitsleistung bei. „Wenn diese durch Fachplaner, Facherrichter und Auditoren aufrechterhalten wird“, sagt Jochen Sauer, „können wir die Tore gegen Cyberangriffe optimal verteidigen“.

Aber: Es liegt auch mit an der Öffentlichkeit, die Problematik ernst zu nehmen – eine Lösung ist nur gemeinsam möglich. ■

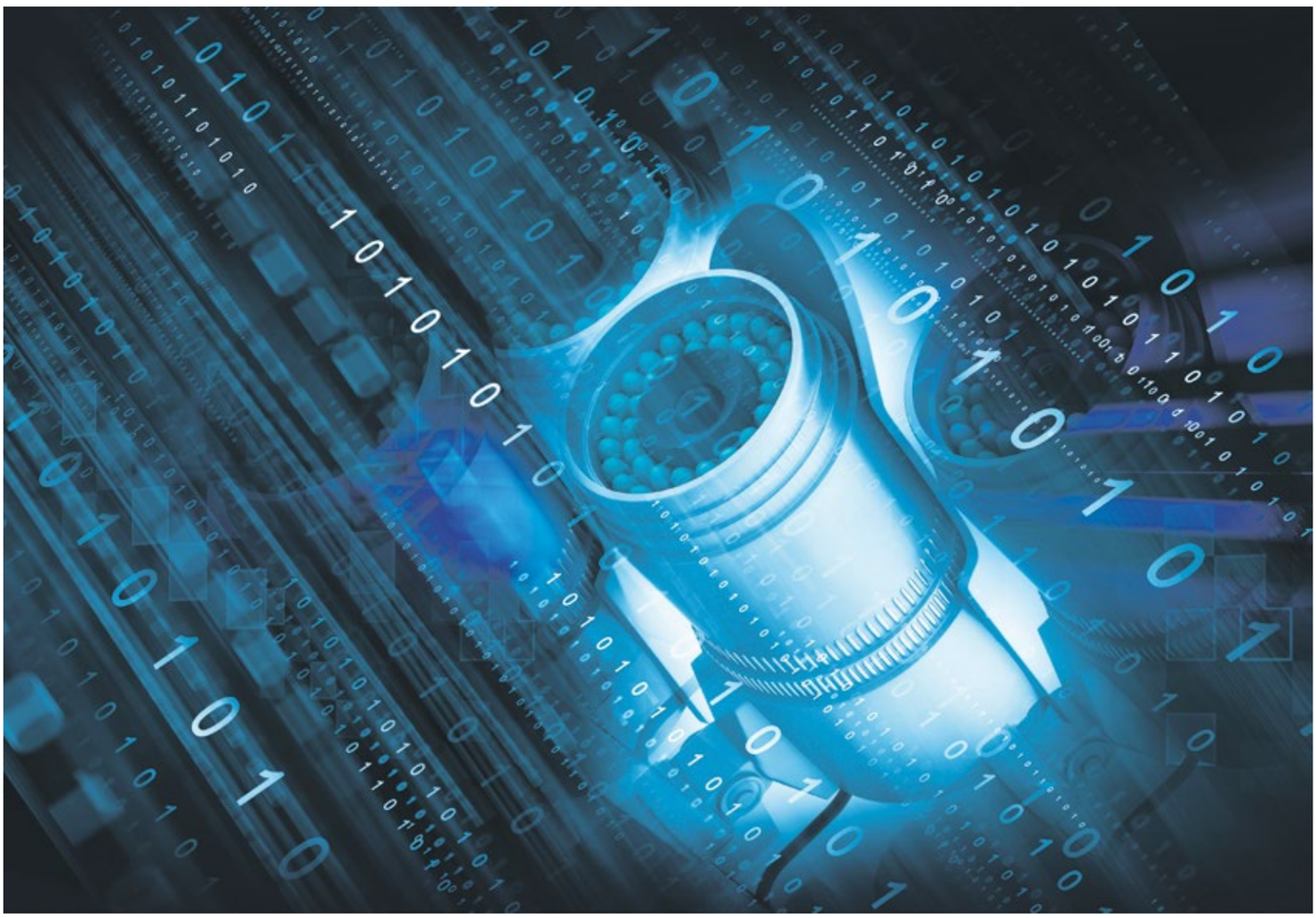
Kontakt

Axis Communications GmbH
Ismaning
Tel.: +49 89 358817 0
info-de@axis.com
www.axis.com

SICHERHEIT FÜR SICHERHEITSSYSTEME

Wie sicher ist Sicherheit?

Überwachungssysteme können zum Einfallstor werden – Risiken und Handlungsempfehlungen



©bluebay2014 - stock.adobe.com

„Uns kann nichts passieren – wir haben doch ein Sicherheitssystem!“ Ein solcher Gedanke ist trügerisch. Denn wer garantiert, dass bei IP-Kameras, Kommunikations- oder Zutrittskontrollsystemen die Sicherheit nicht gänzlich auf der Strecke bleibt? Woran Unternehmer jetzt denken müssen. Ein Beitrag von Bodo Meseke, Leiter der Forensic Technologies bei EY.

Wer ein Auto kauft, achtet vor allem auf das Preis-Leistungs-Verhältnis und Features wie Sitzheizung, Spurassistent oder Navigationssystem. Doch was ist mit Sicherheitsgurten, Bremsen oder Airbags? Diese hat ausnahmslos jeder Neuwagen – ob er nun 10.000 oder 100.000 Euro kostet. Die grundlegende Sicherheit ist also gewährleistet. Wieso ist das nur bei Autos so? Warum wird bei physischen Systemen zur Unterstützung der Sicherheit oft genau an deren eigener (Cyber-)Sicherheit gespart?

Viele Unternehmen arbeiten heutzutage mit Videoüberwachungssystemen (VSS, früher CCTV), Kommunikationssystemen oder Zugangskontrollen. Sie sollen vor Schäden schützen und Eindringlinge fernhalten. Was nicht alle bedenken: Mitunter werden sensible Daten wie Videodateien innerhalb des Systems unverschlüsselt ausgetauscht – und die Geräte sind vergleichsweise leicht zu hacken.

IP-Kameras im Consumer-Bereich kosten heute weniger als dreißig Euro – und auch im Business-Umfeld gibt es Spreu und Weizen. Oft gilt leider: Hauptsache, die zentrale Funktion des Geräts arbeitet ausreichend gut, das Drumherum ist nicht selten „zusätzlicher Aufwand und drückt die Marge“. Da die Geräte zumeist aber Teil des IoT sind, kann sich ein Vernachlässigen der Cyber-Sicherheit der Produkte jedoch fatal auswirken – schafft

Security Systems

Security Systems enthalten meist sensitive Daten und werden durch das Internet der Dinge (IoT) angreifbarer. Sie sollen vor Schaden schützen – und nicht selbst zum Einfallstor werden. Cyber Security ist daher unverzichtbar. Dieser Beitrag informiert über Risiken und gibt Handlungsempfehlungen

Der Cyber-Check

- Fangen Sie an, IT-Sicherheit umzusetzen – noch heute und im ganzen Unternehmen. Jeder Mitarbeiter muss wissen, was im Ernstfall zu tun ist.
- Legen Sie deshalb eine Checkliste mit ersten Handlungstipps und den wichtigsten Telefonnummern an – digital und analog, denn wenn Ihre IT angegriffen wird, ist eine Papierversion vielleicht äußerst hilfreich.
- Machen Sie sich bewusst, wo in Ihrem Unternehmen welche Daten gespeichert werden, wie wichtig diese für Ihr Unternehmen sind und wie Sie sie optimal schützen/sichern.
- Beseitigen Sie Schwachstellen mit Unterstützung von Fachleuten.
- Und: Überprüfen Sie auch die Sicherheitsstandards Ihrer Geschäftspartner – vom Softwareanbieter bis zum Lieferanten.

man so doch unter Umständen ein Einfallstor für genau die Personen, vor denen ein Sicherheitssystem eigentlich schützen sollte.

Das IoT als Türöffner: Kriminelle können etwa die Videoüberwachungsanlage oder Wartungszugänge für Klimageräte hacken, bei vertraulichen Meetings zuhören, Zugriffscodes von Türen ändern, um unbemerkt ins Firmengelände einzudringen – oder auch einfach über diese Einfallstore weiter in das Unternehmensnetzwerk vordringen, bis sie sich Zugang zu wirklich wertvollen Daten verschafft haben. Sind sie einmal im System, ist es schwer, sie aufzuhalten.

Fragen, bevor es zu spät ist

Im Internet der Dinge wird immer mehr miteinander vernetzt: Bis 2020 sollen es 200 Milliarden Geräte sein. Einerseits ist dies verlockend unkompliziert, andererseits gefährlich ungeschützt. Angesichts dessen ist Cyber-Sicherheit eines der wichtigsten Themen, auch für Entwickler neuer IoT-Geräte.

Um das jeweilige Risiko einzuschätzen, sollte jedes Unternehmen hinterfragen, mit welchen kritischen Daten seine Sicherheitssysteme arbeiten und welche Schwachstellen es Hackern ermöglichen, Vorgänge zu manipulieren.

IT-Sicherheit ist kein „Nice-to-have" und längst kein reines Online-Thema mehr. Cyber-Security und physische Sicherheit müssen systematisch verknüpft und die eigenen Sicherheitssysteme sollten gründlich überprüft werden:

- Wie sehr achtet der Hersteller generell auf die Sicherheit seiner Produkte?
- Gibt es regelmäßige Software-Updates?
- Was geht wirklich in unseren Netzwerken vor sich?
- Wie organisieren wir Cybersicherheit effektiv in allen Bereichen?
- Was muss wirklich zwingend miteinander vernetzt sein?

Unser Autor Bodo Meseke ist Partner in der Abteilung Forensic & Integrity Services bei EY. Er ist Experte für Digital Forensics & Incident Response und verantwortlich für die Forensic Technology & Discovery Services, EMEIA Central Zone. Er betreut Kunden aus verschiedenen Industriesegmenten und führt Ermittlungsteams, die fortgeschrittene Angriffe auf IT-Systeme erkennen und aufklären. Bodo Meseke war zuvor u. a. Kriminalbeamter im Bereich Cyber Crime beim Bundeskriminalamt.

Abschließen niemals vergessen

Ein gutes Cybersicherheitssystem zu haben, ist nur die halbe Miete. Denn selbst das beste System bringt nichts, wenn die handelnden Personen nicht wissen, wie es richtig zu nutzen ist. Wir Menschen als „Schwachstelle": Die meisten Fehler gründen leider, zahlreichen Analysen zufolge, noch immer bei Mitarbeitern. Das ist in etwa so, als würde man als Supermarktbetreiber seine Filiale abends nicht abschließen.

Auch darf die Verantwortung für Cybersicherheit nicht bei wenigen IT-Experten in der Firma liegen, sondern bei jedem Mitarbeiter – ausnahmslos. Die Checkliste lässt sich demnach um zwei Fragen erweitern:

- Finden Schulungen zum Umgang mit den Sicherheitssystemen statt?
- Gibt es klare Regeln und Sicherheitsstandards – und werden diese eingehalten?

Gerade vor dem Hintergrund, dass die Frage nicht mehr lautet, ob ein Unternehmen angegriffen wird, sondern nur noch, wann dies der Fall sein wird, wandeln sich die Anforderungen fundamental. Kaum ein Unternehmen kann heute ohne digitale Technologien arbeiten; gerade für eine Wissensnation sind sie wesentlich, doch machen sie zugleich verwundbar. Ein Blick auf die Nachrichten beweist, dass wir nicht über ein fernes Zukunftsszenario diskutieren. Niemals war die Gefährdung durch Cyberkriminalität größer als heute. Trotzdem gehen viele noch zu sorglos mit dem Thema um. Das muss sich schleunigst ändern, damit Sicherheitssysteme Unternehmen auch wirklich schützen. ■

Kontakt

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Eschborn
Bodo Meseke
Tel.: +49 6196 996 22174
bodo.meseke@de.ey.com
www.de.ey.com

UL: Cybersecurity-Forum und -Labor

Die Herausforderungen im Bereich Cybersecurity nehmen auch in Europa branchenübergreifend zu – regionale Lösungen sind notwendig. Um diesem Bedarf gerecht zu werden und die europäische Industrie zu unterstützen, plant UL, ein führendes, unabhängiges und weltweit tätiges Unternehmen für Produktsicherheit und Zertifizierung, zur Eröffnung seines neuen Cybersecurity-Labors in Frankfurt ein Cybersecurity-Forum. Die Tagung bringt eine Reihe von Akteuren der Branche zusammen, darunter Hersteller, Experten aus der Forschung und Gäste aus der Politik. Im Mittelpunkt der Tagesordnung stehen neue Bedrohungen der Cybersicherheit, etwa Side-Channel-Angriffe, bekannt durch die Schwachstellen „Meltdown" und „Spectre". „Es ist absolut notwendig, dass wir uns als globale Organisation für Sicherheitsforschung mit dem Thema Cybersecurity in der vernetzten Welt befassen", sagte Ingo M. Rübenach, Vice President Central, East and South Europe Region. Die IECEE-Organisation (IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components) hat UL offiziell als Zertifizierungsstelle mit eigenen Prüflabors für Industrie-4.0-Standards der IEC 62443 Familie anerkannt. Das Frankfurter Cybersecurity-Prüflabor von UL erbringt in diesem Rahmen Cybersecurity-Services für Europa. ■

Zertifizierung für Industrial Security

TÜV Nord prüft und zertifiziert seit diesem Jahr nach IEC 62443-2-4. Die Norm IEC 62443 (Industrial Communication Networks – Networks and System Security) hat sich als international anerkannter Standard zum Konformitätsnachweis im Umfeld von Industrial Security der Prozess- und Automatisierungsindustrie etabliert. Die voranschreitende Digitalisierung und die Interaktion von Produkten und Systemen führen aber auch hier dazu, dass neben klassischen Konformitätsbewertungen in Safety, Performance und Energieeffizienz das Thema Cyber Security in den Vordergrund rückt. Mit Hilfe der Normenreihe IEC 62443 lässt sich nachweisen, dass Betreiber, Integratoren und Hersteller zeitgemäße Cyber-Security-Standards für industrielle Automatisierungssysteme nutzen. „TÜV Nord hat die Erarbeitung und Umsetzung des IEC-Regelwerks von Beginn an mit vorangetrieben. Umso mehr freuen wir uns, dass wir weltweit unter den ersten drei Prüforganisationen sind, die diese Zertifizierung im IECEE Schema anbieten dürfen", sagt Sandra Gerhartz, Geschäftsführerin TÜV Nord Cert. Die Anerkennung ist nur für IECEE-akzeptierte Prüforganisationen möglich. Mit der IEC 62443-2-4 erweitert das Unternehmen seinen IECEE-Scope. ■

EVENT

Oktoberfest der IT-Profis

Treffpunkt der IT-Security-Professionals: Nürnberg Messe lädt zur it-sa

© Foto: Nürnberg Messe

Zur zehnten Ausgabe der Fachmesse it-sa mit begleitendem Kongress am 9. bis 10. Oktober 2018 werden rund 700 Aussteller im Messezentrum Nürnberg erwartet. Fünf offene Foren und rund 350 Beiträge bieten im „Home of IT-Security" reichlich Informationen und Austauschmöglichkeiten. Das Rahmenprogramm vereint neue Formate wie das „Cyber Economy Match-up" und den gleichnamigen -Award UP 18@it-sa für junge Unternehmen. Das Kongressprogramm mit internationaler Beteiligung ist dieses Jahr unter anderem Veranstaltungsplatz für das internationale Symposium Visit und Bühne für die Verleihung des 7. Deutschen IT-Sicherheitspreises der Horst-Görtz-Stiftung.

Start-up-Award

18 von einer Fachjury ausgewählte junge Unternehmen treten am 8. Oktober 2018 bei UP18@it-sa an, um das Publikum mit ihren Innovationen im Bereich IT-Sicherheit zu überzeugen. Die ausgewählten Start-ups präsentieren neue Produkte und frische Geschäftsideen, mit denen sie Branchenvertreter und potenzielle Geldgeber überzeugen wollen. Dem Sieger winkt neben dem UP18@it-sa-Award ein Coaching der Initiatoren Digital Hub Cybersecurity und Bayerisches IT-Sicherheitscluster. Folgende Start-ups wurden nominiert: Alpha Strike Labs, Authada, Code Intelligence, Crashtest Security, eBlocker, Enginsight, IT-Seal, ITs Scanley, Jolocom, Lucy Security, Meshcloud, Nect, Oculid, Quanticor, Quoscient, Skymatic, Sosafe, Xign Sys. Am Vortag der it-sa findet der Pitch und die Prämierung des Siegers statt: Montag, 8. Oktober 2018, Saal Paris, NCC West. ■

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

Rund 700 Aussteller aus dem In- und Ausland werden dieses Jahr erwartet – „das macht das Messezentrum zum Home of IT-Security“, so Frank Venjakob, Executive Director it-sa beim Veranstalter NürnbergMesse. Die „Cyber-Nation“ Israel beteiligt sich zum dritten Mal mit einem offiziellen Länderpavillon an der it-sa. Neu ist der Gemeinschaftsstand aus den Niederlanden. Fachbesucher finden hier unter anderen Lösungen aus dem Bereich Abhörschutz, Security Awareness, Schutz vor Advanced Persistent Threats und Netzwerksicherheit.

Fünf offene Foren

Das Forenprogramm mit rund 350 Fachbeiträgen in den offenen Foren spricht Entscheider und Experten gleichermaßen an. In den Foren M9 und M10 stehen strategische Weichenstellungen für eine Erhöhung des IT-Security-Level im Mittelpunkt, die Foren T9 und T10 richten sich an technisch orientierte Anwender. Als fünfte Vortragsbühne erweitert das international ausgerichtete Forum I10 mit englischsprachigen Vorträgen in Halle 10.1 das Programm.

Produktneutrale Diskussionen und Beiträge zu übergeordneten Themen werden als „it-sa insights“ gesondert ausgewiesen. Mit der Europäischen Agentur für Netz- und Informationssicherheit ENISA, dem Digitalverband Bitkom, dem Bundesverband IT-Sicherheit Teletrust oder dem Zentralverband Elektrotechnik- und Elektronikindustrie ZVEI beteiligen sich führende internationale und nationale Vereinigungen bei it-sa insights. Alle Forenvorträge sind für Messebesucher und Aussteller frei zugänglich.

Messebegleitender Kongress

Der begleitende Kongress vereint das Informationsangebot renommierter Institutionen und namhafter Unternehmen aus dem In- und Ausland unter einem Dach. Das umfangreiche Programm von „Congress@it-sa“ startet bereits am Montag, den 8. Oktober, also einen Tag vor Eröffnung der Fachmesse. Neu ist das Symposium Visit („Verwaltung integriert sichere Informationstechnologie“). Es findet alle zwei Jahre an wechselnden Standorten statt und bietet IT-Sicherheitsexperten aus der Verwaltung in Deutschland, Österreich, der Schweiz und Luxemburg eine eigene Dialogplattform zum länderübergreifenden Erfahrungsaustausch. Die Jahrestagung der IT-Sicherheitsbeauftragten in Ländern und Kommunen und der IT-Grundschutz-Tag des Bundesamtes für Sicherheit in der Informationstechnik versammeln auch dieses Jahr Experten aus der Verwaltung zur it-sa in Nürnberg.

Es gibt zahlreiches Fachwissen zu Trends und Lösungen im Bereich IT-Sicherheit. Beispielsweise informiert die KPMG über zukünftige Anforderungen an den CISO, ESET klärt über Gefahren aus dem Dark-Web auf. Die Schweizer Ergon Informatik zeigt, worauf es bei der Umsetzung von IAM-Projekten ankommt.

Start-ups im Fokus

Neue Veranstaltungen im Rahmenprogramm unterstreichen die Relevanz der it-sa als Plattform für den intensiven Austausch zum Thema Cybersicherheit: UP18@it-sa bietet Start-ups aus Deutschland, Österreich und der Schweiz eine Bühne, auf der sie Entscheider aus der Branche und potenzielle Finanziers überzeugen. Aussichtsreiche Geschäftsideen und innovative Security-Produkte, die vorab von einer Jury ausgewählt werden, stehen dabei am Montag, den 8. Oktober, im Mittelpunkt. Dem Gewinner winkt ein Coaching des Digital Hubs Cybersecurity und des Bayerischen IT-Sicherheitsclusters. Auf der Sonderfläche Startups@it-sa in Halle 10.1 und in den gleichnamigen Vortragsblöcken in den offenen Foren stehen ebenfalls junge innovative Unternehmen im Fokus.

IT-Sicherheitspreis

Erstmals wird der Deutsche IT-Sicherheitspreis der Horst-Görtz-Stiftung auf der it-sa verliehen. Die zehn Finalisten präsentieren ihre Innovationen am Dienstag, den 9. Oktober, zunächst im Forenprogramm, bevor die drei Sieger in einer feierlichen Preisverleihung gekürt werden. Der Deutsche IT-Sicherheitspreis wird bereits zum siebten Mal verliehen und ist mit insgesamt 200.000 Euro dotiert.

Öffnungszeiten
9.-11. Oktober 2018

- 9:00 bis 18:00 Uhr (Dienstag und Mittwoch)
- 9:00 bis 17:00 Uhr (Donnerstag)

Kontakt

it-sa – Die IT-Security Messe und Kongress
Messezentrum Nürnberg
www.it-sa.de/programm

Special Keynote von Paula Januszkiewicz

Am dritten Messetag, Donnerstag, den 11. Oktober, spricht die polnische IT-Sicherheitsexpertin im neuen internationalen Forum 10. Das Thema ihres Vortrags lautet „Attacks of the Industry: A View into the Future of Cybersecurity“. Paula Januszkiewicz zählt zu den profiliertesten internationalen IT-Sicherheitsexperten. Als Gründerin und Geschäftsführerin von Cqure teilt sie ihr Know-how mit der IT-Sicherheits-Community und berät Kunden in der ganzen Welt. Januszkiewicz wurde als Enterprise Security MVP (Microsoft Most Valuable Professional) ausgezeichnet und zählt zu den wenigen Personen weltweit, die Zugang zu einem Quellcode von Windows haben. Sie war Spitzenrednerin auf bekannten Fach- und Entwicklerkonferenzen, unter anderem in den USA, in Asien und im Nahen Osten.

Paula Januszkiewicz zeigt in ihrer Keynot-Speach auf, wie sich Unternehmen und Organisationen vor häufigen Angriffsformen von Hackern und Cyberkriminellen schützen können

In ihrer Special Keynote geht Paula Januszkiewicz der Frage nach, welche Schwachstellen und häufigen Fehlkonfigurationen in komplexen IT-Infrastrukturen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bedrohen. Sie zeigt mögliche Einfallstore für Spionage oder Sabotage auf und gibt Tipps für eine effektive Verbesserung der IT-Sicherheit in Unternehmen und Organisationen. Dabei erläutert sie unter anderem, wie Cloud-Angebote, zum Beispiel Office 365, Azure oder Amazon Web Services hinsichtlich der Sicherheit einzuordnen sind und beantwortet die Frage: Wann lohnt sich die Migration von Diensten in die Cloud unter Sicherheitsaspekten?

Hacker setzen stärker auf unauffällige Angriffsmethoden

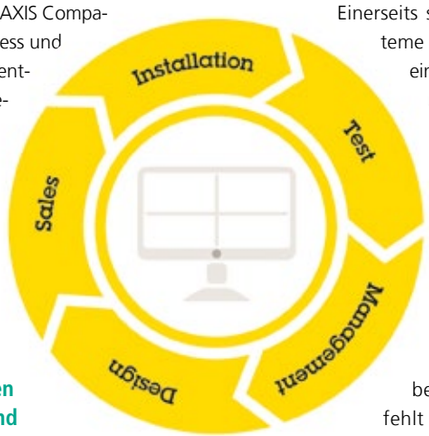
Trend Micro veröffentlichte kürzlich seinen Midyear Security Roundup Report 2018 mit dem Titel „Unseen Threats, Imminent Losses“. Der Bericht des japanischen IT-Sicherheitsanbieters zeigt, dass sich Cyberkriminelle zunehmend von auffälligen Ransomware-Angriffen verabschieden und stattdessen eher unauffällige Angriffsmethoden wählen, um Geld oder Rechenleistung zu stehlen. Die größten Veränderungen in diesem Jahr zeigen sich bisher bei Kryptowährungs-Mining-Malware. Trend Micro verzeichnet im ersten Halbjahr 2018 einen 96-prozentigen Anstieg bei der Erkennung von bösartigen Crypto-Mining-Versuchen im Vergleich zum Jahr 2017. Im Vergleich zum ersten Halbjahr 2017 wird sogar eine Zunahme um 956 Prozent verbucht. Dies deutet darauf hin, dass Cyberkriminelle statt der schnellen Lösegeldauszahlung bei Ransomware immer stärker auf den langsameren, im Hintergrund stattfindenden Diebstahl von Rechenleistung für das Mining von digitalen Währungen setzen. „Cyberkriminelle ändern ihre Tools, Taktiken und Verfahren

(TTPs) ständig, um ihre Erfolgsquoten zu erhöhen“, sagt Udo Schneider, Security Evangelist bei Trend Micro. „Großangelegte Spray-and-Pray-Ransomware-Angriffe und Datenschutzverletzungen sind inzwischen zur Norm geworden. Angreifer ändern deshalb ihre Taktik und versuchen jetzt, unauffälliger zu agieren, indem sie auf bisher unbekannte oder wenig genutzte Angriffsvektoren setzen.“ ■

it-sa, Halle 9, Stand 434

Axis Communications auf der it-sa 2018

Vom 9.-11. Oktober können sich Fachbesucher in Nürnberg über Lösungen zu Cloud, Mobile & Cybersecurity und Daten- & Netzwerksicherheit informieren. Am Stand von Axis Communications (Halle 10.0 / Stand 518) dreht sich alles um IP-basierte Lösungen speziell für kleine und mittelständische Unternehmen. Ob zur Verhinderung eines Diebstahls, zur Lösung eines Vorfalls oder dem effizienten Schutz eines Areals – viele Unternehmen scheuen den Einsatz eines professionellen Sicherheitssystems. „Zu teuer, zu komplex", lauten wiederholt die Vorurteile. Doch mit der Komplettlösung AXIS Companion für Small Business und der Videomanagement-Software Axis Camera Station für Medium Business gibt es spezielle Angebote, die auf die Bedürfnisse dieser Zielgruppen abgestimmt sind.



Spezielle Lösungen für den Mittelstand

Die Verwaltungssoftware Axis Camera Station ist ideal für Produktionsbetriebe, Behörden und Bildungseinrichtung sowie andere Unternehmen, die ein intuitives und anwenderfreundliches Videoverwaltungssystem suchen. Außerdem zu sehen ist die Axis Camera Station Integrator Suite. Dieses Tool-Kit stellt eine perfekt angepasste Plattform für Integratoren und Installer dar, die die Projektierung, Installation und das Management eines Sicherheitssystems erleichtert. Es beinhaltet unter anderem den Site Designer, wodurch eine Projektierung mit wenigen Klicks am Laptop oder Tablet durchgeführt werden kann. Oder das Camera Station System Health Monitoring, womit alle Installationen der Endkunden kontrolliert werden können. So ist beispielsweise schnell ersichtlich, welche Kamera ein Software-Update oder eine Optimierung der Ausrichtung benötigt.

Experten-Gespräch: Sicherheitslösungen für den Mittelstand im Fokus

Der Mittelstand hat spezifische Bedürfnisse im Bereich Sicherheitslösungen. Einerseits sollen die Systeme skalierbar und einfach zu bedienen, andererseits gut in die existierende Infrastruktur einzugliedern sein. Ein weiteres wichtiges Thema ist Cybersecurity. Hier fehlt es Unternehmen dieser Größenordnung oftmals an Know-How sowie einer dezidierten, für diesen Bereich zuständigen Person. Worauf bereits bei der Systemplanung von Sicherheitssystemen zu achten ist und wann es sich für Unternehmen beispielsweise anbietet, die Vernetzung zwischen Geräten, Services und Anwendungen zu begrenzen, erklären die Sicherheits-Experten von Axis im Gespräch in Halle 10.0 / Stand 518. ■

it-sa 2018, Halle 10.0, Stand 518

Managed Security Services

Im Fokus der Telekom Security stehen in diesem Jahr die Themen Next Generation SOC und Managed Security Services. Dazu beantworten Fachexperten den Besuchern Fragen wie „Welche Sicherheitsmaßnahmen sind erforderlich um besser auf APT Angriffe vorbereitet zu sein?", „Wie kann mit Managed SOC Services der Schutz von Unternehmen verbessert werden?" oder „Warum funktionieren Standard IT-Konzepte nicht als industrieorientierte Cyber-Verteidigungsstrategien?" ■

it-sa, Halle 9, Stand 9-642

Endpoint Security

EgoSecure, nach eigenen Angaben deutscher Marktführer für Endpoint Security, gehört seit Juni dieses Jahres zum Frankfurter Endpoint-Management-Spezialisten Matrix42. Durch die Verbindung beider Lösungsportfolios entsteht eine integrierte Lösung für ein Rundum-Security-Management aller Endgeräte, die neben höherer Produktivität der IT kompromisslose Sicherheit garantiert. Auf der it-sa wird zudem die neue Funktion Data Loss Prevention (DLP) präsentiert: Diese prüft Dokumente auf sensible Daten und blockiert, wenn nötig, um Datenmissbrauch oder -verlust zu verhindern. ■

it-sa, Halle 9, Stand 9-411

Industrie 4.0

Nachdem Börsengang 2017 hat sich bei ForeScout und im DACH-Team Einiges getan. Unter der Führung von Regional Director DACH Stephan von Gündell-Krohne liegt der Schwerpunkt nach dem Produkt-Launch von CounterACT 8.0 im Bereich Industrie 4.0. Durch den agentenlosen Ansatz ist der Netzwerksicherheitsexperte der Ansprechpartner beim Thema Sicherheit für OT & IT. ■

it-sa, Halle Halle 9, Stand 9-410

Dynamisches SIEM

LogPoint ist im letzten Jahr stark gewachsen, was sich in seiner stark gewachsenen Präsenz auf der it-sa, neuen Technologiepartnerschaften – beispielsweise mit DFLabs – und einem überarbeiteten Channel-Programm widerspiegelt. Die dynamische SIEM-Lösung mit UEBA und automatisierten Incident Response-Technologien ermöglicht es Organisationen, ihre Daten in verwertbare Informationen zu verwandeln, die ihre Cybersicherheit verbessern und einen geschäftlichen Mehrwert schaffen. ■

it-sa, Halle 9, Stand 9-442

Schwachstellen managen

Qualys, der Pionier und Marktführer im Bereich Schwachstellen-Management hat seine Scans auch auf IoT-IP-Adressen ausgeweitet. Es dreht sich alles darum, Schwachstellen zu scannen und zu erkennen, bevor Angreifer diese über Zero-Day Exploits ausnutzen können. Dazu gibt es eine Menge News rund um die Cloud-Plattform, wie eine kostenlose Community Edition, eine WAS-Lösung für DevOps oder die neue Container Security (CS) App. ■

it-sa, Halle 9, Stand 9-654

TU Darmstadt: Mehr Sicherheit für Alexa, Siri & Co.

Im Profilbereich Cybersecurity der TU Darmstadt arbeiten Wissenschaftlerinnen und Wissenschaftler an verschiedensten Herausforderungen im Bereich von IT-Sicherheit und Privatheit. Das Thema sichere sprachgesteuerte Dienste ist eine von ihnen. Mittlerweile sind sie im Leben vieler Nutzerinnen und Nutzer allgegenwärtig: Amazons „Alexa", Apples „Siri", Googles Assistant oder Microsofts „Cortana" stehen mehr als zwei Milliarden Smartphone-Nutzern jederzeit zur Verfügung. Gleichzeitig steigt die Zahl von Smart-Home-Geräten wie Amazon Echo, Apple HomePod, oder Google Home. Und auch im Unternehmensumfeld werden digitale Assistenten zur Steigerung der Produktivität erprobt.

Zwecks Spracherkennung werden dafür jedoch kontinuierlich Audioaufzeichnungen in die Cloud übertragen. Das birgt erhebliche Risiken, denn diese Aufnahmen enthalten sensible biometrische Daten und potentiell vertrauliche Informationen. Gerieten diese in die falschen Hände, drohte neben dem Verlust von (Betriebs-) Geheimnissen zusätzliche Gefahr, zum Beispiel durch „Fake Recordings". Das sind authentisch wirkende, jedoch künstlich erzeugte Sprachaufnahmen mit kompromittierendem Inhalt.

Um solche Bedrohungen bestmöglich einzudämmen, haben Wissenschaftler

der TU Darmstadt unter der Leitung von Professor Ahmad-Reza Sadeghi und Professor Thomas Schneider gemeinsam mit dem Spracherkennungsexperten Professor Korbinian Riedhammer von der Hochschule Rosenheim eine neue Softwarearchitektur namens „VoiceGuard" entwickelt. VoiceGuard nutzt Intel Software Guard Extensions (SGX), um die Sprachverarbeitungsprozesse von den Systemen des Dienstanbieters oder alternativ des Nutzers vollständig zu isolieren und sämtliche Daten zu schützen. Hierdurch wird sowohl die Privatsphäre des Nutzers als auch das geistige Eigentum des Dienstanbieters geschützt. ■

TU Darmstadt mit CRISP StartUpSecure auf der it-sa, Halle 10.0, Stand 516

Sicherheitstechnologien für Webapplikationen, Clouds und mobile Kommunikation

Zunehmend stellt sich heraus, dass die bisherigen IT-Sicherheitslösungen mit Hackern nicht Schritt halten können. Zudem sind diese oft komplex und schwer bedienbar. Das gilt besonders bei Lösungen für Web- und Cloud-Anwendungen sowie Messenger-Dienste. Rohde & Schwarz Cybersecurity zeigt auf der diesjährigen it-sa neue Sicherheitskonzepte, die diese Lücken schließen und dabei anwenderfreundlich sind. Von diesen und weiteren hochsicheren Security-Lösungen können sich Besucher vom 9.-11. Oktober 2018 überzeugen.

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

Die Firewall verfügt zudem über eine Workflow-Technologie, mit der die Sicherheitseinstellungen der R&S Web Application Firewall übersichtlich visualisiert und ganz einfach administriert werden können. Mit dem R&S Cloud Protector bietet Rohde & Schwarz Cybersecurity zudem eine SaaS-Version der R&S Web Application Firewall an. Sie lässt sich direkt im Browser öffnen und daher von überall aus bedienen.

Im Gegensatz zu herkömmlichen Netzwerk-Firewalls überprüft und schützt die R&S Web Application Firewall auch die Daten, die im http- bzw. https-Protokoll auf der Anwendungsebene verkehren. Diese Protokolle bilden die Grundlage für innovative IT-Prozesse sämtlicher Branchen und sind anfällig für Schwachstellen und daher besonders schutzbedürftig.

Datenzentrische Sicherheit für die Cloud

Rohde & Schwarz Cybersecurity präsentiert auf der Messe auch seine Sicherheitslösung R&S Trusted Gate, die Daten in der Cloud schützt. R&S Trusted Gate setzt auf eine neue Art der Absicherung von Daten in der Cloud und in Collaboration-Tools mittels „datenzentrischer Sicherheit". Dieser Ansatz konzentriert sich auf die Dateien, in welche die Sicherheit direkt integriert wird, anstatt sie an ein äußeres Tor zu übertragen.

Sicherer Messenger dank neuester Verschlüsselungsalgorithmen

Erstmals gezeigt wird die App R&S Trusted Communicator für iOS und Android. Über den R&S Trusted Communicator lassen sich sowohl Telefonate als auch Textnachrichten hochsicher übertragen. Der neuen Lösung liegt das Verschlüsselungsverfahren „AES-256" zugrunde. Mit diesem werden alle versendeten Informationen – Textnachrichten, Emojis, Dateianhänge oder Metadaten, wie z.B. der eigene Standort – sowie alle Telefonate lokal auf dem Smartphone verschlüsselt und erst auf dem Empfänger-Smartphone wieder entschlüsselt. Durch die durchgängige Ende-zu-Ende-Verschlüsselung haben Man-in-the-Middle-Angriffe keine Chance. Auch die lokal gespeicherten Kontakte bleiben – im Gegensatz zu vielen anderen Messenger-Diensten – für Dritte unter Verschluss.

it-sa, Halle 10.0, Stand 112

IoT-Geräte: Risiken von Anfang an zu minimieren

Trend Micro verstärkt sein Engagement für die Sicherheit im Internet der Dinge (IoT) mit einem neuen Programm. Die Zero-Day-Initiative (ZDI) des japanischen IT-Sicherheitsanbieters wird ihre Expertise im Bereich der Schwachstellenforschung zukünftig auch zur Beseitigung von Sicherheitslücken im Rahmen der Entwicklung intelligenter Produkte einsetzen. Trend Micro lädt zusätzlich Gerätehersteller dazu ein, ihre Geräte einzureichen. Sie erhalten dann Hilfe bei der Bewertung möglicher Schwachstellen, bevor sie die Geräte auf den Markt bringen. Untersucht werden diese von den weltweit führenden Forschungsteams des Unternehmens.

Die Analysten von Gartner erwarten, dass der Einsatz von Industrial-IoT-Systemen (IIoT) in Industrieanlagen und die rasante Zunahme der Anzahl der vernetzten Geräte dazu führen werden, dass sich Ereignisse in der virtuellen Welt häufiger auf die reale Welt auswirken. Ihren Schätzungen zufolge werden im Jahr 2021 rund 25 Milliarden IoT-Geräte mit dem Internet verbunden sein und diese Zahl auf absehbare Zeit weiter steigen. Selbst wenn nur ein sehr begrenzter Prozentsatz dieser Geräte IIoT-Geräte sind, welche industrielle Prozesse wie in der Fertigung steuern oder überwachen, wird die reine Anzahl und die Verbreitung von IIoT höchstwahrscheinlich zu einer Zunahme von Sicherheitsvorfällen führen. ■

it-sa, Halle 9, Stand 434

Telekom und Partner mit die Cyber-Sicherheit für DZ Bank

Cyberangriffe auf Finanzinstitute nehmen weltweit zu. Die Anforderungen der Regulierungsbehörden an die IT-Sicherheit der Geldhäuser steigen. Allerdings kann niemand mehr alleine die Herausforderungen der neuen Angriffe wirkungsvoll managen. Das haben die Fiducia & GAD IT AG (der IT-Dienstleister für alle 900 Volks- und Raiffeisenbanken in Deutschland) und die DZ Bank Gruppe erkannt: Gemeinsam mit Telekom Security arbeiten sie künftig zusammen, um die Cybersicherheit der genossenschaftlichen Finanzgruppe langfristig zu erhöhen. Den ersten konkreten Schritt in dieser Kooperation haben die Partner nun vollzogen: Rund um die Uhr bearbeitet ein so genanntes „Security Operation Center" (SOC) bestimmte IT-Sicherheitsvorfälle für die DZ Bank. Telekom Security und die Fiducia & GAD IT AG betreiben diese IT-Sicherheitszentrale gemeinsam. Telekom Security greift dabei auf die Experten im hauseigenen integrierten Cyber Defense und Security Operation Center in Bonn zurück. Diese überwachen rund um die Uhr Auffälligkeiten in den vorhandenen IT-Sicherheitssystemen der DZ Bank. Sobald ein Alarm eingeht, greifen die Bonner ein, analysieren den Vorfall und behandeln ihn nach zuvor mit der DZ Bank abgestimmten Vorgehensweisen. ■

Deutsche Telekom auf der Messe: it-sa, Halle 9, Stand 9-642

VERNETZUNG

HACKenschützen an der Hintertür

Cybersicherheit entlang der Lieferkette

Globale Zuliefer- und Produktionsbeziehungen sind selbst für mittelständische Unternehmen Realität. Diese komplexen Strukturen haben Einfluss auf die Cybersicherheit des Endprodukts. Denn dessen Cybersicherheit hängt stark von den Lieferanten ab. Anforderung ist, dass jedes Produkt nur exakt das tut, wozu es bestimmt ist und weder „Backdoors" noch nicht deklarierte Funktionen aufweist. Hersteller tragen die Verantwortung dafür, dass vernetzbare Smart-TVs, Waschmaschinen, Industriesteuerungen und Medizintechnik durch Schwachstellen nicht zum Einfallstor für Hacker werden.

Die Gewährleistung der Integrität der eigenen Zulieferkette ist eine unternehmerische Aufgabe – und Herausforderung. Die Unternehmen müssen Antworten auf verschiedene Fragen finden: Wie lässt sich sicherstellen, dass eingekaufte Hard- und Software zuverlässig den Erwartungen entspricht? Und wie gewährleisten, dass unsichere externe Produkte nicht die eigene Sicherheit oder die der Kunden gefährdet? Was sind die Möglichkeiten und wo die Grenzen der Bestimmung, Überwachung und Gewährleistung von Vertrauenswürdigkeit? Diese Fragen betreffen die Abteilungen Technik, Recht, Zulieferer- und Kundenmanagement gleichermaßen.

ZVEI-Sicherheitslagebild der Elektroindustrie: Vertrauenswürdigkeit von eingekaufter Hard- und Software hat große Relevanz

Um die aktuelle Lage der Elektroindustrie in puncto Cybersicherheit besser einschätzen zu können, hat der ZVEI gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Mitgliederumfrage durchgeführt. Das daraus entstandene Sicherheitslagebild zeigt: Mehr als die Hälfte der befragten Unternehmen waren in den vergangenen zwei Jahren von Trojanern und Ransomware betroffen. Hauptfaktor für Sicherheitsvorfälle in der Produktion waren Schwachstellen in der eingesetzten Software. Dieses Ergebnis verdeutlicht die Relevanz der Bewertung und Prüfung von eingekaufter Soft- und Hardware. 39 Prozent der Befragten haben das erkannt und geben an, dass das Thema Vertrauenswürdigkeit von eingekauften Komponenten relevant für das Supply-Chain-Management ist. 19 Prozent planen entsprechende Maßnahmen. Allerdings messen auch 28 Prozent der Integrität von eingekaufter Soft- und Hardware noch keine hohe Bedeutung zu.

Was können Hersteller tun?

Aus Sicht des ZVEI besteht hier Nachholbedarf. In Zukunft sollte jeder Hersteller wissen, was eingekaufte Hard- und Software für die Security des Endprodukts leisten und was nicht. Dazu gehört auch die Kenntnis darüber, welche Security-Prozesse die einzelnen Zulieferer für Entwicklung und Fertigung anwenden. Halten diese sich beispielsweise an die entsprechenden Normen ISO 27001 oder IEC 62443-4-1? Zudem sollten sich Hersteller frühzeitig darüber Gedanken machen, wie sie ihren Kunden transparent und aussagekräftig darstellen, dass sie selbst – wie auch ihre Zulieferer – Security ausreichend berücksichtigt haben. Um das Thema anzugehen, gibt es verschiedene Ansätze. Diese betreffen zunächst den Einkauf sowie das Vertragsrecht. Hersteller sollten Cybersicherheit zum festen Anforderungspunkt in ihren Einkaufsrichtlinien machen und außerdem ihre Zulieferer entsprechend abfragen.

Wo liegen die Herausforderungen?

Mit Security-Maßnahmen und -Informationen ist allerdings nur die Hälfte der nötigen Schritte getan, die Cybersicherheit gewährleisten können. Genauso wichtig ist es, Maßnahmen und Quellen auch zu bewerten und zu entscheiden, ob diese tatsächlich das gewünschte Maß an Security bieten. Um Zuliefererangaben und -produkte fachgerecht prüfen zu können, braucht es eigene Bewertungskompetenzen bzw. die Beratungskompetenz von Dritten. Langfristig ist der Aufbau eines P-CERs (=Product Computer Emergency Response Team) hilfreich, das Vorfälle analysiert, Kunden informiert und Security Lessons Learned für neue Produktgenerationen festhält. Nur so wird aus Cybersicherheit auch Vertrauenswürdigkeit in der Lieferkette. Zur Beurteilung der übergreifenden Cybersicherheit (über Landes-, Sektoren- und Ebengrenzen hinweg) gibt es zurzeit jedoch noch keinen fertigen Rahmen wie zum Beispiel internationale Standards oder einheitliche Herstellerselbsterklärungen. Um die Produktsicherheit (im Sinne der Security) zu steigern, sollte das zu den langfristigen Zielen gehören. In der Zwischenzeit muss dennoch jeder Hersteller mit seinen Zulieferern sprechen, Security einfordern und sich über Verbände und Plattformen informieren, was inzwischen allgemeine und übertragbare Security-Anforderungen sind. Neben staatlichen Stellen und dem ZVEI ist auch die Allianz für Cyber-Sicherheit dafür eine gute Anlaufstelle. Sie bietet kostenlos Hilfestellung für Unternehmen und unterstützt zudem ihre Mitglieder mit BSI-Warnungen, aktuellen Lagebildern, Lösungshinweisen und verschiedenen Schulungsangeboten.

Mehr Cybersicherheit entlang der Lieferkette: Was jetzt zu tun ist

Nach Auffassung des ZVEI ist die Vertrauenswürdigkeit von eigenen und Drittprodukten ein entscheidender Faktor, um Cyberangriffen zu begegnen und die Branche robust aufzustellen. Um zukünftig auch entlang der Lieferkette mehr Security gewährleisten zu können, schlägt der ZVEI vor, in allen vernetzbaren Produkten risikobasierte Maßnahmen zur Identifizierung und Authentifizierung, Rollen- und Rechtemanagement, sicheren Kommunikation und Monitoring der Cybersicherheit zu berücksichtigen. Damit diese Maßnahmen erfolgreich sein können, ist es jedoch von großer Bedeutung, dass Deutschland keine Sonderwege geht, sondern

vielmehr europäische und internationale Ansätze gewählt werden. Ziel sollte sein, dass Cybersicherheit international einheitlich von Zulieferern abgefragt und gegenüber den eigenen Kunden dargestellt werden kann. Entsprechende internationale Kategorien, Metriken und Standards fehlen jedoch bisher. Der ZVEI arbeitet an diesem Prozess mit und bringt seine Positionen in Europa sowie in internationale Partnerschaften (z.B. G20- und B20-Prozess) ein.

Vertrauenswürdigkeit ist auch ein Infrastrukturthema. Die IT-Infrastrukturen bilden das Rückgrat der „Economy of Things and Services". Mehrheitlich befinden sich diese in außereuropäischer Hand, was eine Herausforderung für Know-how-Schutz und Souveränität der Bürger, Unternehmen und Behörden in Europa darstellt. Der ZVEI setzt sich zusammen mit dem Bundesverband der Deutschen Industrie (BDI) sowie dem TeleTrust Verband für Ansätze wie der „IT Security Replaceability" in Produkten und Systemen ein. Anwendern soll standardmäßig die Möglichkeit gegeben werden, vertrauenswürdige (Security-)Komponenten an IKT-Produkte anschließen zu können, um ihr eigenes Schutzniveau zu erhöhen.

Zusätzlich fordert der ZVEI eine europäische Forschungs- und Technologieförderung, damit Gesellschaft, Politik und Industrie auch in Zukunft souverän agieren können.

Sicherheitslagebild der Elektroindustrie: https://www.zvei.org/themen/cybersicherheit/sicherheitslagebild-der-deutschen-elektroindustrie/

Autor
Lukas Linke,
Senior Manager Cybersecurity

Kontakt

ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Frankfurt am Main
Tel.: +49 69 6302 0
zvei@zvei.org
www.zvei.org

Multifunktionale Malware breitet sich aus

Kaspersky-Report zeigt Botnet-Aktivitäten für das erste Halbjahr 2018

In der ersten Hälfte dieses Jahres stieg der Anteil multifunktionaler Malware, die nicht für einen bestimmten Zweck entwickelt wurde, in Botnetzen an. Ausgenommen von Minern, die sich verdoppelt haben, ist dagegen der Anteil von monofunktionaler Malware gesunken. Das geht aus dem aktuellen Botnet-Report von Kaspersky hervor, für den mehr als 150 Malware-Familien und ihre Modifikationen in 60.000 Botnetzen untersucht wurden.

Die aktuellen Ergebnisse zeigen, dass der Anteil von monofunktionaler Malware (Single-Purpose-Malware), die über Botnetze verbreitet wird, gegenüber dem zweiten Halbjahr 2017 deutlich gesunken ist. Während in der zweiten Jahreshälfte 2017 noch fast jede vierte (22,46 Prozent) einzigartige schädliche Datei ein Banking-Trojaner war, war es in der ersten Hälfte dieses Jahres noch etwa jede siebte (13,25 Prozent); ein Rückgang um 41 Prozent. Darüber hinaus ging der Anteil von Spamming-Bots von 18.93 Prozent auf 12,23 Prozent und der von DDoS-Bots von 2,66 Prozent auf 1,99 Prozent zurück. Die einzige Art monofunktionaler Malware, die signifikant in Botnetzen anwuchs, waren Miner: ihr Anteil stieg von 2,9 Prozent in der zweiten Jahreshälfte 2017 auf 4,6 Prozent im ersten Halbjahr 2018 an, was dem allgemeinen Trend von bösartigen Minern entspricht [2].

Mehr RAT-Malware und Trojaner

Dagegen wuchs der Anteil von multifunktionaler Malware (Multi-Purpose-Malware), insbesondere RAT-Malware (Remote Access Tools), die nahezu unbegrenzte Möglichkeiten zur Nutzung des infizierten PCs bietet, an. Seit dem ersten Halbjahr 2017 verdoppelte (von 6,55 Prozent auf 12,2 Prozent) sich der Anteil der entdeckten RAT-Dateien, die über Botnetze verteilt werden. Zu den weitverbreitetsten RATs zählen Njrat, DarkComet und Nanocore, die aufgrund ihrer recht einfachen Struktur sogar von einem laienhaften Bedrohungsakteur modifiziert und so leicht für die jeweiligen Regionen angepasst werden können. Trojaner, die ebenfalls für unterschiedliche Zwecke genutzt werden können, zeigten dagegen nur ein geringes Wachstum (im zweiten Halbjahr 2017: 32,89 Prozent; im zweiten Halbjahr 2018: 34,25 Prozent). Wie auch Backdoors können Trojaner-Familien modifiziert und durch mehrere Command-and-Controll-Servers kontrolliert werden – je mit einem eigenen Ziel wie Cyberspionage oder Diebstahl von Anmeldeinformationen.

„Der Grund, warum RATs und andere multifunktionale Malware, bei Botnetzen die Nase vorn haben, liegt auf der Hand: Der Besitz eines Botnets ist sehr kostenintensiv; um Profit zu machen, müssen Cyberkriminelle jede Gelegenheit nutzen können, um mit der Malware Geld zu machen", so Alexander Eremin, Sicherheitsexperte bei Kaspersky Lab.

„Ein Botnet, das aus Multi-Purpose-Malware besteht, kann seine Funktionen relativ schnell ändern – vom Senden von Spam über DDoS hin zur Verteilung von Banking-Trojanern. Dies ermöglicht den Botnet-Betreibern, zwischen verschiedenen „aktiven" bösartigen Geschäftsmodellen zu wechseln, aber damit eröffnet sich auch die Möglichkeit eines passiven Einkommens: Der Eigentümer kann sein Botnet einfach an andere Kriminelle vermieten." ■

Kaspersky-Empfehlungen

Damit die eigenen Geräte nicht zum Teil eines Botnetzes werden, sollten Nutzer:

- die Software auf dem Computer stets auf dem aktuellsten Stand halten und Sicherheitsupdates gegen die neuesten Bedrohungen schnellstmöglich installieren. Denn ungepatchte Geräte können von Cyberkriminellen ausgenutzt und zum Teil eines Botnets gemacht werden.
- keine raubkopierte Software oder andere illegale Inhalte downloaden, da diese oft dazu genutzt werden, schädliche Bots zu verbreiten.
- eine robuste Sicherheitslösung wie Kaspersky Internet Security [3] verwenden, die eine Infektion mit Malware jedes Typs verhindert.

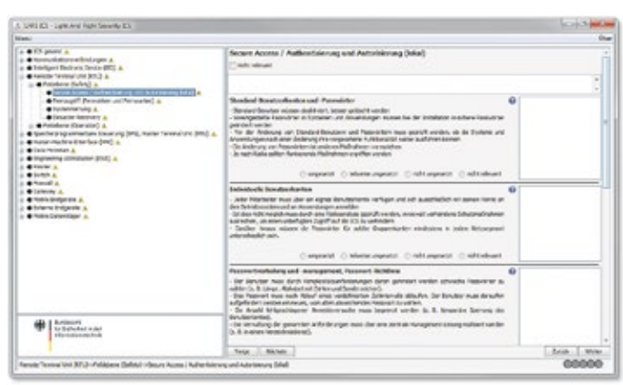
Kaspersky auf der Messe:
it-sa, Halle 9, Stand 520

KRITIS

Keine Panik!

Praktische Tipps für IT-Sicherheit in vernetzten Industrieanlagen

Durch die fortschreitende Vernetzung von Industrie und IT wird Cybersecurity zur Grundvoraussetzung für die Sicherheit moderner Industrieanlagen. Der IT-Sicherheitsexperte Udo Schneider vom IT-Sicherheitsanbieter Trend Micro erklärt, welche grundlegenden Maßnahmen zum effektiven Schutz vernetzter Industrieanlagen zu beachten sind. Angesichts immer wieder verbreiteter Bedrohungsszenarien ruft er zur Besonnenheit auf: „Keine Panik" ist laut Schneider das erste Prinzip einer sinnvollen IT-Sicherheitsstrategie. Ein Beitrag von Udo Schneider, Security Evangelist bei Trend Micro.



LARS ISMS: Geleitete ICS-Strukturanalyse

LARS-Hilfstext

Der Aufbau einer wirkungsvollen Security-Architektur ist nichts, was im Affekt passiert oder passieren sollte. Hier ist eine rationale Abwägung von Risiken und Gegenmaßnahmen gefragt. Daher sollten die Verantwortlichen nicht in Panik geraten (oder sich dazu drängen lassen), sondern mit der gebotenen Sorgfalt an das Thema herangehen.

Vorbild funktionale Sicherheit

Auch eine Risikoanalyse für die IT-Security lässt sich grob nach Begrifflichkeiten von bewährten Industrienormen der funktionalen Sicherheit (wie IEC 61508/ISA84) modellieren:

Basis einer sinnvollen Security-Strategie ist das Wissen um schützenswerte Güter. Im Grunde genommen handelt es sich dabei um eine Inventur aller am Produktionsprozess beteiligten Komponenten und deren Anbindung. Das schließt auch auf den ersten Blick „unschützbare" Geräte wie Steuerungen (SPS) aber natürlich auch nachgeschaltete Kontroll- und

Verwaltungssysteme wie SCADA oder HMI-Komponenten ein. Im ersten Schritt geht es dabei ausschließlich um die Erhebung der Komponenten – unabhängig von Bedrohungsszenarien und Schutzmöglichkeiten.

Im nächsten Schritt gilt es zu bewerten, welche Gefährdung von den zuvor gefundenen Komponenten ausgeht. Dabei sind Gefährdungen sowohl für die funktionale Sicherheit des Prozesses als auch die Verfügbarkeit, Integrität und Vertraulichkeit zu betrachten.

Risikoeinschätzung und -bewertung

Nun wird die Frage beantwortet, welche Lücken oder Verwundbarkeiten in den gefundenen Komponenten existieren. Dies fängt an mit einfachen Dingen, wie ungeänderten Wartungspasswörtern auf Steuerungen (SPS), oder nicht eingespielten Patches, zum Beispiel auf HMI-Systemen.

Die Informationen aus den vorherigen Schritten erlauben dann letztendlich eine Bewertung des Risikos. Damit einher geht auch eine Priorisierung der nötigen Minderungsmaßnahmen. Wie auch bei der „klassischen" funktionalen Sicherheit steht man nun vor der Entscheidung, was mit dem verbleibenden Risiko zu tun ist:

- Das Risiko ist klein genug, so dass sich eine weitere Reduktion nicht lohnt und nur noch dessen Dokumentation bleibt.
- Das Risiko ist in dieser Form nicht tragbar, so dass Risikominderungsmaßnahmen nötig sind.

Risikominderung

Aus der Risikobewertung entstehen priorisierte Risiken, die einer Minderung bedürfen. Die Minderungsmaßnahmen können dabei sowohl organisationstechnischer Natur (beispielsweise Einschränkung des physischen Zugangs) als auch technischer Natur (zum Beispiel Netzwerksegmentierung) sein. Wichtig ist, entsprechende Lösungen vor dem Hintergrund der Risikoanalyse auszusuchen. Der Griff zum erstbesten IT-Sicherheits-Produkt ist hier zu kurz gedacht. Das ist für die Sicherheit eines Betriebs schlicht nicht ausreichend und kann gefährlich werden, wenn die dazugehörenden Schritte zur Risikominderung nicht unternommen werden.

Zyklische Risikoanalyse

Der Risikoanalyse-Prozess der „normalen" funktionalen Sicherheit ist irgendwann abgeschlossen. Im Gegensatz dazu ist die Risikoanalyse im Bereich IT-Sicherheit endlos zyklisch. Das heißt aufgrund von neu bekannten Schwachstellen oder Angriffsmethoden ändert sich Gefährdungen und Risikoeinschätzung regelmäßig. Dementsprechend ist auch eine Risikoanalyse zyklisch durchzuführen.

Obwohl man durchaus eine IT-Security-Risikoanalyse nach Grundsätzen der funktionalen Sicherheit durchführen kann, gibt es inzwischen mit IEC62443/ISA99 neue Normen und Rahmenwerke, die deutlich expliziter auch IT-Security als Teil des Sicherheits- und Betriebskonzepts von industriellen Systemen modellieren.

IEC62443/ISA99

Die IEC62443/ISA99 ist eine Reihe von internationalen Industrienormen, die sich explizit auch mit der IT-Security in industriellen Umgebungen beschäftigt. Unter diesem Aspekt könnte man diese als „großen Bruder" der klassischen funktionalen Sicherheit nach IEC61508 beschreiben. Im Unterschied zu dieser werden aber konkret Anforderungen und auch Maßnahmen der IT-Sicherheit beschrieben.

Im Gegensatz zur funktionalen Sicherheit nach IEC61508, die man für IT-Sicherheit adaptieren muss – insbesondere bei der zyklischen Risikoanalyse, modelliert die IEC62443 von Anfang an einen zyklischen Risikobewertungsprozess, wie er aus anderen IT-Normen wie ISO27000 oder dem BSI-Grundschutz (entwickelt vom Bundesamt für Sicherheit in der Informationstechnik) bekannt und bewährt ist.

Maßnahmen

Die Erhebung und Dokumentation der Anlagen, deren Gefährdungen und Risiken, lassen sich sicherlich auch auf Papier durchführen. Sinnvoller ist aber die Nutzung eines ISMS – eines „Information Security Management System", das diese Informationen sinnvoll speichert, bündelt und wieder abrufbar macht. ISMS-Systeme, wie sie auch in der normalen IT-Sicherheit vorkommen, gibt es in jeder Geschmacks- und Preisklasse.

Eine Empfehlung zum Einstieg ist BSI LARS (Light And Right Security). Dabei handelt es sich um eine kostenlose ISMS-Software, die bewusst nur die im Industrieumfeld sinnvollen Maßnahmen modelliert. LARS mag zwar nicht so leistungsfähig sein wie andere Systeme – besser als die unstrukturierte Ablage der Informationen ist es aber auf jeden Fall. Nicht zu unterschätzen sind auch die mitgelieferten Hilfstexte, die verständlich die Gefährdungen und Maßnahmen erklären und gewissermaßen eine Übersetzung von Industrie-Deutsch in den IT-Security-Jargon erlauben.

Technische Maßnahmen

Technische Maßnahmen sind so vielfältig wie komplex. Angefangen bei einfachen Dingen, wie dem Ändern von Passwörtern, können unter anderem folgende Maßnahmen ergriffen werden: Netzwerksegmentierung, Gateway-Sicherheit, Absicherung von Schnittstellen und Fernzugriffen, Antiviren-Programme, Application Whitelisting, sichere Softwareentwicklung und Ausrollen auf SPS, Protokollierung und Reaktion. Diese Liste ließe sich beliebig fortführen.

Die Liste der technischen Maßnahmen zeigt schon allein aufgrund der schieren Anzahl von Technologien deutlich auf, dass der blinde Einsatz von Technologien und Produkten nicht sinnvoll ist. Wann welche Maßnahme Sinn ergibt, ist aber genau das Resultat eines sinnvoll betriebenen Risikoanalyseprozesses. Und damit schließt sich der Kreis: Panik hilft nicht. Das sinnvolle Vorgehen nach Best Practices der Industrie hingegen schon. ■

„Nicht verrückt machen lassen"

GIT SICHERHEIT: Herr Schneider, was ist für Sie die oberste Prämisse in der IT-Security?

Udo Schneider: Am wichtigsten ist es, die Ruhe zu bewahren. Insbesondere produktionsferne Branchen wie die IT-Security malen gerne den Teufel an die Wand. Da werden oft Schreckensszenarien bezüglich der Erreichbarkeit und Verwundbarkeit von Industrieanlagen und IoT-Geräten heraufbeschworen. Obwohl diese Szenarien durchaus realistisch sein können, sollten sich die Verantwortlichen davon nicht verrückt machen lassen.

Wo soll ein Unternehmen anfangen, wenn es seine IT-Sicherheit auf den neusten Stand bringen will?

Udo Schneider: Zunächst ist es ausschlaggebend, einen Überblick über alle schützenswerten Güter zu erstellen. Dabei handelt es sich im Wesentlichen um eine Inventur aller Komponenten und deren Anbindung an das Netz. Davon ausgehend können dann Risikobewertungen und -minderungen vorgenommen werden.

Wodurch unterscheidet sich IT-Security von klassischen Sicherheitsstandards in der Industrie?

Udo Schneider: Die Risikoanalysen für Industrieanlagen waren aus Safety-Sicht traditionell irgendwann abgeschlossen. Im Gegensatz dazu erfordert IT-Security eine zyklische Risikoanalyse. Sie muss regelmäßig neu betrachtet werden, da ständig neue Bedrohungen durch neu entdeckte Schwachstellen aufkommen können.

Kontakt

Trend Micro Deutschland
Hallbergmoos
Tel.: +49 811 88 99 0 700
thomas_rademacher@trendmicro.de
www.trendmicro.de

Wolf im Schafspelz: Cybergefahren müssen rechtzeitig identifiziert werden

KRITIS

Gefahr auf versteckten Pfaden

Kritische Infrastrukturen gegen Cyberattacken und Störungen sichern

Kritische Infrastrukturen sind einer zunehmenden Vernetzung der Anlagen und Prozesse unterworfen. Die dadurch vollzogene Öffnung und steigende Komplexität der Netzleittechnik hat nicht nur Auswirkungen auf die Cybersicherheit. Auch die operative Prozessstabilität und Kontinuität sind betroffen, wie aktuelle Ergebnisse aus Infrastrukturaudits zeigen.

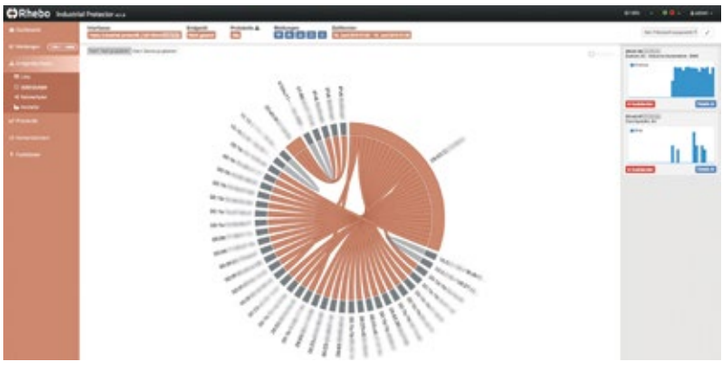
Der Cyber Check

- Industrial Security und Kontinuität basieren auf der lückenlosen Sichtbarkeit aller Vorgänge in den Netzwerken
- Eine industrielle Anomalieerkennung gewährleistet detailliertes Echtzeit-Monitoring der Netzleittechnik in KRITIS sowie ICS in Industrieunternehmen

Laut einer aktuellen Studie des Analystenhauses Forrester Consulting können nur 18 Prozent der Netzwerkverantwortlichen aus weltweit 600 Großunternehmen wirklich alle Komponenten und Teilnehmer in ihren Netzwerken identifizieren. 82 Prozent fehlt dagegen die Transparenz. Die Auswirkungen dieser Blindheit auf die Kostenstruktur können nur geschätzt werden. Allein im Bereich Cyberkriminalität bezifferte der Bitkom e.V. die Schäden in deutschen Unternehmen jüngst auf jährlich 55 Milliarden Euro. Dies berücksichtigt noch nicht die Schäden aufgrund operativer Störungen, die sich z. B. aus Netzwerkdegradation oder Fehlkonfigurationen ergeben.

Die Ergebnisse verschiedener Network-Condition-Monitoring-Projekte mit industrieller Anomalieerkennung zeigen diese Lücken immer wieder. Die Anomalieerkennung wird dafür rückwirkungsfrei und ohne Unterbrechung der operativen Prozesse in die Netzleittechnik integriert. Das System lernt dann die vorherrschende, erlaubte Standardkommunikation im Netzwerk und visualisiert vollständig alle Netzwerkteilnehmer und Verknüpfungen. Nachfolgend beginnt die kontinuierliche Überwachung jeglicher Kommunikation in der Netzleittechnik auf Inhaltsebene. Von der Standardkommunikation abweichende Datenpakete und Operationen werden in Echtzeit erkannt, nach Risiko bewertet und den Netzwerkverantwortlichen gemeldet.

Selbst in der Netzleittechnik und Industrial Control Systems (ICS), die mittels Firewalls, Intrusion Detection Systemen und ähnlichen Breach-Pre-



Vollständige Inventarisierung: industrielle Anomalieerkennung identifiziert Netzwerkteilnehmer und visualisiert Kommunikationsverbindungen

vention-Lösungen gesichert werden, finden sich durch diesen Monitoringansatz regelmäßig bislang unbekannte Netzteilnehmer, Schadprogramme und infrastrukturelle Schwächen.

Risiken durch Fehlkonfigurationen

Die Cybersicherheit kann dabei über versteckte Pfade gefährdet werden, wie das Bekanntwerden von Schwachstellen und professionellen Phishing-Kampagnen immer wieder zeigt. In vielen Fällen verraten sich Schadprogramme und Angreifer jedoch durch Kommunikation, die in einer industriellen Umgebung untypisch oder unerwünscht ist. So fand sich bei einem Monitoringprojekt das Protokoll HTTP in einem ICS. Die Detailanalyse der als PCAP gespeicherten Vorfallsdaten identifizierte ein Gerät im Netzwerk, das wiederholt versuchte, von einem externen Server ein Update herunterzuladen. Der Grund für diese Anomalie war glücklicherweise kein gezielter Cyberangriff, sondern war Teil der Standardeinrichtung des betroffenen Geräts. Jedoch war auch die Konfiguration des Netzwerkrouters fehlerhaft, welche die Kommunikation bis dato nicht unterband.

Angriff durch NotPetya

In einem anderen Fall wurde unerwartet über das Protokoll Server Message Block (SMB) kommuniziert. Dieses Netzwerkprotokoll für Datei-, Druck- und andere Serverdienste ist in industriellen Netzwerken in der Regel unerwünscht und daher auffällig. Gleichzeitig wurden neue Geräte im Netzwerk registriert. Auf den ersten Blick schien das legitim, denn das Gerät wurde als bereits bekannter Wartungslaptop identifiziert. Die Detailanalyse des Kommunikationsverhaltens zeigte jedoch, dass über das SMB-Protokoll eine Authentifizierung erfolgte und versucht wurde, eine unbekannte Datei auf einem anderen Rechner abzulegen. Diese entpuppte sich als Variante der Ransomware NotPetya.

Die Kommunikation konnte umgehend unterbunden und die involvierten Geräte unter Quarantäne gestellt werden.

Netzwerküberlastung durch unerwünschte Protokolle

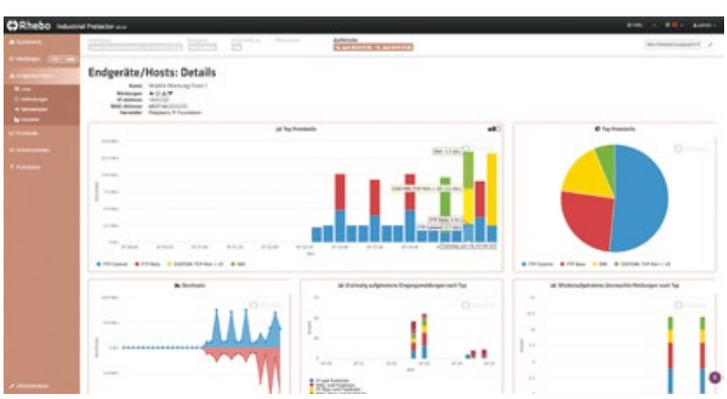
Störungen entstehen nicht immer durch Cyberangriffe. Bei einem Netzbetreiber fand sich so z. B. eine unverhältnismäßig hohe Netzwerkauslastung, welche die operativen Kapazitätsgrenzen bedrohte. Das kontinuierliche Network Condition Monitoring offenbarte eine Fehlkonfiguration bei den verwendeten Protokollen. Wie sich zeigte, wurden 40 Prozent der Kapazitäten durch Kommunikation über das LLC-Protokoll verbraucht. Das Protokoll kommt in der Regel nur vereinzelt zum Einsatz, um zwischen anderen Protokollen auf höheren Schichten der Netzwerkarchitektur zu vermitteln. In diesem Fall war dies aber unnötig und vom Betreiber unerwünscht. Aufgrund der Monitoringergebnisse konnte die Performance der Netzleittechnik maßgeblich verbessert werden.

Produktivität und Sicherheit entstehen über Sichtbarkeit

Diese Anomalien stellen nur einen Bruchteil der identifizierten Anomalien dar, die durch das Monitoring mittels industrieller Anomalieerkennung erstmalig sichtbar wurden. Die Network-Condition-Monitoring-Lösung schafft bei Unternehmen nicht nur eine grundlegende Transparenz der Netzleittechnik. Sie meldet im laufenden Betrieb auch jegliche verdächtige Kommunikation, die auf eine Veränderung des Netzwerkverhaltens und somit ein potentielles Störungsrisiko zurückschließen lässt. Als Anomalien werden dabei sowohl Übertragungsfehler, Netzwerkprobleme und -verschlechterung gemeldet, als auch bekannte und unbekannte Cyberangriffe (z. B. Advanced Persistent Threats) sowie manuelle Manipulation und Sabotage.

Das BSI fordert deshalb nicht ohne Grund ein Neudenken beim Management der Infrastrukturen. Im aktuellen IT-Sicherheitskatalog des BSI heißt es: »Zur Gewährleistung eines angemessenen Sicherheitsniveaus für TK- und EDV-Systeme, die für einen sicheren Anlagenbetrieb notwendig sind, ist die bloße Umsetzung von Einzelmaßnahmen, wie zum Beispiel der Einsatz von Antivirensoftware, Firewalls usw. nicht ausreichend.«

Eine industrielle Anomalieerkennung schließt als Teil des Defense-In-Depth-Konzepts diese Lücke.



Anomalieerkennung zeigt anomale Kommunikation einer Netzwerkkomponenten über die Zeit

Kontakt

Rhebo GmbH
Leipzig
Tel.: +49 341 3937900
info@rhebo.com
www.rhebo.com

IMPRESSUM

Herausgeber
Wiley-VCH Verlag GmbH & Co. KGaA

Geschäftsführer
Sabine Steinbach
Dr. Guido F. Herrmann

Geschäftsleitung Corporate Solutions
Roy Opie, Dr. Heiko Baumgartner,
Steffen Ebert, Dr. Katja Habermüller

Wissenschaftliche Schriftleitung
Dipl.-Verw. Heiner Jerofsky

Commercial Manager
Oliver Scheel +49 6201 606 748

Redaktionsteam
Dr. Heiko Baumgartner +49 6201 606 703
Regina Berg-Jauernig M.A. +49 6201 606 704
Dipl.-Betrw. Steffen Ebert +49 6201 606 709
Matthias Erler ass. iur. +49 6723 994 99 82
Sophie Platzer +49 6201 606 761
Lisa Schneiderheinze +49 6201 606 738

Mediaberatung
Miryam Reubold +49 6201 606 127
Textchef
Matthias Erler ass. iur. +49 6723 994 99 82

Herstellung
Jörg Stenger +49 6201 606 742
Claudia Vogel (Anzeigen) +49 6201 606 758

Satz + Layout Ruth Herrmann
Lithografie Elli Palzer

Sonderdrucke
Sophie Platzer +49 6201 606 761

Wiley GIT Leserservice (Abo und Versand)
65341 Eltville
Tel.: +49 6123 9238 246
Fax: +49 6123 9238 244
E-Mail: WileyGIT@vuservice.de
Unser Service ist für Sie da von Montag–Freitag zwischen 8:00 und 17:00 Uhr

Wiley-VCH Verlag GmbH & Co. KGaA
Boschstr. 12, 69469 Weinheim
Telefon +49 6201 606 0
E-Mail: git-gs@wiley.com
Internet: www.git-sicherheit.de

Verlagsvertretungen
Manfred Höring +49 61 59 50 55
Dr. Michael Leising +49 36 03 89 42 800

Bankkonten
J.P. Morgan AG, Frankfurt
Konto-Nr. 6161517443
BLZ: 501 108 00
BIC: CHAS DE FX
IBAN: DE55501108006161517443

Zurzeit gilt Anzeigenpreisliste Nr. 28 vom 1.10.2017. Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors.

Einzelheft 16 € zzgl. Porto + Mwst.
Schüler und Studenten erhalten unter Vorlage einer gültigen Bescheinigung einen Rabatt von 50 %.

Druck
pva, Druck und Medien, 76829 Landau
Printed in Germany, ISSN 0948-9487

SEE THE IIOT IN ACTION

London, UK – Oct 25th
Milan, Italy – Nov 8th
Munich, Germany – Nov 14th
Paris, France – Nov 20th

For more information:
www.moxa.com/IIoT/solution-day

JEDER SPRICHT ÜBER DAS IIOT

... wir setzen es einfach um.

Netzwerke und Computer für eine „smartere“ Industrie.

- Leistungsstarke Computer für Ihre Bedürfnisse designt
- Sichere und verlässliche Netzwerke – immer und überall
- Vertikale Integration von SCADA bis zu Feldgeräten

Moxa. Wo Innovation passiert.

www.moxa.com

MOXA®
Reliable Networks ▲ Sincere Service