GIT CYBER SECURITY

2019

EIN SPECIAL VON GIT SICHERHEIT + MANAGEMENT

PLUS:
Microsite
GIT-SICHERHEIT.de/
Cybersecurity

© rimom - stock.adobe.com

DIE RICHTIGEN SCHUTZMASSNAHMEN GEGEN CYBER-ATTACKEN

- **Chefsache Cybersicherheit** – und was zu tun ist
- **Produktregulierung** – welcher industrieübergreifende Plan helfen kann
- **Best Practices** – für das Industrial IoT
- **Angriffe auf Kritische Infrastrukturen** – und wie effiziente Abwehr aussieht

Mit Tipps und Cyber-Checks

Event-Partner: itsa

Gefördert von: AXIS COMMUNICATIONS | II/I | FP | INOVOLABS | MOXA | CHEManager | PHOENIX CONTACT

WILEY

ORGANISATIONEN INSTITUTIONEN UND UNTERNEHMEN IM HEFT INDEX SCHNELLFINDER

INHALT

CYBERTORIAL

Cyber-Karten auf den Tisch

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

Sprechen wir gleich mal Klartext: Es geht um Erpressung, es geht um Spionage, es geht um Sabotage. Das bedeutet Cyberkriminalität aus Sicht von Unternehmen aller Branchen. Der Kostenpunkt ist schwer einzuschätzen – aber nach Untersuchungen von Accenture werden in Deutschland im Schnitt so etwa 13 Millionen US-Dollar dafür bezahlt (2018), die Weltwirtschaft steuert wohl die 5 Billionen Dollar an Schäden an. Das sind Kosten und Umsatzeinbußen. Diese Zahlen stammen von Accenture – siehe den Beitrag „Cyber-Sicherheit ist Chefsache" ab Seite 9. Die Autoren empfehlen ihrer eigenen Branche eine „markant steilere Lernkurve", Investitionen in IT-Sicherheit und die Kooperation mit staatlichen Stellen und anderen Unternehmen.

Geht es um Cybersecurity, also Technik und Maßnahmen gegen Cyberkriminelle, ist die im Zusammenhang mit der Kindererziehung oft empfohlene Gelassenheit nicht das Mittel der Wahl, wie IT-Dienstleister Erwin Kruschitz von Anapur im Beitrag von Volker Oestreich (Seite 12) zitiert wird: Proaktives Handeln ist nötig. Dazu gehört auch die Weiterentwicklung der normativen Seite. Am besten geschieht das auf europäischer Ebene, sagt der ZVEI: Uwe Bartmann, Siemens-CEO und Vorsitzender des ZVEI-Fachverbands Sicherheit will dabei vor allem uneinheitliche Vorschriften für einzelne Produktsektoren verhindern. Er wünscht sich einen industrieübergreifenden Plan für eine einheitliche europäische Regelung der Cybersicherheit (unser Interview ab Seite 4).

In diesem Sonderheft zur Cyber-Security gehen unsere Autoren auch wieder vielen Einzelaspekten des Themas auf den Grund. Um den sicheren Datentransfer von der Maschinensteuerung in eine Cloud geht es ab Seite 20 im Beitrag von Carmen Klingler-Deiseroth – sie stellt u.a. den B&R-Site-Manager vor. Wie wichtig die Tugenden Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit für die Sicherheit in der digitalen Transformation sind, besprechen wir ab Seite 28 mit Dirk Rosenau von FP Innovolabs. Weitere Leseempfehlungen für diese Ausgabe: Videosicherheit mit Axis Communications (ab Seite 32) und das Thema Schifffahrt: Auch hier gibt es Cyber-Attacken, wie der Beitrag von Phoenix Contact auf Seite 22 deutlich macht. Schließlich geben wir Ihnen auf Seite 24 mit Moxa noch die Best Practices fürs Industrial Internet of Things mit auf den dann hoffentlich cybersicheren Weg.

Wir wünschen Ihnen eine interessante und hilfreiche Lektüre.
Bleiben Sie (cyber-)sicher!

Dr. Heiko Baumgartner
Heiko.Baumgartner@Wiley.com

Steffen Ebert
Steffen.Ebert@Wiley.com

Matthias Erler
Matthias.Erler@Wiley.com

PRODUKTREGULIERUNG

Harmonie erwünscht

ZVEI fordert EU-einheitliche Produktregulierung für Cybersicherheit

Eine Produktregulierung für Cybersicherheit muss EU-weit einheitlich und kompatibel zu globalen Standards und WTO-konform erfolgen – dies streicht der ZVEI in seinem Whitepaper „Horizontale Produktregulierung für Cybersicherheit" heraus. Dies in enger Abstimmung mit der Industrie umzusetzen, sei Aufgabe der europäischen Politik. Insbesondere die nachträgliche Einbringung der Cybersicherheit in bestehende Produktregulierungen schwäche die Wettbewerbsfähigkeit europäischer Unternehmen. Matthias Erler von GIT SICHERHEIT befragte dazu Uwe Bartmann, CEO Siemens Germany und Vorsitzender ZVEI-Fachverband Sicherheit.

Uwe Bartmann ist CEO Siemens Germany und Vorsitzender des ZVEI-Fachverbands Sicherheit

GIT SICHERHEIT: Herr Bartmann, Cybersicherheit ist Thema des Koalitionsvertrages – Stichworte sind an dieser Stelle das zweite IT-Sicherheitsgesetz und die Idee eines Gütesiegels. Gleichzeitig arbeitet die EU an einem europäischen Rahmenwerk für Cybersicherheits-Zertifizierungen. Der ZVEI befürchtet, dass es zu uneinheitlichen Vorschriften zur Cybersicherheit kommt. Wie real ist die Gefahr tatsächlich?

Uwe Bartmann: Leider sehr real. Denn neben IT-Sicherheitsgesetz, Gütesiegel und europäischem Rahmenwerk für Cybersicherheits-Zertifizierungen laufen zusätzlich noch die Sondierungsrunden der EU-Kommission zur Einbringung von Cybersicherheit in die Funkanlagen- und Maschinenrichtlinie. So wird derzeit von ganz unterschiedlichen Seiten die Regulierung von Cybersicherheit, auch auf Produktebene, bearbeitet. Bedenkt man, dass allein schon auf Seiten der EU-Kommission, des Ministerrats und des EU-Parlaments verschiedene Ausschüsse, Arbeitsgruppen und Akteure involviert sein werden, wird schnell klar, dass Inkonsistenzen bei der Regulierung von Cybersicherheit vorprogrammiert sind. Und die unterschiedlichen Prozesse und Stakeholder in den Mitgliedsstaaten kommen noch hinzu. Unsere Forderung im ZVEI ist daher: Eine Produktregulierung für Cybersicherheit muss vor allem EU-weit einheitlich erfolgen.

Wie sähe denn aus Sicht der Elektroindustrie die perfekte Lösung aus?

Uwe Bartmann: Wir brauchen zuallererst europäische Regelungen. Denn schließlich geht es auch um den europäischen digitalen Binnenmarkt. Wenn wir uns auf europäischer Ebene einigen, bleibt allerdings immer noch die Gefahr von verteilten, patchworkartigen Lösungen. Daher schlagen wir als ZVEI einen horizontalen Ansatz für Cybersicherheit auf EU-Ebene vor. Statt Cybersicherheit einzeln und im ungünstigsten Fall unterschiedlich zu integrieren, sollten wir eine übergreifende horizontale Regelung, ähnlich der EMV-Richtlinie, der Richtlinie für elektromagnetische Verträglichkeit, erstellen. Auf diese Weise kann man Cybersicherheit als Querschnittsthema zentral regeln und dennoch auf unterschiedliche Kontexte und Einsatzszenarien hin anpassen. Von Bedeutung ist, dass wir bei einer horizontalen Regelung innerhalb des sogenannten „New Legislative Framework" bleiben. Das heißt, Gesetze und Richtlinien formulieren das verbindliche Schutzziel für Cybersicherheit. Der Normung wird es jedoch überlassen, hierfür die konkreten Anforderungen und Bewertungskriterien zu definieren. Das ist wichtig, da die Gesetze andernfalls viel zu schnell immer wieder überarbeitet werden müssten, denn schließlich entwickelt sich der Stand der Technik schnell weiter.

Warum sind Sie dagegen, Cybersicherheitsregeln in bereits bestehende Produktrichtlinien einzubauen? Dies würde dann doch zu mehr oder

weniger EU-einheitlichen Regelungen führen, oder?

Uwe Bartmann: Eben nicht. Bestenfalls hätte man ein einheitliches Vorgehen. Doch bei der Anzahl der zu involvierenden Akteure würden sich auch die unterschiedlichen Interessen pro Richtlinie multiplizieren. Es ist sehr unwahrscheinlich, konsistente Ergebnisse zu erzielen, wenn wir so dezentral vorgehen. Ein weiterer Aspekt ist noch wichtig. Die Elektroindustrie liefert ihre B-to-C- und B-to-B-Produkte in unterschiedliche Bereiche und Domänen. Das gleiche Produkt kann somit einmal im Kontext der Funkanlagenrichtlinie und ein anderes Mal im Kontext der Maschinenbau- oder Niederspannungsrichtlinie oder Bauproduktenverordnung zum Einsatz kommen. Würden nun unterschiedliche Anforderungen, Bewertungskriterien und Prüfungsverfahren festgeschrieben, haben Hersteller und Kunden keine Chance mehr wettbewerbsfähig zu bleiben.

Gegen die „horizontale" Lösung könnte sprechen, dass Cybersicherheit ein Querschnittsthema ist, das alle Lebensbereiche früher oder später betrifft. Dennoch sind Sie gegen spezifische Lösungen, etwa für einzelne Industriesektoren?

Uwe Bartmann: Der Einwand beruht auf einem Missverständnis. Wenn wir als ZVEI von einem zentralen horizontalen Ansatz sprechen, dann bedeutet das nicht „One Size Fits All". Natürlich kann man nicht alle vernetzten Produkte im Verbraucher- und Industrieumfeld mit den gleichen Anforderungen, Maßnahmen und Bewertungskriterien belegen. In Abhängigkeit vom Einsatzzweck und dem entsprechenden Risikoumfeld müssen mehrere Produktgruppen gebildet werden. Hier können dann gestufte Anforderungen und Bewertungsmodule zum Einsatz kommen. Dieses Prinzip des „risikobasierten Ansatzes" kennt das „New Legislative Framework" bereits seit seiner Entstehung. Das ist nichts Neues. Eine zentrale horizontale Regelung lässt eine Stufung der Maßnahmen problemlos zu.

Horizontale Produktregulierung für Cybersicherheit: Ein Whitepaper des ZVEI

Die Herausforderung:
Die Digitalisierung und vernetzbare Endprodukte prägen immer stärker das Umfeld von Menschen, Unternehmen und Staaten. Einerseits entsteht dadurch tatsächlicher Nutzen. Andererseits steigt die Verantwortung jedes Endprodukts und damit jedes Herstellers, da sich die Endprodukte im Zuge der Vernetzung in größere Systeme integrieren lassen (z. B. Kommunikations- und Energienetz).

Spätestens mit dem Internet der Dinge (englisch IoT) wird de facto alles mit allem vernetzt werden können. Folglich können kompromittierte Produkte Einfluss auf das gesamte System nehmen und die Summe vieler kompromittierter vernetzter Produkte kann das Umfeld von Menschen, Unternehmen und nicht zuletzt Staaten prägen. Werden grundlegende Maßnahmen der Cybersicherheit (hier englisch Security) nicht umgesetzt, kann dies zur Beeinträchtigung von Umwelt, Gesundheit und Leben beziehungsweise der öffentlichen Sicherheit führen.

Die Folge:
Angesichts dieser Herausforderungen und jüngsten Ereignisse (siehe Mirai, WannaCry, Router-Vorfall etc.) ist verständlich, dass Cybersicherheit aus Gründen des Verbraucherschutzes durch die Politik adressiert wird. So hat die Bundesregierung die Erstellung eines zweiten IT-Sicherheitsgesetzes beschlossen, das Unternehmen und Produkte außerhalb der bisher definierten kritischen Infrastrukturen (Kritis) erfassen soll.

Darüber hinaus sieht der Koalitionsvertrag die Einführung eines Gütesiegels für IT-Sicherheit für vernetzbare Konsumgüter vor. Erste Pilotprojekte für technische Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Breitbandrouter und den Smart-Home-Bereich wurden gestartet. Es wird deutlich, dass Produkte zusätzlich zum bisherigen Kritis-Betreiber-Ansatz im Fokus der Politik stehen. Auf EU-Ebene steht die Einführung eines europäischen Rahmenwerks für Cybersicherheit-Zertifizierungen kurz bevor (siehe EU Cybersecurity Act). Zusätzlich gibt es ernst zu nehmende Überlegungen, Regeln für Cybersicherheit in bestehende Produktrichtlinien wie der Funkanlagen- oder Maschinenrichtlinie einzubringen.

Die Antwort der Elektroindustrie:
Aus Sicht der Elektroindustrie dürfen die Initiativen auf keinen Fall zu einer nationalen oder inkonsistenten Regulierung der Cybersicherheit führen. Es besteht die klare Notwendigkeit, dass eine Produktregulierung für Cybersicherheit EU-weit einheitlich und kompatibel zu globalen Standards und WTO-konform erfolgt. Dies in enger Abstimmung mit der Industrie umzusetzen, ist Aufgabe der europäischen Politik. Die nachträgliche Einbringung der Cybersicherheit in bestehende Produktregulierungen schwächt die Wettbewerbsfähigkeit europäischer Unternehmen.

Es darf nicht zu uneinheitlichen, inkompatiblen Vorschriften für einzelne Produktsektoren kommen. Die Elektroindustrie bevorzugt daher eine europäische horizontale Produktregulierung für Cybersicherheit für vernetzbare Endprodukte, wenn dadurch die Einbringung von Security-Vorgaben in bestehende sektorale Produktregulierungen verhindert und eine risikobasierte Basis-Cybersicherheit auf Grundlage des NLF etabliert wird.

Im Gegensatz dazu sollte es Ziel eines gemeinsamen Vorgehens der europäischen Politik und Industrie sein, ein domänen- und industrieübergreifendes Security-Schutzziel für vernetzbare Endprodukte verbindlich zu etablieren.

Das vollständige Whitepaper „Horizontale Produktregulierung für Cybersicherheit. Die Stärken des New Legislative Framework für den Digital Single Market nutzen" können Sie hier downloaden: https://bit.ly/2LRhJuR

Integratoren spielen neben den Herstellern für die Cybersicherheit dadurch eine Rolle, dass sie eine Lösung aus mehreren Einzelteilen herstellen, die dann erst eine Sicherheitsproblematik entstehen lassen. Welchen Regelungsbedarf sehen Sie hier?

Uwe Bartmann: Grundsätzlich muss auch der Integrator auf Basis einer Risikoanalyse und Abstimmung mit dem Kunden ein sicheres System bereitstellen. Dabei kommt es auf das Handling der Lieferkette und der Vorprodukte an. Der Integrator muss sein eigenes Risikoumfeld und das seines Kunden kennen und die Security daraufhin ausrichten. Entsprechend ist auch für den Integrator eine konsistente und übergreifende Regelung der Cybersicherheit – inklusive der Vorprodukte – wichtig.

Was sind aus Ihrer Sicht nun die nächsten Schritte, um die beste Lösung zu erreichen?

Uwe Bartmann: Die Idee der horizontalen Regelung muss eine europäische werden. Der ZVEI setzt sich jetzt dafür ein, dass der Ansatz nicht nur intensiv mit dem BSI, dem Bundesamt für Sicherheit in der Informationstechnik, abgestimmt wird, sondern vor allem auf europäischer Ebene mit Partnern, wie zum Beispiel Orgalim. Ziel ist, nach den Wahlen der neuen EU-Kommission einen industrieübergreifenden Plan für eine konsistente, einheitliche und europäische Regelung der Cybersicherheit vorzulegen. Ich bin fest davon überzeugt, dass diese Idee Ihre Wirkung nicht verfehlt. ■

Kontakt

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

EVENT

Cybersicherheit im Zeichen der Burg

Die Nürnberg Messe lädt zur it-sa 2019

Vom 8. bis 10. Oktober 2019 bietet die it-sa 2019 im Messezentrum Nürnberg ein umfassendes Angebot an Produkten und Lösungen für mehr IT-Sicherheit. Themen der Fachmesse sind u.a. Kritische Infrastrukturen, die globale Vernetzung von Produktionsketten und E- Health.

Der anhaltende Wachstumskurs der it-sa zeigt sich u. a. daran, dass die Fachmesse dieses Jahr erstmals vier Hallen belegt. Das begleitende Kongressprogramm Congress@it-sa startet bereits am Vortag, auch in diesem Jahr mit der Jahrestagung der IT- Sicherheitsbeauftragten in Ländern und Kommunen. Ebenfalls bereits am 7. Oktober findet UP19@it-sa statt, die zweite Ausgabe des „CyberEconomy Match-up" zur it-sa.

Seit mehreren Jahren zeichnet die it-sa mit zweistelligen Wachstumsraten bei der Aussteller- und Besucherbeteiligung die rasante Entwicklung der IT- Sicherheitsindustrie nach. Bei einer Befragung des Bundesverbands IT- Sicherheit TeleTrusT zur Messe-Präferenz seiner Mitgliedsunternehmen setzte sich die it-sa erneut mit an die Spitze.

Messe-, Foren-und Kongressprogramm

Wie in den Vorjahren präsentieren sich auf der Sonderfläche Startup@it-sa junge Unternehmen.

Das Programm der offenen Foren lockt auch in diesem Jahr mit rund 350 erwarteten Vorträgen: In jeder Halle finden zahlreiche Kurzvorträge der Aussteller statt, die IT-Sicherheitsfragen aus Perspektive von Management und Technik beleuchten.

Zu den Höhepunkten zählen die als „it-sa insights" ausgewiesenen Programmpunkte – produktneutrale Vorträge und Expertendiskussionen von Verbänden und Organisationen – sowie das „International Forum" als rein englischsprachige Vortragsbühne. Im Mittelpunkt der Forenbeiträge stehen unter anderem rechtliche Fragen und IT-Security-Trends wie der Einsatz künstlicher Intelligenz sowie IT- Sicherheit für Industrie 4.0 und kritische Infrastrukturen.

Das begleitende Kongressprogramm startet am 7. Oktober. Herausforderungen für IT- Sicherheitsverantwortliche werden dabei in mehreren Veranstaltungen aufgegriffen, die verschiedene Aspekte der IT-Security beleuchten. Die Jahrestagung der IT-Sicherheitsbeauftragten in Ländern und Kommunen macht Congress@it-sa erneut auch zur wichtigen Informationsplattform für Experten in Behörden und Verwaltung.

CyberEconomy Match-up geht in die zweite Runde

Am Tag vor der it-sa treten bei UP19@it-sa zwölf Start-ups aus dem IT- Sicherheitsbereich an, um potenzielle Investoren in einem Speed-Pitch zu überzeugen. Beim CyberEconomy Match-Up für Start-ups, Macher und Entscheider darf sich präsentieren, wer vorab die Fachjury überzeugen konnte. Sie bewertet das Gesamtpaket aus Angebot, Unternehmen sowie Vertriebs- und Marketingstrategie. Dem Gewinner des UP19@it-sa Award winkt ein individuelles Coaching und Mentoring durch den Digital Hub Cybersecurity und das Bayerische IT-Sicherheitscluster. Weitere Informationen unter: www.it-sa.de/up19. ■

Kontakt

NürnbergMesse GmbH
Tel.: +49 911 8606 4926
besucherservice@nuernbergmesse.de
www.nuernbergmesse.de
www.it-sa.de

FP Secure IoT

Smart-Retrofit für jede Produktionsanlage. Aber sicher.

FP Secure IoT: Sicher geschützter Cloudzugriff auf Ihre Produktion mit der Erfahrung von über 200.000 erfolgreichen Anwendungen

Bewährte Sicherheit fürs IoT von FP

Unsere Lösungen für harte Sicherheit in der Automatisierung

High-Security-Cloud-Zugang für sicheres Schreiben

Auf Basis des **FP**-Know-hows für hochsichere Datenübertragung steht eine führende Hochsicherheits-Edge-Technologie für das industrielle IoT zur Verfügung, die nicht nur in vielen Infrastrukturprojekten eingesetzt wird, sondern zunehmend auch in industriellen Produktionsanlagen ihre Vorteile ausspielt. Ein Beispiel ist die abgesicherte Übertragung von Parametern und Rezepturen direkt aus der Cloud-Software in die Maschinen. Für höchste Sicherheit bei dem kritischen Schreibzugriff sorgt ein zentraler Verschlüsselungs-Connector kombiniert mit lokalen HSM an den lokalen Edge-Gateways.

High Security: www.fp-secureconnect.com

Skalierbare Sicherheit mit FP Secure IoT Edge-Gateways

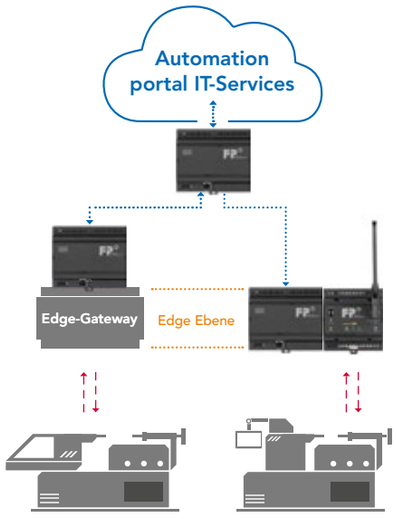
Zum modularen **FP**-Sicherheitskonzept gehören Elemente wie kryptografische integrierte Schaltkreise in den **FP**-Edge-Gateways für eine eindeutige Identifizierung. Trusted Platform Module (TPM) ist ein sicherer Einzelchip-Coprozessor, der kryptografische Schlüssel speichern und kryptografische Primitive für diese Schlüssel bereitstellen kann. Die dritte Stufe für den abgesicherten Schreibzugriff auf sicherheitsrelevante Anlagen beinhaltet das Hardware-Sicherheitsmodul. Dieses lässt sich jederzeit mit dem vorhandenen Edge-Gateway bei wachsenden Sicherheitsanforderungen kombinieren.

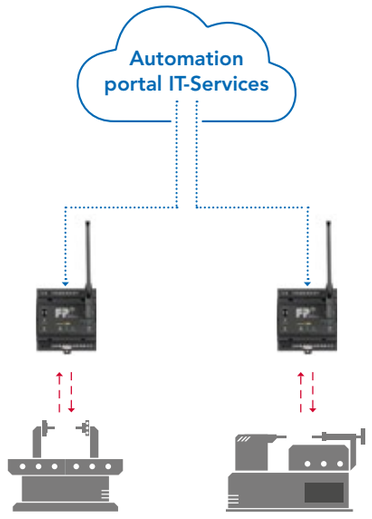
Retrofit: www.fp-otguard.com

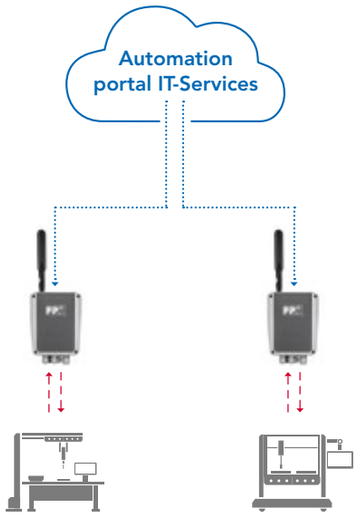
FP Secure IoT Compact-Gateways – kostengünstig und sicher

Auch die kostengünstigen Compact-Gateways sparen nicht an der Sicherheit. Mit integrierten Security-Smartcards oder aktivierbaren TPM-Prozessoren können die für kleinere Maschinen konzipierten Gateways die Sicherheit der übertragenen Daten gewährleisten. Durch die vielfältigen integrierten Schnittstellen und den gesicherten Cloud-Zugriff über Standard-Protokolle sind diese Gateways die ideale Lösung für die Retrofit-Nachrüstung von vorhandenen Maschinen oder Handarbeitsplätzen und dies, ohne Abstriche für die Sicherheit der Daten.

Economy: www.fp-compact.com







fp-secureiot.com

FP GERMAN MAILGENEERING

KRITIS – CHEMIE

Cyber-Sicherheit ist Chefsache

Mehr Sicherheit für Operational Technology und entlang der Supply Chain

Durch eine umfassende Vernetzung von Anlagen und Prozessen können Chemieunternehmen ihre Effizienz steigern und neue Geschäftsmodelle entwickeln. Das stellt jedoch hohe Anforderungen an die Cyber-Sicherheit der eigentlich als Insellösung konstruierten Operational Technology (OT) in den Werken. Und auch IT-Ökosysteme mit Partnern entlang der Lieferkette müssen besser geschützt werden. Vor allem aber muss Cyber-Sicherheit als Chefsache ernst genommen und entsprechend strategisch aufgesetzt werden. Ein Beitrag aus der Fachzeitung CHEManager – wie GIT Cyber Security aus dem Wiley Verlag.

Durch eine umfassende Vernetzung von Anlagen und Prozessen können Chemieunternehmen ihre Effizienz steigern und neue Geschäftsmodelle entwickeln. Das stellt jedoch hohe Anforderungen an die Cyber-Sicherheit der eigentlich als Insellösung konstruierten Operational Technology (OT) in den Werken. Und auch IT-Ökosysteme mit Partnern entlang der Lieferkette müssen besser geschützt werden. Vor allem aber muss Cyber-Sicherheit als Chefsache ernst genommen und entsprechend strategisch aufgesetzt werden.

Es kann jeden treffen – jederzeit. Rund um die Uhr attackieren Cyber-Kriminelle mit Viren, Trojanern oder anderer Malware IT/OT-Systeme. Bekannt sind derzeit etwa 800 Mio. Schadprogramme, gut 390.000 Varianten kommen täglich hinzu. Nur in der öffentlichen Wahrnehmung griffen Hacker lange bevorzugt dort an, wo Kundendaten als Beute locken – etwa, um Online-Konten bei Banken oder Internetshops zu kapern und so schnelles Geld zu machen. Tatsächlich sind aber auch Unternehmen der Chemie-, Pharma- und Metallindustrie sowie Energieversorger bei Cyber-Kriminellen beliebt.

Liste der Angriffsziele liest sich wie ein Branchen-Who-is-Who

Die Liste der Ziele von Attacken mit „Winnti“, „NotPetya“ oder „LockerGoga“ liest sich wie ein Who-is-Who der Branche. Laut IT-Verband Bitkom wurden in den letzten zwei Jahren drei von vier deutschen Chemie- und Pharmaunternehmen via Internet angegriffen. Auch Accenture-Studien zum Thema Cyber-Sicherheit zeigen, dass sich die Bedrohungslage durch Cyber-Angriffe weltweit verschärft und Unternehmen mehr Geld denn je ausgeben, um sich mit den Kosten und Folgen immer komplexerer Angriffe auseinanderzusetzen. In Deutschland lagen die durchschnittlichen Kosten für Cyber-Kriminalität im Jahr 2018 bei 13 Mio USD. Weltweit könnten die mit Angriffen verbundenen Kosten und Umsatzeinbußen in den nächsten fünf Jahren über alle Branchen hinweg auf bis zu 5,2 Bio. USD steigen. Denn sowohl die Zahl der erfolgreichen Angriffe als auch der im Schnitt verursachte

Firewalls mit BSI-Zulassungen bis VS-NfD ▲

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Firewall & VPN-Appliance Genuscreen 7.2 und das Mobile Security Device Genucard 7.2 für den Einsatz bis zur Geheimhaltungsstufe „VS - Nur für den Dienstgebrauch" (VS-NfD) zugelassen. Erstmals umfasst die Zulassung gemäß der neuen Verschlusssachenanweisung (VSA) neben den VPN- auch die Firewall-Funktionen beider Lösungen. Damit ist das deutsche IT-Sicherheitsunternehmen Genua GmbH der erste Hersteller, der Firewalls mit BSI-Zulassungen anbietet. Im staatlichen Geheimschutzbereich dürfen eingestufte Daten nur mit zugelassenen IT-Systemen bearbeitet werden. Die Lösungen von Genua ermöglichen die Einrichtung von sicheren Schnittstellen und verschlüsselten Übertragungswegen, um eingestufte Daten schnell und komfortabel auszutauschen. Die jetzt erteilten Zulassungen gelten für die Geheimhaltungsgrade VS-NfD sowie Nato und EU Restricted. „Mit diesem Erfolg setzen wir die Reihe unserer Produktzulassungen für den Geheimschutzbereich fort. Die Zulassungen bestätigten die hohe Qualität unserer Lösungen und sind starke Vertrauensanker für unsere Kunden", sagt Matthias Ochs, Geschäftsführer von Genua. ■

it-sa, Halle 10.0, Stand 112

Sicherer Datenaustauch in der deutschen grünen Cloud

Windcloud, deutsches Rechenzentrum mit ganzheitlichem CO_2-neutralen Ansatz, bietet seinen Kunden mit Managed Nextcloud eine Lösung, mit der sie Daten speichern und bereitstellen können. Die Nextcloud ist DSGVO-konform und damit auch für die Speicherung personenbezogener Daten nutzbar. Die Managed Nextcloud wird im deutschen Rechenzentrum von Windcloud gehostet und sticht aus der Menge der Anbieter – wie Dropbox oder Onedrive – vor allem durch den konsequent nachhaltigen Ansatz und die hohe Sicherheit hervor. Sie ist damit besonders für die Speicherung hochsensibler Daten geeignet und adressiert Anwender, für die Rechtssicherheit und Datenschutz besonders wichtig sind. Windcloud hat zu keinem Zeitpunkt inhaltlichen Zugriff auf die Nextcloud und die darin enthaltenen Daten, die Datenhoheit bleibt unberührt. Unter Verwendung von CEPH-Speichern ist die Managed Nextcloud dreifach redundant. Jeder Windcloud-Kunde erhält seinen eigenen virtuellen Server mit eigener Domain. Verschlüsselt werden die Daten per SSL. Zudem ist die lokale Verschlüsselung der Datenträger nach ISO 27001 zertifiziert. Windcloud mit Sitz in Schleswig-Holstein bezieht seinen Grünstrom für sein Rechenzentrum vorrangig aus lokalen Wind- und Solarparks. Darüber hinaus integriert Windcloud CO_2-absorbierende Technologien in die Rechenzentrumskühlung.

www.windcloud.org

Sicherer Datenverkehr

Als Teil der Digitalisierungsstrategie vom Tüv Süd bietet die Uniscon GmbH aus München hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. Uniscon legt den diesjährigen Messeschwerpunkt auf die Sealed Platform, die höchsten Datenschutz-Anforderungen gerecht wird. Anwendungen, die auf der versiegelten Cloud-Platform laufen, sind so sicher, dass selbst privilegierter Zugriff im Rechenzentrum oder auf Applikationsebene durch den Admin technisch ausgeschlossen ist. Zum Einsatz kommt die Cloud-Plattform überall, wo besonders schützenswerte und sensible Daten ausgetauscht werden, wie etwa in der Finanz- und Versicherungsbranche, im Gesundheitswesen und der Industrie. Am Uniscon-Stand erläutert Ihnen Dr. Hubert Jäger CTO und Gründer der Uniscon GmbH gerne die Sealed-Cloud Technologie. ■

it-sa, Halle 9, Stand 109

Schaden stieg in den vergangenen fünf Jahren um rund 70 %.

Die Wege der Hacker sind vielfältig: Erpressung, Spionage, Sabotage

Tatsächlich scheinen die Grundstoff- und Chemiebranche besonders verlockend für Hacker zu sein: Die Trans-Alaska-Pipeline etwa muss täglich im Schnitt rund 22 Mio. Cyber-Attacken abwehren und bezeichnet das als eines der drei größten Risiken für das Unternehmen. Wer tief genug ins Computersystem eindringt, kann erpressen: Angreifer verschlüsselten z. B. per „LockerGoga" Daten und forderten Lösegeld für den Freigabecode. Er kann Geschäftsgeheimnisse stehlen: Mithilfe von „Winnti" haben Hacker versucht, wertvolle Daten von deutschen Konzernen zu erbeuten. Außerdem kann er schlicht sabotieren, mit möglicherweise verheerenden Folgen: Hacker sollen versucht haben, die Sicherheitsmechanismen eines Gaswerks in Saudi-Arabien so zu manipulieren, dass diese bei Fehlfunktionen eine Explosion nicht verhindern. So eine Form der digitalen Sabotage könnte viele Menschenleben kosten.

Operational Technology muss besser geschützt werden

Gerade dieses Beispiel zeigt, warum die Chemieindustrie ihre Bemühungen um IT/OT-Sicherheit weiter intensivieren muss. Viele Konzerne setzen auf die Vorteile von Digitalisierung sowie Industriellem Internet der Dinge (IIoT) und vernetzen dafür auch früher weitgehend mit IT-Insellösungen betriebene Anlagen – etwa um mit den Betriebsdaten per Digital Twin eine effizientere Steuerung zu simulieren oder die Supply Chain zu verbessern. Dann muss die OT solcher Anlagen genauso gut geschützt sein wie die via Internet und Cloud laufende Konzern-IT – bis zur letzten Ventilsteuerung in der hintersten Ecke des Geländes, falls diese digital angebunden und nicht für reinen Handbetrieb ausgelegt ist.

Jede Schnittstelle bietet einen Angriffspunkt: Unlängst hätte ein Verschlüsselungstrojaner fast die Anlagensteuerung eines Chemieunternehmens lahmgelegt, weil ein Ingenieur versehentlich eine smarte Kaffeemaschine per WiFi mit dem Internet wie auch mit dem OT-System verbunden hatte. Auf dem Umweg über die Kaffeemaschine war die Schadsoftware in die Anlagensteuerung eingedrungen.

Schadprogramme verbreiten sich entlang der Supply Chain

Oft passiert so etwas auch über Geschäftspartner. Jede zweite Cyber-Attacke erfolgt in Form des sog. Inselhüpfens, gerade in der Industrie. Digitale Schädlinge springen dabei entlang der Supply Chain von einem Unternehmen zum nächsten. Alle Partner müssen bei Gegenmaßnahmen also an einem Strang ziehen. In den Führungsetagen der Chemiekonzerne wird dieses Thema durchaus ernstgenommen. 80 % der von Accenture befragten Top-Manager sind überzeugt, dass die Cyber-Sicherheit durch gemeinsame Anstrengungen verbessert werden sollte. Wachsende Komplexität in der Zusammenarbeit mache es unmöglich, sich innerhalb eines Partnernetzwerks punktuell von Betrieben abzuschotten, bei denen Zweifel an der IT-Sicherheit bestehen. Es fehlen aber noch passende Lösungen – und kritische Selbsteinschätzung: 77 % der Befragten meinen mit Blick auf ihre IT-Sicherheit, dass professionelle Partner unentbehrlich sind. Gleichzeitig ist kaum jeder Dritte überzeugt, dass seine Partner sich so gut um IT-Sicherheit kümmern wie die eigene Organisation. Es gibt also noch eine ganze Menge für mehr Vertrauen und Vertrauenswürdigkeit zu tun.

Chemiebranche braucht bei IT/OT-Sicherheit eine steile Lernkurve

Dabei hätten gerade Chemieunternehmen beste Voraussetzungen für IT/OT-Security auf Topniveau: Die Branche ist geprägt von einer Philosophie der Sicherheit. Über Jahrzehnte hinweg wurden Produkte und Prozesse immer sicherer, weil kleinste Fehler beim Betrieb einer Chemieanlage große Folgen haben können. Tatsächlich laufen die Werke heute unter physischen Gesichtspunkten so sicher wie nie zuvor. Nun gilt es, diese Erfahrung und Tradition in die digitale Welt zu bringen – mit einer markant steileren Lernkurve. Was sich bei Anlagen über Jahre hinweg optimieren ließ, gilt es beim IT-Einsatz angesichts der enormen Zahl von Cyber-Angriffen eher in Wochen als Monaten zu verbessern. Dafür sollte die Kooperation mit anderen Unternehmen sowie staatlichen Stellen verstärkt, die Zusammenarbeit mit Partnern im eigenen Ökosystem geprüft, die Investition in moderne Lösungen intensiviert sowie die IT-Kompetenz der Mitarbeiter erhöht werden.

Cyber-Sicherheit zählt zu den strategischen Aufgaben des CEO

Das erfordert Entscheidungen auf Vorstandsebene. In einigen Konzernen laufen die Fäden in Sachen IT-Sicherheit bereits beim Chief Information Security Officer (CISO) zusammen. Aber vorangehen muss der CEO. Denn vor umfassenden Investitionen in technische und organisatorische Lösungen sowie der Mitarbeiterschulung braucht es grundlegende Antworten auf die Frage, wie das Unternehmen für sich sowie als Teil eines Ökosystems mit Partnern arbeiten soll. Der Übergang zum digital ausgerichteten Geschäftsmodell muss begleitet werden von wirkungsvollen Maßnahmen für Cyber-Sicherheit, die dieses neue Geschäftsmodell ermöglichen. Das sind Chefentscheidungen – und deshalb sollten Maßnahmen zur IT-Sicherheit konzernweit einheitlich überwacht sowie optimiert werden. Ist die Richtung klar, können IT-Experten und Fachabteilungen die einzelnen Themen wie das Erkennen von Angriffen sowie das Response Management betrachten – und bspw. ein Sicherheitsprotokoll von ganz oben absegnen lassen, das die Abschaltung aller PCs binnen einer Stunde vorschreibt, um eine Virusinfektion einzudämmen. Ist ein Angriff erstmal erkannt, gilt: je rascher die Reaktion, desto besser. Hier hilft ein zuvor beschlossener detaillierter Reaktionsplan. Im Schnitt dauert es heute noch immer 206 Tage, bis verdächtige Aktivitäten überhaupt entdeckt werden.

So schützen sich Chemieunternehmen gegen Cyber-Attacken

Governance: Chemiekonzerne sollten auf globaler Ebene mit anderen Unternehmen sowie Regierungen und Aufsichtsbehörden kooperieren. Die Zusammenarbeit ihrer Führungskräfte und Experten mit externen Spezialisten erleichtert es, potenzielle Angriffe zu erkennen und wirkungsvolle Gegenmaßnahmen zu entwickeln.

Geschäftsarchitektur: Jedes Unternehmen muss sich intensiv mit den Grundprinzipien der Cyber-Sicherheit beschäftigen und sein Geschäftsmodell konsequent schützen – in der eigenen Organisation ebenso wie bei seinen Partnern entlang komplexer Lieferketten. So entsteht digitales Vertrauen innerhalb des gesamten Ökosystems.

Technologie: Investitionen in IT/OT-Sicherheit müssen Priorität bekommen – auch ohne sofort messbare Rendite. Es gilt, neue Technologien anzuwenden, moderne Software zu installieren, IIoT-Security zu beherrschen, Update-Funktionen auf mobilen und IIoT-Geräten zu aktivieren sowie sich auf die Quantum-Herausforderung vorzubereiten.

Schulungen: Selbst wenn die Technik perfekt scheint, bleibt der Risikofaktor Mensch. Die Mitarbeiter brauchen nicht nur eine moderne IT-Ausstattung, sondern müssen ihre Geräte auch richtig bedienen können. Zudem sollte ihnen ein Grundverständnis für verschiedene Arten von Cyber-Attacken sowie generell eine hohe Sensibilität für das Thema vermittelt werden.

Durchdachte IT/OT-Security wird künftig zum Verkaufsargument

Für mehr Cyber-Sicherheit müssen Unternehmen sich mit Partnern entlang der Supply Chain koordinieren: Mithilfe der Blockchain-Technologie könnte man Bestellungen z. B. transparenter und weniger angreifbar abwickeln. Die firmeninterne Entwicklung von Abwehrstrategien kann erfahrungsgemäß kaum das Tempo gehen, mit dem Cyber-Kriminelle immer wieder neue Angriffsvarianten austüfteln. Externe Spezialisten für Schutzmaßnahmen unterziehen nicht nur Business-Architektur sowie technische Ausrüstung einer genauen Überprüfung und unterstützt mit Konzepten für bessere Mitarbeiterschulung oder zielführendere Prozesse inklusive Sicherheitshandbücher. Sie können regelmäßig Angriffe auf Konzern-IT sowie OT-Systeme simulieren und so testen, ob bzw. wie gut Cyber-Attacken bemerkt und abgewehrt werden. Diese Erkenntnisse sollten in die kontinuierliche Verbesserung der Cyber-Sicherheit einfließen. Das wäre auch der erste Schritt von einer rein defensiven IT-Sicherheit hin zu einem offensiven System, in dem die erstklassige Sicherheitsarchitektur als Verkaufsargument beim Aufbau neuer Geschäftsbeziehungen dient. Außerdem müssen gut aufgestellte Unternehmen kaum fürchten, früher oder später vom Staat zu mehr IT-Sicherheit verpflichtet und eventuell in ein vorgegebenes System gezwängt zu werden. ■

Die Autoren

© Accenture

Götz Erhardt,
Geschäftsführer Grund- und Werkstoffindustrien sowie Energie, Accenture GmbH, Kronberg
goetz.erhardt@accenture.com

© Accenture

Herbert Kunzmann,
Geschäftsführer bei Accenture Security im Bereich Grund- und Werkstoffindustrien sowie Energie, Accenture GmbH, Kronberg
herbert.kunzmann@accenture.com

KRITIS – CHEMIE

Monitoring und Anomalieerkennung

Cyber-Angriffe auf Industrienetzwerke nehmen zu

Mit der zu beobachtenden Zunahme von Angriffen auf Produktionsnetzwerke und Netze in kritischen Infrastrukturen werden Maßnahmen zur Erkennung solcher Angriffe mehr denn je erforderlich. Diese müssen den komplexen Strukturen gerecht werden und erfordern daher entsprechende Systeme. Monitoring und Anomalieerkennung sind wichtige Komponenten der Verteidigungsstrategie. Ein Beitrag von Volker Oestreich aus der Wiley-Fachzeitung CHEManager.

Mit der zu beobachtenden Zunahme von Angriffen auf Produktionsnetzwerke und Netze in kritischen Infrastrukturen werden Maßnahmen zur Erkennung solcher Angriffe mehr denn je erforderlich. Diese müssen den komplexen Strukturen gerecht werden und erfordern daher entsprechende Systeme. Monitoring und Anomalieerkennung sind wichtige Komponenten der Verteidigungsstrategie.

Monitoring macht die Teilnehmer und Kommunikationsbeziehungen in einem Produktionsnetzwerk transparent und dient damit den allgemeinen Zwecken der Inbetriebnahme und Wartung. Als Überwachungslösung ist Monitoring ein geeignetes Mittel, um Abweichungen von vorgegebenen Verhaltensweisen und festgelegten Mustern zu erkennen. Anomalieerkennung ermöglicht die Erkennung untypischen Verhaltens und somit neben technischen Fehlerzuständen und Fehlkonfigurationen auch die Detektion bisher unbekannter Angriffsformen auf solche Netze. Dies unterscheidet die Anomalieerkennung von anderen Maßnahmen, die auf der Erkennung bereits bekannter Angriffe beruhen. In einer kürzlich veröffentlichten Cyber-Sicherheits-Empfehlung weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf die Bedeutung von „Monitoring und Anomalieerkennung in Produktionsnetzwerken“ hin.

Anomalien in prozesstechnischen Anlagen

Normungen und Vorgaben erfüllen das Herz eines Betreibers nicht immer mit Freude. Bei der BSI CS 134 wurde allerdings ein wichtiger Schritt in die richtige Richtung der IT / OT Security gemacht. Davon ist Dieter Barelmann, CEO von Videc Data Engineering, überzeugt. Er beschreibt den Ist-Zustand vieler Anlagen bezüglich der Security-Maßnahmen so: „Man stelle sich einmal vor, wir würden heute in prozesstechnischen Anlagen ohne Leit- oder SCADA System Produkte herstellen wollen. Keine Sichtbarkeit, keine Kontrolle über den Prozess. Die Automatisierung läuft, jedoch kann man nichts über den Zustand der Anlage aussagen. Undenkbar – aber im Bereich der OT Security ist es Stand der Dinge.“

Wir beobachten einen Anstieg der Angriffe auf deutsche Unternehmen mit teilweise existenzbedrohenden Datenverlusten.“

Jens Wiesner, BSI

Nur wenn wir IT Security als Voraussetzung der Digitalisierung begreifen, können wir langfristig von ihr profitieren.“

Arne Schönbohm, BSI-Präsident

Durch die immense Erhöhung der Teilnehmer in Prozessanlagen und entsprechend auch der Kommunikation ist kaum noch jemandem bekannt, wer mit wem kommuniziert – berechtigt oder auch nicht; insbesondere wenn mehrere Anlagenteile von unterschiedlichen Lieferanten installiert werden. „Durch die steigende Komplexität im Netzwerk und die Implementierung von nicht immer vollständig IP-standardkonformen Geräten kommt es immer wieder zu Seiteneffekten im Netzwerk, die zunächst nicht bemerkt werden und irgendwann zu einem Störfall werden können. Dies wäre mit einer kontinuierlichen Überwachung des Netzwerkverkehrs aufgefallen und vermeidbar gewesen“, äußert sich Barelmann und bricht eine Lanze für das passive Monitoring: „Wenn erst einmal ein Netzwerk z. B. über einen infizierten Programmierrechner unbemerkt befallen ist, kann sich der Angreifer weiter austoben. Sogar Schadcode nachzuladen würde von einer Firewall nicht verhindert werden, da der Verbindungsaufbau ins Internet aus der internen Zone erfolgt. Hier hat das BSI aus Sicht der IT-Sicherheit dem Hase-und-Igel-Spiel zwischen dem Angreifer und dem Schützenden einen wichtigen Impuls zugunsten des Betreibers gegeben. Die Vorteile des passiven Monitorings sind dabei neben der Möglichkeit der Angriffserkennung vielschichtig: Jeder Anlagenbetreiber hat sofort alle Teilnehmer im Blick und externe Dienstleister lassen sich über die Zugänge genau kontrollieren. Zusätzlich erhält die IT wichtige Informationen für die Feinjustierung der Firewall, ein wichtiger Punkt bei der Angriffsabwehr. Bei der Alarmierung in der Angriffserkennung lässt sich der Servicebereich in der Regel optimieren und spart Kosten.“

Die unterschiedlichen Ansichten über eine aktive bzw. passive Abfrage der Assets sind für Barelmann aus Sicht der Automatisierung sehr einfach zu klären: Die sensible Struktur der Automatisierungsgeräte mit ihren unterschiedlichen Generatio-

nen ist bei einem 24/7 Betrieb keine Spielwiese für aktive Abfragen. Das höchste Gut der OT ist die Verfügbarkeit – diese verträgt lediglich die passive Variante.

Gezielte Cyber-Angriffe auf Unternehmen

Generell registriert das BSI derzeit verstärkt Netzwerkkompromittierungen bei Unternehmen, die mit der manuellen und gezielten Ausführung eines Verschlüsselungstrojaners (Ransomware) enden. Dabei verschaffen sich die Angreifer mittels breit angelegter Spam-Kampagnen wie Emotet zunächst Zugang zu einzelnen Unternehmensnetzwerken und erforschen dann manuell Netzwerk und Systeme der Betroffenen. "Wir erleben derzeit die massenhafte Verbreitung von raffinierten Angriffsmethoden durch die organisierte Kriminalität, die bis vor einigen Monaten nachrichtendienstlichen Akteuren vorbehalten waren. Unternehmen sollten auch kleine IT-Sicherheitsvorfälle ernst nehmen und ihnen konsequent begegnen, da es sich dabei durchaus auch um vorbereitende Angriffe handeln kann", konstatiert BSI-Präsident Arne Schönbohm.

Das BSI konnte in den letzten Monaten großangelegte Malware-Kampagnen analysieren, bei denen vor allem maliziöse Anhänge oder Links zu gefälschten Webseiten in massenhaft versendeten Spam-Mails als Einfallsvektor dienten. Nach einer erfolgreichen Infektion wurde häufig weitere Malware (z. B. Trickbot) nachgeladen, um sich im Netzwerk auszubreiten, Zugangsdaten zu erbeuten und das Netzwerk bzw. die Systeme auszuwerten. Nach einer erfolgreichen Ransomware-Infektion sind teilweise sehr hohe Bitcoin-Forderungen gestellt worden. Dabei sind wiederholt keine pauschalen Forderungen aufgestellt, sondern individuelle Zahlungen ausgehandelt worden.

Insbesondere in Deutschland ist diese Vorgehensweise verstärkt mit der Ransomware GandCrab beobachtet worden. Bei den bekannten Fällen haben die Angreifer sich zunächst über Fernwartungstools (z. B. RDP, RescueAssist, LogMeIn) Zugriff auf das Netzwerk verschafft, auf verschiedenen Systemen im Netzwerk der Opfer eine Backdoor installiert, potentielle weitere Opfer ausgespäht und schließlich die Ransomware zur Ausführung gebracht.

Obwohl bei diesem Szenario prinzipiell keine neuartigen Angriffstechniken verwendet werden, waren derartig gezielte und manuell ausgeführte Angriffe im Cybercrime-Umfeld bisher selten zu beobachten. Insbesondere die folgenden drei Aspekte sind zu berücksichtigen:

- Jede einfache Infektion kann zu einem gezielten Angriff führen, da die Angreifer sich zunächst über groß angelegte Kampagnen Zugriff auf viele Netzwerke verschaffen. Jede Primärinfektion (z. B. mit Emotet) kann später weitreichende Folgen haben. Es sollte genau geprüft werden, welche Zugangsdaten potenziell abgeflossen sein könnten und Maßnahmen ergriffen werden, die eine spätere Rückkehr des Angreifers verhindern.
- Es droht ein kompletter Datenverlust, da im Gegensatz zu automatisierten und breit angelegten Ransomware-Kampagnen die manuell ausgeführten Angriffe zwar einen deutlich höheren Arbeitsaufwand für die Angreifer bedeuten, sie jedoch gezielt lukrativere Ziele angreifen und u.U. Backups so manipulieren bzw. löschen, dass diese nicht mehr zur Wiederherstellung der Systeme zur Verfügung stehen.

> Keine Sichtbarkeit, keine Kontrolle über den Datenverkehr – im Bereich der OT Security ist es Stand der Dinge."
>
> **Dieter Barelmann, Videc Data Engineering**

- Die Gefahr für deutsche Unternehmen steigt. Das BSI beobachtet einen Anstieg der Fallzahlen bei deutschen Unternehmen mit teilweise existenzbedrohenden Datenverlusten. Dabei haben unterschiedliche Gruppen unterschiedliche Ransomware und Tools verwendet.

Unternehmen, die eine Malware-Infektion erlitten haben, sollten Geschäftspartner oder Kunden zeitnah über den Vorfall informieren und auf mögliche zukünftige Angriffsversuche per E-Mail mit gefälschten Absenderadressen ihrer Organisation hinweisen.

> Das IT-Sicherheitsgesetz in der zweiten Version bringt Verschärfungen für Systemhersteller und Anwender."
>
> **Erwin Kruschitz, Anapur**

Um sicherzugehen, dass die Unternehmen nicht selbst durch einen Geschäftspartner oder Dienstleister infiziert werden, sollten Netzwerkzugriffe und die Berechtigungen externer Dienstleister überprüft werden. Sollte der Dienstleister selbst Opfer eines Ransomware-Angriffs werden, könnten die Angreifer sonst z. B. über existierende VPN-Verbindungen in das eigene Firmennetzwerk eindringen.

Grundsätzlich rät das BSI dringend davon ab, auf etwaige Forderungen der Täter einzugehen.

Angriffspfade und Fehlerkultur

Auch auf die Prozessindustrie sind in jüngster Zeit zahlreiche dokumentierte Angriffe ausgeübt worden. Darauf weist Jens Wiesner, Referatsleiter „Cybersicherheit in Industrieanlagen" des BSI, hin. Nach dem bekannten Cyber-Angriff auf Norsk Hydro im März 2018 mit LockerGoga gab es im Januar 2019 mit der gleichen Ransomware Angriffe auf die französische Ingenieurgesellschaft Altran, die vor allem in der Technologieberatung tätig ist. Im März 2019 waren die beiden amerikanischen Chemieunternehmen Hexion, ein Produzent von Duroplastharzen und verwandten Spezialprodukten, und die Momentive Performance Materials, der weltweit zweitgrößte Hersteller von Silikon und Silikon-Derivaten, betroffen.

Über welche Wege finden die Angreifer ihre Ziele? Wiesner nennt als die wichtigsten Angriffspfade, die in den letzten Jahren mit wachsender Tendenz benutzt wurden:

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten.

Viele der Angriffe nutzen bis an den Leichtsinn grenzendes fehlendes Know-how und mangelnde Ausbildung aller Beschäftigten bezüglich Cyber Security. So beschreibt dann auch Erwin Kruschitz, Vorstand der Anapur, die Situation bildlich: „Aus meiner Wahrnehmung als Berater und Auditor kann ich sagen, dass die Security in der Prozessindustrie den Kinderschuhen entwächst. Über die Pubertät sind wir allerdings wohl auch noch nicht hinweg." Als wichtige Komponenten auf dem Weg zum erwachsen werden fordert er,

- Komponenten zu entwickeln, die Security bereits mitbringen d. h. nicht erst noch abgesichert werden müssen
- Vertrauensvolle Kommunikations- und Fehlerkultur zu leben, z. B. zwischen Herstellern und Anwendern oder zwischen Betroffenen und dem Rest der Community
- mehr Know-How aufbauen.

Entsprechend dieser Erkenntnis reagiert auch der Staat, so Kruschitz. Aktuell entsteht das IT-Sicherheitsgesetz in der zweiten Version mit Verschärfungen für Systemhersteller und Anwender. Das BSI entwickelt ein Grundschutzprofil für die Chemieindustrie. Das kann dazu beitragen, dass es eine deutschlandweite Harmonisierung der Security- Anforderungen geben wird. Aktuell variieren die Vorgaben noch in Abhängigkeit vom Bearbeiter beim jeweiligen Regierungspräsidium bzw. Gewerbeaufsichtsamt.

Auf sein Bild mit den Heranwachsenden zurückkommend resümiert Kruschitz: „Gelassenheit ist sicher eine entscheidende Tugend von Eltern pubertierender Kinder. Im Gegensatz dazu gilt für den Bereich der Cybersecurity, dass ausschließlich proaktives Handeln aus der Adoleszenz führt. Dabei gibt es noch viel zu tun." ■

www.bsi.bund.de
www.anapur.de
www.videc.de

KRITIS – CHEMIE

Gemeinsam gegen Hacks

Sichere IT-Strukturen in der Prozessindustrie

NAMUR (Interessengemeinschaft Automatisierungstechnik der Prozessindustrie) und BSI (Bundesamt für Sicherheit in der Informationstechnik) eint das Ziel sicherer IT-Strukturen in der Prozessindustrie. Deshalb wurde im Herbst 2018 die enge Zusammenarbeit beschlossen und institutionalisiert. Wie sieht der aktuelle Stand der Kooperation aus? Lesen Sie hierzu ein Interview mit Felix Hanisch, dem Vorstandsvorsitzenden der NAMUR und Leiter Industrial Automation bei Bayer. Das Gespräch führte Volker Oestreich für die Wiley-Fachzeitung CHEManager.

NAMUR (Interessengemeinschaft Automatisierungstechnik der Prozessindustrie) und BSI (Bundesamt für Sicherheit in der Informationstechnik) eint das Ziel sicherer IT-Strukturen in der Prozessindustrie. Deshalb wurde im Herbst 2018 die enge Zusammenarbeit beschlossen und institutionalisiert. Wie sieht der aktuelle Stand der Kooperation aus? CHEManager sprach dazu mit Felix Hanisch, dem Vorstandsvorsitzenden der NAMUR und Leiter Industrial Automation bei Bayer. Das Gespräch führte Volker Oestreich.

CHEManager: Herr Hanisch, mit der zunehmenden Vernetzung ergeben sich auch für die Chemieindustrie neue Bedrohungsszenarien. Wie sieht es mit der Cyber-Security in der Branche aus?

Felix Hanisch: Für die Chemie- und Pharmaindustrie steht Sicherheit schon lange an erster Stelle bei allem, was wir tun. Dabei geht es um die Sicherheit unserer Produkte, Prozesse und Anlagen, um die Sicherheit und den Schutz der Mitarbeiter, Kunden und Partner sowie der Umwelt. Sicherheit hat viele Facetten und IT-Security ist eine weitere, die in den letzten Jahren für uns in der Pro-

„Wir müssen noch immer mit Lieferanten von Anlagenmodulen oder Package Units über IT-Security entlang des Lebenszyklus diskutieren."

Felix Hanisch, Vorstandsvorsitzender der NAMUR

zessindustrie ständig an Bedeutung gewonnen hat. Heute ist IT-Security integraler Bestandteil unseres Sicherheitsmanagements.

Vor diesem Hintergrund haben wir uns bei der NAMUR letztes Jahr besonders gefreut, als das BSI auf unserer Hauptsitzung 2018 NAMUR-Mitglied geworden ist. Gleichzeitig haben wir uns dazu verpflichtet, die Allianz für Cybersicherheit des BSI in der Prozessindustrie bekannter zu machen und deren Ziele aktiv zu unterstützen.

Was kann die NAMUR in diese Zusammenarbeit einbringen?

F. Hanisch: Die NAMUR kann hier mit viel eigener Kompetenz punkten: seit vielen Jahren befasst sich unser Arbeitskreis 4.18 „Automation Security" unter der Leitung von Erwin Kruschitz und mit Beteiligung des BSI bereits mit den speziellen Aspekten von IT-Sicherheit in der automatisierungstechnischen Praxis. 2015 hat der Arbeitskreis mit der NAMUR Empfehlung NE 153 „Automation Security Agenda 2020" technologische Anforderungen an zukünftige Automatisierungslösungen formuliert. Hier war die Forderung klar: IT-Security muss integraler Bestandteil aller zukünftigen Komponenten sein und darf nicht beim Betreiber „on top" draufgesattelt werden müssen. Vor diesem Hintergrund ist es bedauerlich, dass wir noch immer mit Lieferanten, insbesondere von Anlagenmodulen oder Package Units, über IT-Security entlang des gesamten Lebenszyklus diskutieren müssen. Hier herrscht nach wie vor eine Denke von „gekauft wie gesehen". Sobald das Modul beim Betreiber steht, muss er sich drum kümmern. Fragen von Software-Versionierung und Hardware-Kompatibilität in der Zukunft werden gerne dem Kunden überlassen.

Die besonders enge Verknüpfung von Anlagensicherheit und IT-Security greifen wir mit dem NAMUR-Arbeitsblatt 163 auf …

Das was genau beinhaltet?

F. Hanisch: Bei der NA 163 geht es um die „IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen": Die IEC 61511 fordert IT- Risikobeurteilungen für PLT-Sicherheitseinrichtungen. NA 163 erläutert, für welchen Umfang, durch wen und wie häufig eine solche Risikobeurteilung durchzuführen ist. Anhand einer Checkliste kann diese Risikobeurteilung durch einen PLT-Ingenieur mit Grundkenntnissen in IT und Netzwerktechnik durchgeführt werden.

Unmittelbar vor der Veröffentlichung steht das NA 169 „Automation Security Management in der Prozessindustrie", womit konkrete Schritte zur Einrichtung eines systematischen Security-Managements unter Bezug auf die etablierten Normen und Standards wie IEC 61442, die ISO27000-Familie und VDI 2182 beschrieben werden. Und da sich die Bedrohungslage ständig und schnell verändert, haben wir mit der NAMUR „AK-Praxis" ein Format geschaffen, in dem Arbeitskreise sich schneller zu aktuellen Entwicklungen äußern können. Hier sind vom AK 4.18 Dokumente zum Patch-Management, zur Härtung oder Architektur von IT-Systemen veröffentlicht worden.

Was sind aktuell wichtige Themen, die die Zusammenarbeit zwischen NAMUR und BSI betreffen?

F. Hanisch: Mit dem vorliegenden Referentenentwurf zum IT-Sicherheitsgesetz 2.0 werden nicht nur die Befugnisse des BSI deutlich ausgeweitet, sondern auch die Anforderungen an und die Zugehörigkeit zu den KRITIS-Bereichen. Beides sind gute Gründe – neben dem schon gelebten intensiven fachlichen Austausch – warum NAMUR und BSI auch zukünftig weiter gemeinsam gegen Hacks vorgehen werden. Zu tun gibt es genug: der rasche Austausch zu Ereignissen in der Prozessindustrie, der das einzelne betroffene Unternehmen schützt, aber trotzdem eine zeitnahe Information aller ermöglicht, die Analyse neuer Angriffsvektoren und die Weiterentwicklung und Kommunikation von Gegenmaßnahmen. ■

Die Bedrohungsszenarien für industrielle Netzwerke verändern sich mit deren zunehmender Vernetzung und Komplexität ständig. Während neue Angriffsvektoren und -methoden auftauchen, bemühen sich die Betreiber von Automatisierungsnetzwerken, deren Sicherheit trotz dieser wechselnden Bedingungen weiterhin aufrecht zu erhalten. Eine Co-Veröffentlichung aus der Wiley-Fachzeitung CHEManager.

PRODUKTION

Orchestrierung in unternehmenskritischen Netzen

Mehr Transparenz, sicherere Authentifizierung und punktgenaue Zugriffsteuerung

Die Bedrohungsszenarien für industrielle Netzwerke verändern sich mit deren zunehmender Vernetzung und Komplexität ständig. Während neue Angriffsvektoren und -methoden auftauchen, bemühen sich die Betreiber von Automatisierungsnetzwerken, deren Sicherheit trotz dieser wechselnden Bedingungen weiterhin aufrecht zu erhalten.

Bereits den Überblick über die verbundenen Geräte zu behalten stellt dabei eine erste Herausforderung dar. Darüber hinaus stellen formale Anforderungen aufgrund neuer Normen und Regularien die Betreiber von OT-Netzwerken vor zusätzliche Herausforderungen. Bei der Bewältigung dieser beiden sehr unterschiedlichen und schwierigen Problembereiche spielt eine effektive Netzwerkzugangskontrolle eine wichtige Rolle.

Integrierte Lösungen können durch einen ganzheitlichen Ansatz den Weg für eine Zugangskontrolle der nächsten Generation in OT-Netzwerken ebnen. Diese bestehen aus einer Netzwerkzugangskontroll-Plattform, welche für Netzwerksichtbarkeit, Gefahrenbewertung und Zugriffskontrolle sorgt und Industrial Ethernet Switches, welche die Umsetzung der Netzwerkzugangskontrolle bis hinunter auf den Shop-Flor ermöglichen.

Neue Herausforderungen für die Cyber-Sicherheit

Die zunehmende Vernetzung mit der IT-Welt und des Internet of Things führt zu neuen Angriffsflächen in OT-Netzwerken. Dies zwingt deren Betreiber, bewährte aber überholte

Best Practices für die Sicherheit zu überdenken, um auf die neuen Anforderungen und Bedrohungen zu reagieren. Darüber hinaus sind einfache und früher wirksame Sicherheitsmethoden wie der Perimeter-Schutz durch eine zentrale Firewall und der sprichwörtliche „Air Gap“, also die vollständige Trennung des OT-Netzwerks von allen anderen vernetzten Ressourcen, nicht mehr praktikabel oder ineffektiv geworden.

Bei der Umsetzung neuer Sicherheitsmaßnahmen zur Bewältigung der veränderten Bedrohungsszenarien und der Ausweitung von Angriffsflächen stehen die Betreiber von OT-Netzwerken vor vier großen Herausforderungen:

- Mangelnde Transparenz ihrer Netzwerke

©stokkete - stock.adobe.com

- Eine große Anzahl installierter älterer Geräte
- Zusätzlicher Druck durch neue Vorschriften und Compliance-Regeln
- Anforderung, für alle unternehmenskritischen Anlagen der OT-Netzwerke auch weiterhin hohe Zuverlässigkeit und lange Betriebszeiten zu gewährleisten.

Wie können neue IT-Sicherheitsmaßnahmen bei der Erfüllung der Anforderungen in OT-Netzwerken hilfreich sein?

Fehlende Transparenz

Obwohl die Geräte und deren Kommunikationsbeziehungen in OT-Netzwerken oft klar definiert sind, kann es in der Praxis schwierig sein, den Überblick über die tatsächlich kommunizierenden Geräte zu behalten. In größeren Netzwerken herrscht zudem eine hohe Fluktuation an Netzwerkteilnehmern. Lieferanten und Wartungstechniker verwenden z. B. oft unterschiedliche mobile Systeme, um die Wartungsarbeiten durchzuführen. Darüber hinaus können „kreative“ Lösungen und schnelle Problembehebungen zu einer beträchtlichen Anzahl von versteckten oder unbekannten Geräten in der Fertigung führen. Diese sogenannte „Schatten-IT“ hat oft unzureichende Sicherheitseinstellungen und läuft oft mit veralteter Software, da sie beim regulären Patch-Prozess nicht beachtet wird. Bei versteckten oder vorübergehend verbundenen Geräten wie etwa Service Laptops und extern durch Remote Maintenance generierten Netzwerkaktivitäten ist im Netzwerk ein konstanter potenzieller Bedrohungsgrad vorhanden, der überwacht und beherrscht werden muss.

Konvergenz von Automatisierung und IT

Automatisierungsgeräte sollen teilweise jahrzehntelang betrieben werden können, um eine solide Kapitalrendite zu erzielen. Deshalb steht ein Austausch bereits installierter und ggf. zertifizierter bzw. qualifizierter Geräte meist nicht zur Diskussion. Somit muss oft auch langfristig mit einer Mischung aus Neu- und Altgeräten geplant werden, was die Umsetzung eines einfachen und einheitlichen Sicherheitskonzepts schwierig macht und oft zu verminderter Sicherheit führt. Die Kombination von Automatisierungs- und IT-Geräten mit unterschiedlichen Software- und

Security-Lösungen in einem Industrienetz kann leicht zu einer Verringerung der Sicherheit und der Verfügbarkeit führen.

Druck durch Audits und Compliance-Regeln

Vorschriften für kritische Infrastrukturen (Verkehrswesen, Stromerzeugung und -verteilung, Nahrungsmittel und Getränke, Wasser etc.) erhöhen den Druck, neue Sicherheitsprozesse einzuführen und zusätzlichen Standards zu beachten. Diese Standards erfordern sowohl organisatorische als auch technische Änderungen. Die zunehmenden Regulierungsanforderungen stellen die Betreiber deshalb vor zusätzliche Aufgaben, da sie Compliance-Aspekte in ihren technischen Sicherheitskonzepten jederzeit berücksichtigen müssen.

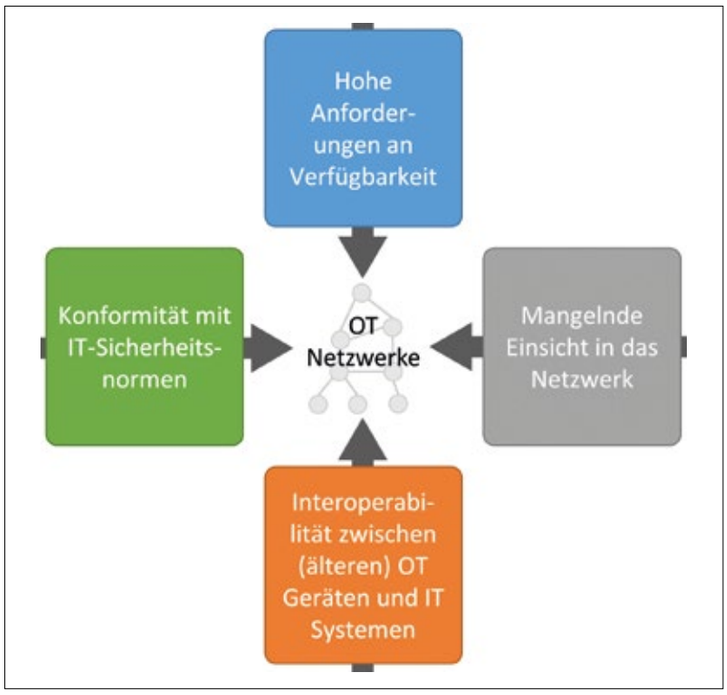
Notwendigkeit eines kontinuierlichen Betriebs

Der Ausfall eines OT-Netzwerks führt in der Regel dazu, dass auch wichtige Unternehmensprozesse ausfallen. Die Folgen können neben Produktionseinbußen auch weitere große materielle und immaterielle Schäden sein. Deshalb wird in unternehmenskritischen Netzwerken der Aspekt der Verfügbarkeit häufig über die Integrität und die Vertraulichkeit der Daten gestellt.

Netzwerkzugangskontrolle in der IT- und OT-Sicherheit

Wie können moderne Sicherheitsprinzipien kombiniert und genutzt werden, um die Netzwerksicherheit in unternehmenskritischen Installationen zu gewährleisten, ohne die Sicherheit oder Verfügbarkeit zu beeinträchtigen? Der Sicherheitsmechanismus der Netzwerkzugangskontrolle kann dabei eine tragende Rolle spielen, um die vier beschriebenen Problemfelder zu adressieren. Lösungen sollten sowohl ein vorgeschaltetes (pre connect) als auch ein nachgeschaltetes (post connect) Zulassungsverfahren ermöglichen. Bei Ersterem wird die Identität eines Geräts überprüft, bevor es eine Verbindung zum Netzwerk herstellen kann. Mit post-connect-Verfahren können Geräte aus dem Netzwerk entfernt oder dort isoliert werden, wenn festgestellt wird, dass sie nicht den erforderlichen Sicherheitsstandards entspechen oder sich nicht wie erwartet verhalten.

Damit wird die Netzwerkzugangskontrolle und die Konvergenz zwischen IT und OT zu einem Schlüsselelement für die Netzwerksicherheit.



Aktuelle Herausforderungen für OT-Netzwerke

Durch die Steuerung, welche Geräte unter welchen Umständen auf das Netzwerk zugreifen dürfen, wird die erfolgreiche Umsetzung jeder Netzwerksicherheitsstrategie vorangetrieben. Eine effektive Lösung für die Netzwerkzugangskontrolle kann die vier erörterten Hauptprobleme beheben.

Segmentierung industrieller Netzwerke

Ein weiteres wichtiges Sicherheitskonzept ist das Zonen- und Leitungsprinzip (zones and conduits). Es ist einer der zentralen Aspekte der weithin akzeptierten ISO/IEC 62443 Standards und schreibt die Segmentierung eines industriellen Netzwerks in getrennte Funktionsbereiche vor. Diese Sicherheitszonen isolieren verschiedene unabhängige Bereiche einer Anlage voneinander. Die Verbindungsleitungen zwischen diesen Zonen dienen sozusagen als Wächter, die darüber entscheiden, welcher Verkehr die Grenzen einer Zone überschreiten darf.

Um ein bestehendes hochverfügbares Netzwerk zu modernisieren oder ein unternehmenskritisches Netzwerk für die heutigen Sicherheitsanforderungen auszulegen, ist Netzwerkhardware erforderlich, die sowohl den Anforderungen der Zuverlässigkeit als auch der Sicherheit gerecht wird. Darüber hinaus müssen die Switches in moderne Lösungen für die Netzwerkzugangskontrolle integriert sein und sicherheitsrelevante Netzwerkinformationen erfassen, damit die Netzwerkkonnektivität entsprechend verwaltet werden kann.

Ein Lösungsansatz

Die heutigen Betreiber von OT-Netzwerken stehen vor zahlreichen Herausforderungen bei der Planung und Umsetzung einer umfassenden Netzwerksicherheitsstrategie in industriellen Umgebungen. Diese Herausforderungen stellen ein Risiko für industrielle Anlagen und Anwendungen dar, weil sie die Transparenz der Aktivitäten im gesamten Netzwerk beeinträchtigen und die Einhaltung verbindlicher Standards und Vorschriften gefährden.

Ein leistungsstarkes Orchestrierungssystem für die Netzwerkzugangs- und Netzwerkzugriffskontrolle erfüllt in Kombination mit industriegerechten Netzwerkgeräten für den Produktionsbereich diese Herausforderungen. Eine Integration von industrietauglichen Netzwerkgeräten und einer Netzwerkorchestrierungslösung für die Sicherheitsorchestrierung bringt State-of-the-Art Zugriffskontrolle bis tief in die industriellen Netzwerke. So können modernste Sicherheitskonzepte umgesetzt werden, während bewährte industrielle Funktionen wie höchste Zuverlässigkeit und Verfügbarkeit durch Einsatz von Redundanzprotokollen erhalten bleiben.

Die Umsetzung einer abgestimmten Netzwerk-Orchestrierung für Industrienetzwerke ist durch die Kooperation von ForeScout und Hirschmann entstanden, bei der die ForeScout-Plattform als übergreifende Orchestration Engine für den Netzwerkzugang dient und in Echtzeit eine Vielzahl von Variablen wie etwa die Geräteidentität sowie den Besitz/Benutzer, die Integrität und den Sicherheitsstatus eines Geräts bewertet. Entscheidungen über den Zugriff auf das Netzwerk werden in detaillierte Zugangs- und Autorisierungsregelwerke übersetzt, welche die Hirschmann Geräte im Produktionsbereich und an den Netzwerkeintrittspunkten durchsetzen. ■

Die Autoren

Tobias Heer,
Senior Architect CTO Office

Oliver Kleineberg,
Global CTO Industrial Networking, Hirschmann Automation and Control, Neckartenzlingen

Gilad Walden,
Vice President Technology Strategy, ForeScout, San José, CA, USA

Auch im Web:
www.chemanager.com
www.lvt-web.de

Top-Titel

für die Chemie-, Pharma- und Lebensmittelindustrie

CHEManager
Die führende Branchenzeitung für die Märkte der Chemie und Life Sciences

LVT LEBENSMITTEL Industrie
Die Zeitschrift für Fach- und Führungskräfte der Lebensmittel- und Getränkeindustrie

CITplus
Das Praxismagazin für Verfahrens- und Chemieingenieure

ReinRaumTechnik
Die führende Fachpublikation für Betreiber und Nutzer von Reinräumen

Ihre Ansprechpartner:

Redaktion

Michael Reubold
Leitung/Chefredakteur CHEManager
Tel.: +49 (0) 6201 606 745
michael.reubold@wiley.com

Ralf Kempf
stellv. Chefredakteur CHEManager
Tel.: +49 (0) 6201 606 755
ralf.kempf@wiley.com

Wolfgang Sieß
Chefredakteur CITplus
Tel.: +49 (0) 6201 606 768
wolfgang.siess@wiley.com

Jürgen Kreuzig
Chefredakteur LVT
Tel.: +49 (0) 6201 606 729
juergen.kreuzig@wiley.com

Roy Fox
Chefredakteur ReinRaumTechnik
Tel.: +49 (0) 6201 606 714
roy.fox@wiley.com

Mediaberatung

Roland Thomé
Tel.: +49 (0) 6201 606 757
roland.thome@wiley.com

Thorsten Kritzer
Tel.: +49 (0) 6201 606 730
thorsten.kritzer@wiley.com

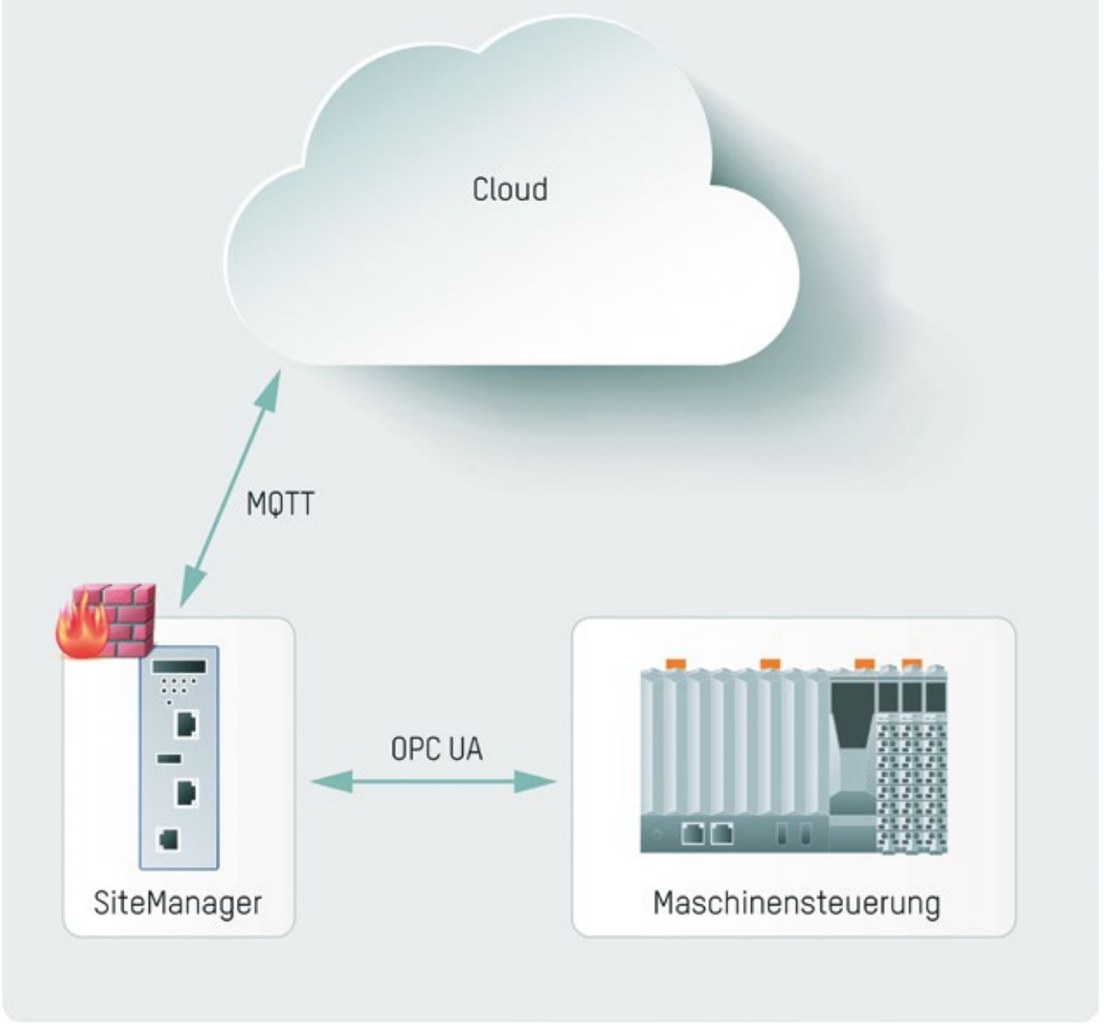
Marion Schulz
Tel.: +49 (0) 6201 606 565
marion.schulz@wiley.com

Corinna Matz
Tel.: +49 (0) 6201 606 735
corinna.matz@wiley.com

Jan Käppler
Tel.: +49 (0) 6201 606 522
jan.kaeppler@wiley.com

WILEY

Bei einer DDoS-Attacke verteilt ein Hacker seine Angriffsprogramme auf ein Botnetz und kann durch eine gezielte Attacke eine Maschinensteuerung lahmlegen ▶



Der Datentransfer von der Maschinensteuerung in eine Cloud erfordert eine Verbindung zum Internet. Dadurch steigt jedoch die Anfälligkeit für Cyberattacken. Steuerungen, die Daten in die Cloud schicken, müssen daher besonders geschützt werden.

SICHERE AUTOMATISIERUNG

Industrial IoT

Cybersecurity für Steuerungen

Bevor das Industrial Internet of Things (Industrial IoT) aufkam, kommunizierten Maschinensteuerungen – wenn überhaupt – untereinander oder mit übergeordneten Systemen im Firmennetzwerk. Eine direkte Verbindung mit dem Internet gab es nur in speziellen Fällen. Das Thema Cybersecurity spielte für Maschinenbauer und Maschinenbetreiber keine Rolle.

„Doch das ändert sich gerade", erklärt Andreas Hager, Produktmanager Control Systems bei B&R. Industrie-PCs und andere Geräte werden im Industrial IoT als Edge-Geräte eingesetzt und sind direkt mit dem Internet verbunden. Damit bieten Sie ein potenzielles Angriffsziel für Hacker.

Bei einer DDoS-Attacke verteilt ein Hacker seine Angriffsprogramme auf ein Botnetz und kann durch eine gezielte Attacke eine Maschinensteuerung lahmlegen.

DDos-Attacken

Hacker können zum Beispiel mit Überlastungsangriffen Steuerungen und damit ganze Maschinen lahmlegen. Bei solch einer DDoS-Attacke (Distributed-Denial-of-Service) verteilt ein Hacker seine Angriffsprogramme auf ein sogenanntes Botnetz aus mehreren hundert bis tausend Rechnern, Smartphones und Tablets, die letztendlich zum Angriffswerkzeug werden. Auf Kommando bombardieren die Bots eine Maschinensteuerung gleichzeitig mit so vielen Anfragen, dass sie unter der Last zusammenbricht und die Maschine stoppt – wie erst kürzlich ein Malware-Angriff auf einen Prozessorhersteller gezeigt hat.

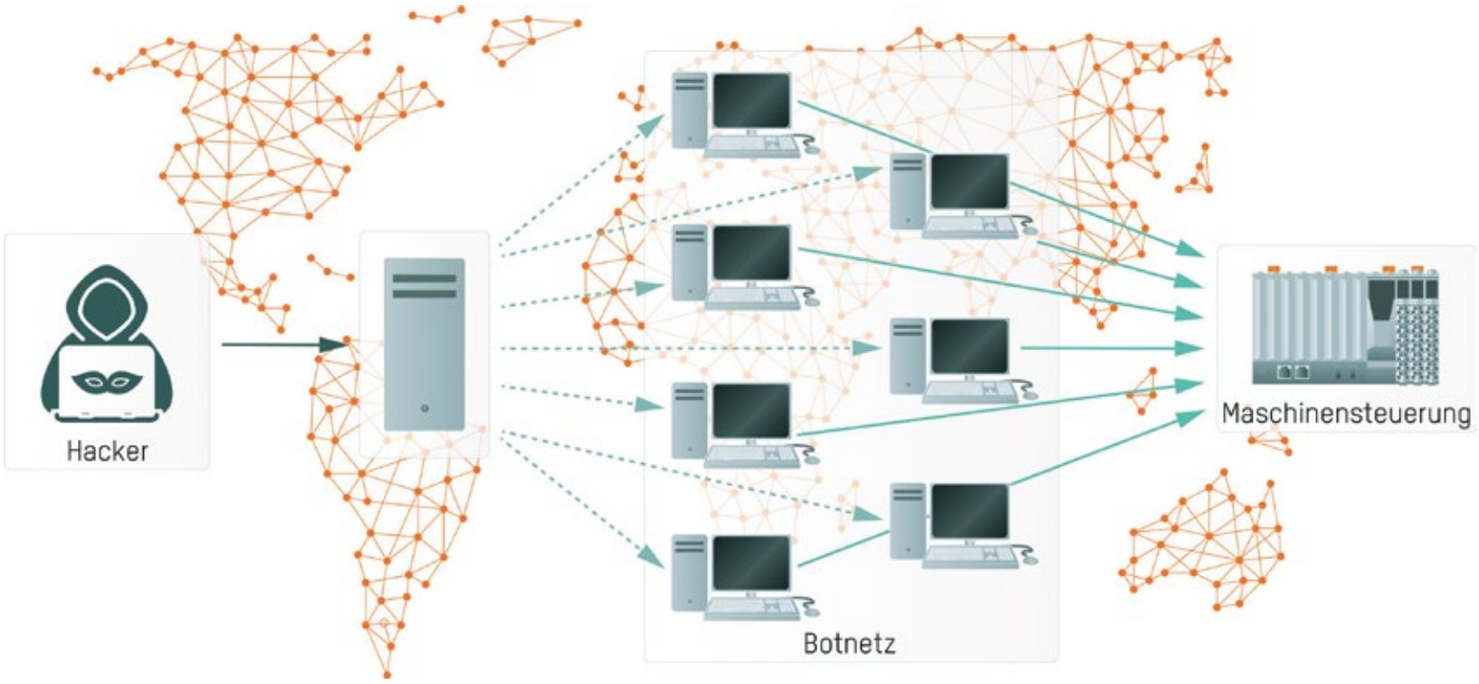
Offene Ports

Um Daten in die Cloud zu übertragen, müssen auf der Maschinensteuerung Ports geöffnet werden. „Während der Übertragungskanal zwischen Steuerung und Cloud-Gateway geöffnet ist, bieten diese Ports dann eine Möglichkeit für Hackerangriffe", erklärt Hager. Zudem ergeben sich weitere Probleme: Geräte, die direkt mit dem Internet verbunden sind, müssen mit

Der SiteManager ermöglicht eine sichere Übertragung von Daten in die Cloud

Edge Computing

Beim Edge Computing werden große Datenmengen möglichst nahe an der Datenquelle erfasst, komprimiert und aggregiert, um dann an übergeordnete Systeme weitergeschickt zu werden. Das dafür benötigte Bindeglied zwischen der echtzeitgetriebenen Maschinen- und Prozessebene (OT = Operational Technology) und der IT heißt Edge-Gerät. B&R bietet drei unterschiedliche Edge-Gerätetypen an, um alle Anwendungsfälle abzudecken: Edge Controller, Edge Embedded und Edge Connect.



Der B&R-Hypervisor ermöglicht, dass ein Industrie-PC gleichzeitig als Maschinensteuerung und als Embedded-SiteManager eingesetzt wird. Ein zusätzliches Hardwaregerät ist nicht nötig

Updates ständig aktuell gehalten werden, um neu entdeckte Sicherheitslücken zu schließen.

„Viele Maschinen laufen wochen- oder monatelang ohne Unterbrechung durch", gibt Hager zu bedenken. Ein Update lässt sich jedoch nur bei gestoppter Maschine einspielen. Zudem muss gegebenenfalls sogar die Applikation nach einem Update angepasst werden. „Das ist zu aufwendig und auf Dauer nicht praktikabel."

Die Lösung für dieses Dilemma ist einfach: Steuerungsfunktion und Kommunikationsfunktion müssen getrennt sein. Somit kann zum Beispiel eine DDoS-Attacke nicht mehr bis zur Maschinensteuerung durchdringen. „Im schlimmsten Fall wird nur die Kommunikation in die Cloud lahmgelegt, die Maschine kann trotzdem weiterlaufen", bekräftigt Hager.

B&R hat für diesen Zweck den SiteManager im Portfolio. Dieses Gerät hat eine integrierte Firewall und übernimmt alle Aufgaben, die für die Cybersecurity gefordert sind: zum Beispiel Cloud-Zertifikate auf dem neuesten Stand halten und Patches anwenden, um Sicherheitslücken zu schließen.

Cloud-Connectivity

Um Daten in die Cloud zu übertragen, wird die Steuerung via OPC UA mit dem SiteManager verbunden. Der Anwender definiert bei der Konfiguration, welche Daten übertragen werden sollen. Es ist auch möglich, unterschiedliche Daten an unterschiedliche Cloudanbieter zu übertragen. Die Konfiguration erfolgt durch Setzen von Häkchen in der Weboberfläche des SiteManagers.

Benötigt ein Cloud-Zertifikat ein Update, muss der Maschinenbetreiber nichts tun. Der SiteManager lädt Updates automatisch herunter und installiert diese – ohne die Maschinenfunktion zu beeinträchtigen. Somit wird gewährleistet, dass die Sicherheitsrichtlinien der Cloudanbieter stets eingehalten und potenzielle Sicherheitslücken schnell geschlossen werden.

Sicherer Fernwartung

„Bei der Fernwartung ergeben sich ganz ähnliche Sicherheitsanforderungen, wie bei der Übertragung von Daten in die Cloud", erklärt Hager. Daher bietet sich auch für diese Anwendung der SiteManager an.

Das Gerät ermöglicht, dass sich ein Service-Techniker des Maschinenbauers über eine sichere VPN-Verbindung mit der Maschinensteuerung verbindet und auf Fehlersuche gehen kann. Ein Benutzerverwaltungssystem regelt eindeutig und manipulationssicher, welcher Techniker auf welche Steuerungen zugreifen darf. „Mit dem Techniker vor Ort kann dann gezielt ein Problemlösungsprozess gestartet werden", sagt Hager. Der SiteManager sorgt dafür, dass jeglicher Datentransfer zwischen der Maschine und unterschiedlichen Applikationen außerhalb des Firmennetzwerkes vor unberechtigten Zugriffen wie Cyber-Attacken geschützt ist. ■

Der B&R SiteManager

Der B&R-SiteManager steht in unterschiedlichen Varianten zur Verfügung. Je nach Version lässt sich das Gerät via LAN, WLAN oder Mobilfunk an das Internet anbinden. Alle drei Varianten verfügen über eine integrierte Firewall. Um Sicherheitskonflikte mit werksseitigen Firewalls zu vermeiden, läuft die Kommunikation in das Internet über firewallverträgliche, verschlüsselte Web-Protokolle.

Der SiteManager von B&R steht in unterschiedlichen Varianten zur Verfügung. Er lässt sich wahlweise via LAN, WLAN oder Mobilfunk anbinden

Neben den Hardwarevarianten des SiteManagers steht auch eine Software-Version zur Verfügung. So lassen sich Maschinensteuerung und SiteManager in einem Gerät vereinen. Dazu werden mithilfe des B&R-Hypervisors auf einem Industrie-PC zwei Betriebssysteme installiert: Das Echtzeitbetriebssystem für die Maschinensteuerung und ein Linux-oder Windows-System für den SiteManager. Diese Betriebssysteme sind vollständig unabhängig voneinander. Selbst wenn der SiteManager durch einen Angriff blockiert wird oder das allgemeine Betriebssystem abstürzt, ist die Maschinensteuerung davon nicht betroffen.

Autorin
Carmen Klingler-Deiseroth,
freie Fachjournalistin

Industrielle Security Router von Phoenix Contact schützen Schiffsnetzwerke vor Cyber-Angriffen

Cyber-Attacken auf die Schiffs-IT

So übernimmt der Versicherer das Risiko

Auch auf Schiffen steigt die Anzahl an Vorfällen im Bereich Cyber Security. Die klassischen Kaskoversicherungen für Schiffe decken derartige Angriffe jedoch in der Regel nicht ab. Deshalb haben die Lampe & Schwartze Gruppe und Phoenix Contact eine Lösung auf Basis der Security-Router FL mGuard entwickelt, die sich für alle Beteiligten als vorteilhaft erweist.

Ist die Schiffs-IT durch eine Cyber-Attacke beeinflusst, sind daraus resultierende Schäden am Schiff sowie die Kosten einer Havarie von der Versicherungsdeckung über die „Clause 380" ausgeschlossen. Mit dem Ship Owner´s Marine Cyber Cover (SOMCC) bietet Lampe & Schwartze Marine Underwriting (L&S Gruppe) den Reedereien nun eine Alternative, die das Cyber-Risiko für Schiffe im Rahmen des Wiedereinschlusses des Cyber-Risikos übernimmt. Das Portfolio der Gruppe umfasst darüber hinaus Module für die Landseite, die unter anderem die Loss-of-Hire, also den Verdienst- und damit verbundenen Frachtausfall, sowie den Verlust von Banking-Geldern einschließen. Neben dem reinen Versicherungsschutz stellt das SOMCC über den Verein Hanseatischer Transportversicherer (VHT) und den IT-Schadensdienstleister Maritime Cyber Emergency Response Team (MCERT) außerdem umfangreiche Dienstleistungen zur Verfügung. MCERT bindet die Security Router der Produktfamilie FL mGuard in sein für die Reedereien abrufbaren Frühwarnsysteme ein und verkürzt damit die Alert Response Time erheblich.

Auf Schiffen wird eine zunehmende Anzahl von Maschinen und Anlagen via Ethernet miteinander vernetzt. Ohne entsprechende Schutzmaßnahmen breiten sich Störungen oder Ausfälle daher sehr schnell über das Schiffsnetzwerk aus. Auslöser für die Beeinträchtigungen können sowohl Cyber-Angriffe als auch die Unwissenheit der eigenen Mitarbeiter sein. Um Schäden auf den Schiffen, Stillstandzeiten und hohe Kosten zu vermeiden, fordern Banken, Versicherungen und Kunden immer häufiger eine adäquate Absicherung der Schiffe vor solchen Szenarien.

Meist Ausschlussklausel für Cyber-Angriffe

Die Herausforderungen, die sich aus der Cyber Security ergeben, sind vielschichtig. Für die Reeder kommt folgenden Gefahren eine besondere Bedeutung zu: Zum einen fürchten sie den Kontrollverlust des auf See befindlichen Schiffs. Auf der anderen Seite möchten sie Unterbrechungen der Betriebskontinuität an der Hafenmauer verhindern. Das Be- und Entladen der Schiffe soll nicht gestört werden. Doch viele Reeder bedenken dabei nicht, dass die Mehrheit der Kaskoversicherungen für Schiffe eine Ausschlussklausel für Cyber-Angriffe beinhalten (CL380 10/03). Unter Punkt 1.1 ist dort folgendes zu lesen: „Vorbehaltlich der nachstehenden Ziffer 1.2 deckt diese Versicherung in keinem Fall die Haftung oder die Kosten für Schäden, die direkt durch die Verwendung oder den Betrieb von Computern, Computersystemen, Computersoftwareprogrammen, bösartigem Code, Computerviren oder -prozessen oder elektronischen Systemen verursacht oder dazu beigetragen haben oder sich daraus ergeben".

Es sind bereits zahlreiche einschneidende Szenarien von gehackten Steuer- und Navigationssystemen untersucht worden. Die internationale Seeschifffahrts-Organisation IMO hat Leitlinien für den Aufbau eines IT-Sicherheitsstandards herausgegeben. Als erheblich zeigte sich beispielsweise der Security-Vorfall bei der Maersk Shipping Company. Hier war das komplette IT-System des Unternehmens betroffen. Folglich konnten die Schiffe weder be- noch entladen werden. Zur Verkürzung der Betriebsunterbrechungszeiten tauschte Maersk die meisten seiner Server und Router aus. In Summe entstand ein Schaden von mehreren hundert Millionen US-Dollar, der im wesent-

Eigenes Kompetenzzentrum für Cyber-Sicherheit

Als einer der weltweiten Marktführer und Innovationsträger in der Elektrotechnik, Elektronik und Automatisierung betreibt Phoenix Contact unter anderem ein eigenes Kompetenzzentrum für Cyber Security am Standort Berlin. Auf Basis des langjährigen Know-hows in diesem Umfeld stellt das Unternehmen individuelle Produkte und Netzwerklösungen zur Verfügung, die die besonderen industriellen Anforderungen umsetzen. Kern des Security-Produktspektrums sind die Security-Router der Produktfamilie FL mGuard.

lichen versicherbar gewesen wäre. Über Schäden an der Schiffs-IT wurde nichts bekannt. Für den Reeder ist es somit wichtig zu wissen, dass das Ship-IT- und das Onshore-IT-System als ein einziges IT-System mit allen spezifischen Belangen betrachtet und versichert werden muss.

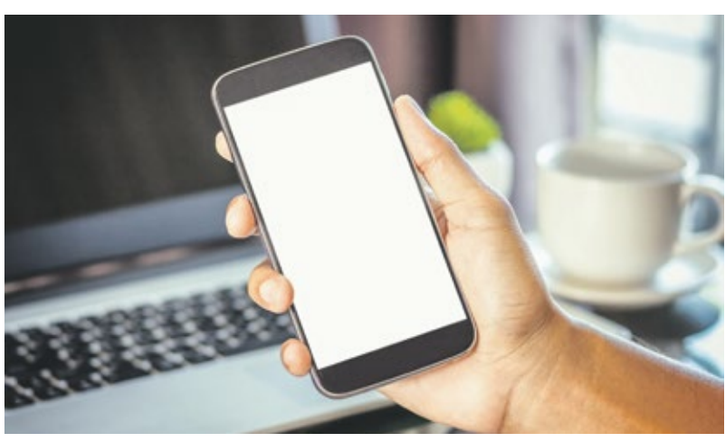
Schnelle Ausbreitung im gesamten Netzwerk

Welche Gefahren können nun auftreten? Die von den privaten Laptops der Besatzungsmitglieder ausgehenden Störungen übertragen sich zum Beispiel direkt in das Schiffsnetzwerk. Handelt es sich um große, flache Netzwerkstrukturen, breiten sich die Störungen dann schnell im gesamten Netzwerk aus. Oder ein Mitarbeiter führt aus der Ferne versehentlich Änderungen am falschen System durch. Denkbar ist ebenfalls, dass Kriminelle Daten über eine ungeschützte Internet-basierte Satellitenverbindung kopieren oder auf diese Weise Einstellungen am Schiffssystem verändern. Ferner könnte Schadsoftware über infizierte Hardware – wie USB-Sticks oder Laptops – in das Netzwerk gelangen. Gleiches gilt für infizierte Smartphones oder Smart Devices, die sich über die WLAN-Schnittstellen des Schiffs mit dem Netz verbinden. An Bord werden zudem in der Regel identische oder nur leicht modifizierte Passwörter vergeben. Verlassen die Schiffsbesatzungen das Schiff dauerhaft, findet keine Änderung der Passwörter oder Zugriffsrechte statt. Im Laufe der Zeit wird ein Cyber-Security-Vorfall so immer wahrscheinlicher, was zu großen Schäden führen kann. Denn ungeplante Stillstandzeiten, eine Wiederherstellung des Systems, die Bezahlung externer Spezialisten, der entgangene Umsatz sowie der Imageverlust des Reeders ziehen hohe Kosten nach sich.

Einfache Nachrüstung in bestehenden Netzen

Was kann der Reeder also tun? Die Wahrscheinlichkeit und Auswirkungen von Cyber-Security-Vorfällen sollten grundsätzlich reduziert werden. Als Beispiel seien folgende Maßnahmen genannt, die Abhilfe schaffen:

- unbefugten Personen keinen Zugang gewähren
- sensible Bereiche stets abschließen
- große Schiffsnetzwerke in kleinere Einheiten aufteilen
- ungenutzte Schnittstellen deaktivieren oder blockieren
- Lese- und Schreibrechte einschränken
- Fernzugriffe mit Hilfe eines Schlüsselschalters kontrollieren
- wichtige Informationen und die externe Kommunikation verschlüsseln
- Notfallpläne für Cyber Security ebenso leben und trainieren wie Brandschutzübungen.



Schadsoftware kann über infizierte Smartphones oder Smart Devices, die sich über die WLAN-Schnittstellen des Schiffs mit dem Netzwerk verbinden, in dieses gelangen

Im ersten Schritt kann ein industrieller Security-Router mit maritimer Schiffszulassung bei der Absicherung des Schiffs unterstützen. Phoenix Contact bietet entsprechende Geräte für den maritimen Bereich an, die derzeit über Zulassungen von DNV GL, LR, ABS und BV verfügen. Die industrietauglichen, lüfterlos konzipierten Security-Router FL mGuard überzeugen durch zuverlässige Sicherheit und Leistung in einem kompakten, hutschienenmontablen Metallgehäuse. Neben dem zugriffssicheren Aufbau von VPN-Tunneln (Virtual Private Network) umfassen die Geräte verschiedene industriespezifische Firewall-Funktionen. Dazu gehört eine User Firewall, eine Conditional Firewall zur Aktivierung definierter Firewall-Regeln sowie Deep Packet Inspection für die Durchleuchtung jedes via OPC Classic oder Modbus/TCP übertragenen Datenpakets. Auf diese Weise lässt sich das auf den internationalen Standards ISA-99 und IEC 62443 basierende Defense-in-Depth-Konzept fachgerecht in den Anwendungen realisieren.

Durch den sogenannten Stealth-Mode sind die Security-Router FL mGuard im Netzwerk nicht sichtbar, was die Sicherheit grundsätzlich erhöht. Der größte Vorteil ergibt sich allerdings beim Nachrüsten bestehender Schiffsnetzwerke. Werden die Geräte dort eingebaut, müssen die IP-Adressen der anderen Netzwerkkomponenten nicht angepasst werden. Der Installations- und Dokumentationsaufwand erweist sich somit als einfach und gering.

Online-Überwachung der verbauten Steuerungen

Haben die Reedereien die Security-Router von Phoenix Contact korrekt auf ihren Schiffen montiert, ist der für den Versicherungsmakler NW Assekuranz mindestens notwendige Schutz vor unbefugten Zugriffen gegeben. Die Produktfamilie FL mGuard erweitert die Ship-IT folglich systematisch und macht die Schiffe versicherbar respektive die Versicherungslösung erschwinglicher. Die Geräte passen dabei exakt in die SOMCC-Philosophie. Ein wesentlicher Teil der Versicherungslösung beruht auf der Online-Überwachung der auf dem Schiff verbauten Steuerungen. Über das vom L&S-Dienstleister MCERT durchgeführte Monitoring werden die IT-Systeme in ein Frühwarnsystem eingebunden, das jedes Schiff individuell vor systemspezifischen oder regionalen Angriffen warnen kann. Kommt es trotzdem zu einem „Breach", koordiniert MCERT die Beauftragung der lokalen Security-Spezialisten von Phoenix Contact zur Schadensregulierung. Die Kosten eines versicherten Schadens übernimmt die Versicherung.

Umfassendes Programm an Leistungen und Lösungen

Der fehlende Schutz vor Cyber-Attacken stellt für die Versicherungen ein schweres Risiko dar. Deshalb ist eine Cyber-Angriffs-Ausschlussklausel (CL380 10/03) in die Verträge aufgenommen worden, die für viele Reeder erhebliche finanzielle Risiken birgt. Eine stetig steigende Zahl von Schiffen sieht sich mit Cyber-Angriffen konfrontiert. Als Lösung bietet sich das Cyber-Paket von Phoenix Contact und der Lampe & Schwartze Gruppe an. Durch die Installation der Security-Router FL mGuard zeigt sich das Versicherungsrisiko als überschau- und für L&S versicherbarer. Die Lampe & Schwartze Gruppe stellt den Reedereien über ihre assoziierten Marine Broker hier ein umfassendes Programm an Beratungsleistungen und Versicherungslösungen zur Verfügung. ■

it-sa, Halle 9, Stand 610

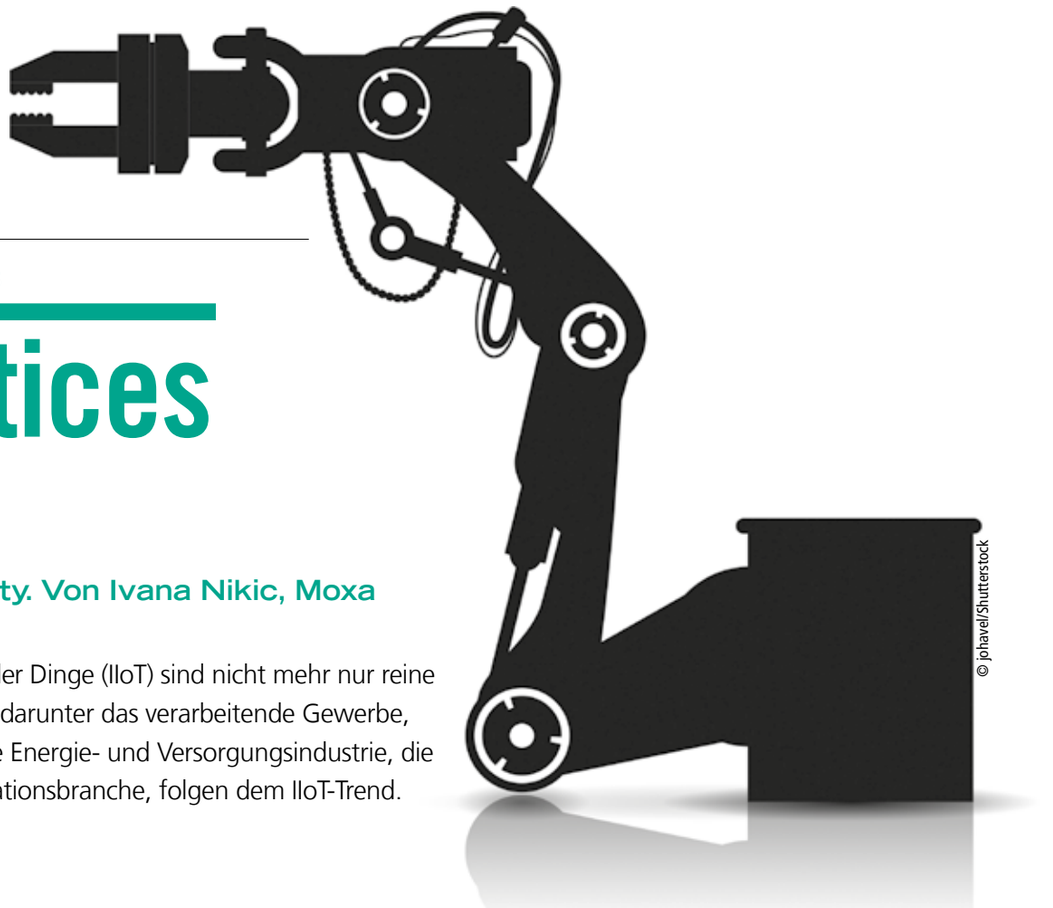
Die Autoren

Gerrit Boysen,
Manager Product Marketing Security, Phoenix Contact Electronics GmbH, Bad Pyrmont

Achim Fischer-Erdsiek,
Managing Partner,
Lampe & Schwartze-Gruppe, Bremen

Kontakt

Phoenix Contact GmbH & Co. KG
Blomberg
Tel.: +49 5235 3 12000
info@phoenixcontact.de
www.phoenixcontact.de/security
www.nw-assekuranz.de


© johavel/Shutterstock

INDUSTRIAL INTERNET OF THINGS

Best Practices fürs IIoT

Industrial Network Cybersecurity. Von Ivana Nikic, Moxa

Industrie 4.0 oder das industrielle Internet der Dinge (IIoT) sind nicht mehr nur reine Schlagworte. Viele verschiedene Branchen, darunter das verarbeitende Gewerbe, der Consumer- und Einzelhandelssektor, die Energie- und Versorgungsindustrie, die Automobilindustrie und die Telekommunikationsbranche, folgen dem IIoT-Trend.

Insbesondere Hersteller nehmen das IIoT schneller an als viele andere Branchen. Das zeigt, welche enormen Auswirkungen das IIoT und die Realisierung von Industrie 4.0 auf das verarbeitende Gewerbe haben können.

Cybersicherheit ist für Manager jedoch nach wie vor ein wichtiges Anliegen, bevor sie IIoT- oder Industrie 4.0-Systeme bereitstellen können. Einer der Hauptgründe dafür ist, dass die Cybersicherheit für traditionelle Systeme der Betriebstechnologie (OT) nicht immer die höchste Priorität hat.

Wenn OT-Systeme mit dem Internet oder mit anderen IT-Systemen verbunden sind, wird das OT-System zu einer Schwachstelle für böswillige Angriffe oder versehentlichen Datenverlust.

Warum wird die Cybersicherheit von OT-Ingenieuren so oft übersehen? Die Antwort kann auf vier verbreitete Mythen zurückgeführt werden.

Vier verbreitete Mythen über die industrielle Cybersicherheit

Mythos 1: Mein industrielles Netzwerk ist physisch isoliert und nicht mit dem Internet verbunden, daher ist mein Netzwerk sicher.

Jedoch: Heutzutage sind viele IIoT-Geräte bereits direkt mit dem Internet verbunden und umgehen traditionelle IT-Sicherheits-Schichten.

Mythos 2: Hacker verstehen ICS-, SPS- und SCADA-Systeme nicht, daher ist mein Netzwerk sicher.

Jedoch: Seit 2010 gab es tatsächlich mehrere ausgeklügelte Cyberangriffe, die auf ICS-Netzwerke abzielten, wie Stuxnet (Ziel: SPSen) und Industroyer (Ziel: Leitungsschutzschalter). Trend: Angriffe auf Industriesektoren werden in Zukunft wahrscheinlich zunehmen.

Mythos 3: Mein Netzwerk ist zu klein, um als Ziel ausgewählt zu werden, daher ist mein Netzwerk sicher.

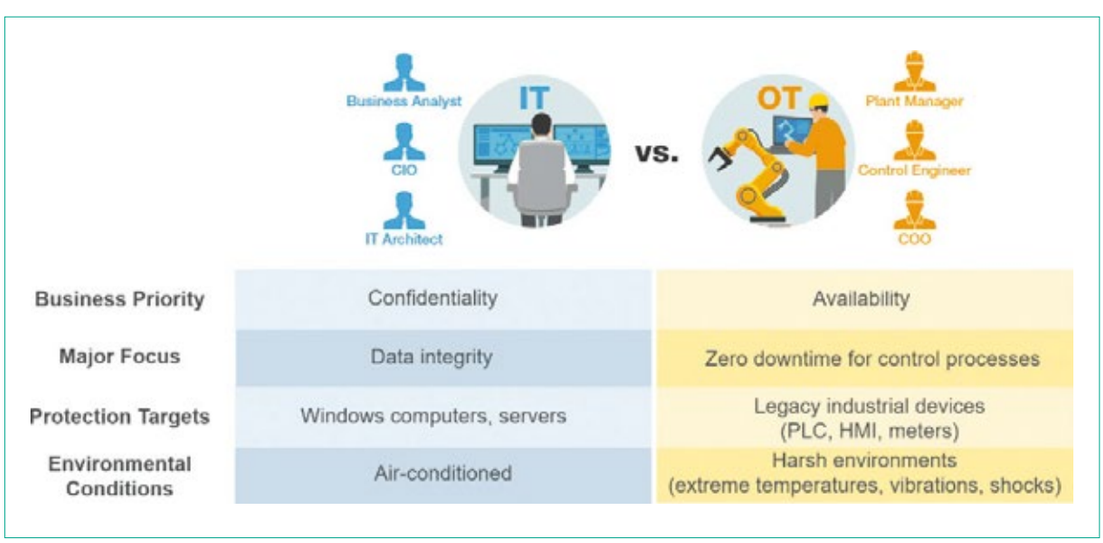
Jedoch: Oft ist unbeabsichtigte Verletzung auf menschliches Versagen oder auf eine Fehlfunktion eines Geräts zurückzuführen, die für die Größe Ihres Unternehmens nicht relevant ist.

Mythos 4: Ich habe bereits eine Firewall zum Schutz meines industriellen Netzwerks, sodass mein Netzwerk sicher ist.

Jedoch: Firewalls sind möglicherweise eine erste Schutzstufe, sie sind jedoch nicht zu 100 % wirksam. Darüber hinaus sind die meisten Firewalls nicht für Industrieprotokolle (z. B. Modbus TCP, EtherNet/IP und Profinet) ausgelegt.

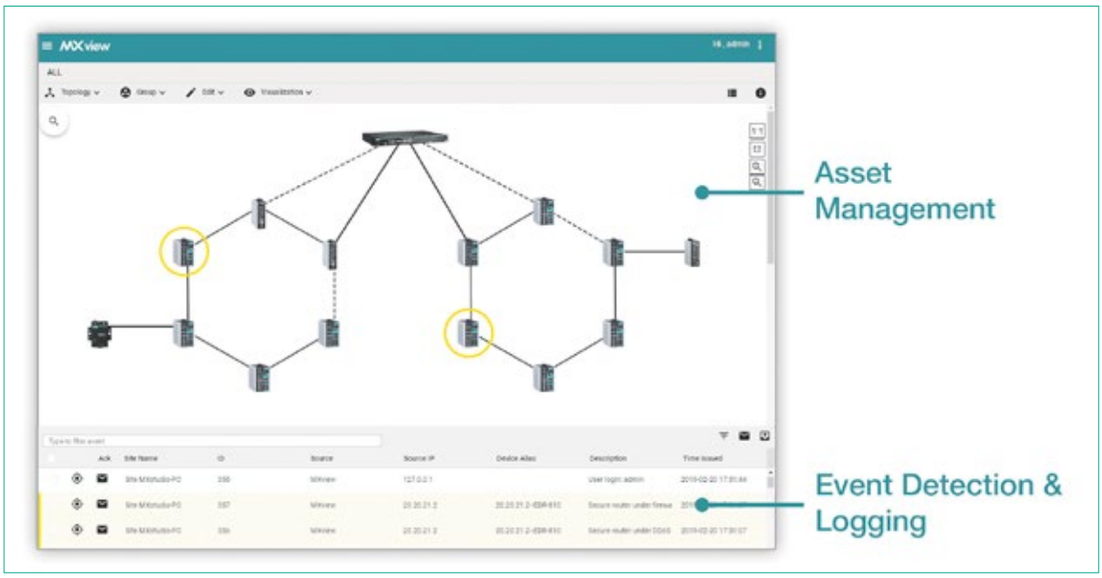
Unterschiede zwischen industriellen Netzwerken und IT-Netzwerken

Industrielle Netzwerke und IT-Netzwerke haben unterschiedliche Prioritäten für das Unternehmen und den Betrieb, unterschiedliche Schwerpunktbereiche, Sicherheitsziele und sogar Umgebungsbedingungen. Unterschiedliche Prioritäten werden



IT- und OT-Netzwerke: Die Verantwortlichen und ihre Prioritäten

auch von verschiedenen Managern innerhalb derselben Organisation festgelegt. Auf der IT-Seite sind Business-Analysten, CIOs und IT-Architekten die Hauptentscheidungsträger, die das IT-Netzwerk und die Cybersicherheit planen und verwalten. Aus ihrer Sicht hat die Vertraulichkeit oberste Priorität. Auf der OT-Seite sind Werksleiter, COOs und Steuerungsingenieure die Hauptentscheidungsträger. Aus ihrer Sicht ist die Produktions- oder Systemverfügbarkeit das Hauptanliegen. Daher ist es für eine erfolgreiche IT-OT-Integration wichtig, die unterschiedlichen Geschäftsprioritäten und -anforderungen von IT- und industriellen Steuerungssystemen zu kennen.



MXview von Moxa sorgt für ein Plus an Cybersecurity: Industrielle Netzwerkmanagementsoftware, entwickelt für konvergente Automationsnetze

Best Practices zur Verbesserung Ihrer industriellen Netzwerksicherheit

Trotz der großen Unterschiede in den Prioritäten und Techniken zum Schutz industrieller Steuerungssysteme im Vergleich zu Unternehmens-IT-Systemen haben mehrere Industrieverbände Standards und Sicherheitsrichtlinien für die Verbindung oder Konvergenz von ICS mit IT-Systemen entwickelt. Insbesondere konzentrieren sich das Industrial Internet Consortium (IIC), das National Institute of Standards and Technology (NIST) und die International Electrotechnical Commission (IEC) auf drei Hauptbereiche zur Verbesserung der Cybersicherheit von IKS. Diese drei Säulen zur Sicherung industrieller Netzwerke umfassen:

- Umfassenden Schutz für industrielle Netzwerke bereitstellen
- Sicherheitseinstellungen in den industriellen Netzwerken aktivieren
- Die Sicherheit durch Schulung, Richtlinien und Überwachung verwalten

Basierend auf diesen drei Säulen empfehlen wir die folgenden Best Practices als ersten Schritt, um Ihre ICS-Cybersicherheit abzusichern.

Best Practice I:
Sichere Netzwerkinfrastruktur

- Segmentieren Sie Ihr ICS in mehrere Subsysteme und definieren Sie die Datenkommunikationsanforderungen zwischen den Subsystemen
- Installieren Sie industrielle Firewalls zwischen den einzelnen Segmenten und konfigurieren Sie die Datenkommunikationsrichtlinie ordnungsgemäß
- Installieren Sie ein Intrusion Prevention System (IPS) oder Intrusion Detection System (IDS), um böswillige Aktivitäten in Ihrem industriellen Netzwerk zu überwachen
- Richten Sie VPN-Verbindungen für den Fernüberwachungs- oder Fernwartungszugriff ein

Best Practice II:
Gehärtete Gerätesicherheit

- Vergewissern Sie sich, dass Sie keine Standardkennwörter für Ihre Geräte verwenden
- Wählen Sie ein sicheres Passwort mit mindestens acht Zeichen, das schwer zu erraten ist*
- Aktivieren Sie die Zugriffsperrfunktionen
- Zugriffssteuerungslisten aktivieren: Mit dieser Funktion können Geräte-IP- oder MAC-Adressen auf dem industriellen Netzwerkgerät vorregistriert werden, und nur Geräte, die den Zugriffssteuerungsregeln entsprechen, können das Netzwerk verwenden
- Verwenden Sie eine VPN- oder HTTPS-Sitzung, um die Kommunikation für den dezentralen Remote-) Zugriff auf industrielle Geräte über eine Webkonsole zu verschlüsseln
- Erkundigen Sie sich bei Ihrem Gerätehersteller, wie Sie innerhalb kürzester Zeit nach Verfügbarkeit Geräte-Sicherheitspatches und -updates erhalten

* Weitere Informationen finden Sie unter: NIST Special Publication 800-63-3B: https://pages.nist.gov/800-63-3/sp800-63b.html#reqauthtype

Best Practice III:
Sicherheitsmanagement und -schulung

- Entwickeln Sie Sicherheitsrichtlinien für die Bediener, die das System entwerfen, betreiben und warten.
- Schulen Sie Systemingenieure und bilden Sie sie weiter, damit sie die Bedeutung der Cybersicherheit verstehen und sich mit neuen Richtlinien vertraut machen können
- Entwickeln Sie Sicherheitsrichtlinien für Netzwerk-Endpunkte, Geräte und Netzwerkgeräte
- Investieren Sie in Sicherheitsüberwachungstools, um Sicherheitseinstellungen auf Ihren Geräten und Netzwerkgeräten zu überwachen und zu sichern
- Sichern Sie Ereignisprotokolle für industrielle Steuerungssysteme und industrielle Netzwerkgeräte und zeichnen Sie diese auf
- Verwenden Sie ein ICS, das die Integration in vorhandene IT-SIEM-Systeme unterstützt (z. B. Systeme, die RESTful APIs oder SNMP unterstützen)

Fazit: Industrial Cybersecurity ist jedermanns Aufgabe!

Letztendlich hängt die erfolgreiche Einführung von IIoT- oder Industrie 4.0-Systemen von einer effektiven Cybersicherheit für industrielle Steuerungssysteme ab, die sich nahtlos in die neuesten Unternehmensnetzwerke integrieren lassen. Es ist jedoch nur der erste Schritt, anzuerkennen, dass OT-Netzwerke und industrielle Geräte nicht mehr gegen Cyberangriffe immun sind. Hersteller müssen auch die unterschiedlichen Prioritäten ihrer IT- und OT-Abteilungen kennen und abwägen, um die organisatorischen Silos effektiv aufzulösen und Best Practices zur Stärkung der industriellen Netzwerksicherheit zu implementieren: Bereitstellung eines umfassenden Schutzes, Ermöglichung von Sicherheitseinstellungen in industriellen Netzwerken und Verwalten von Sicherheitsrichtlinien durch Aufklärung und Überwachung. Wie aus diesen Richtlinien hervorgeht, liegt die Verantwortung für die Gewährleistung der Cybersicherheit für industrielle Netzwerke bei mehr als einer Person in Ihrer Organisation. Letztendlich spielt jeder in Ihrem Unternehmen eine entscheidende Rolle, wenn es um die industrielle Cybersicherheit und die erfolgreiche Umstellung älterer OT-Systeme auf Industrie 4.0 in einer Zukunft geht, in der alles mit dem Internet verbunden ist.

Autorin:

Ivana Nikic

Kontakt

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

Mehr zum Thema auf dem OnePager
www.iiot-cybersec.com

KRITIS

Darf einfach nicht vorkommen!

Früherkennung von IT-Angriffen im Energiesektor

© snapfoto105 – Fotolia.com

Der Energiesektor zählt zu den kritischen Infrastrukturen – entsprechend muss deren IT besonders gut abgesichert sein. Der Ausfall eines Großkraftwerks zöge enorme Kosten und teure Folgeschäden nach sich. Im Forschungsprojekt Indi wurde vor diesem Hintergrund ein Intrusion Detection System (IDS) entwickelt: Mittels maschinellem Lernen kann es Hinweise auf Angriffe und Störungen zuverlässig erkennen. Christoph Moder, Forscher und Microkernel-Entwickler bei Genua, stellt es uns vor.

Bei Industriesteuerungen (ICS, Industrial Control System) handelt es sich um spezialisierte Rechner für eng begrenze Aufgaben, die sie jedoch mit sehr hoher Zuverlässigkeit erfüllen müssen. Da sie in einem vom Internet abgetrennten Netz ohne Nutzerinteraktion betrieben werden, treten viele Probleme der Büro-IT dort nicht auf. Dafür sind die möglichen Schäden umso höher: Der Ausfall eines Großkraftwerks kostet schnell enorme Summen, und dazu können noch teure Folgeschäden in der Außenwelt kommen. So etwas darf einfach nicht vorkommen. Zwar ist bei kritischer Infrastruktur eine solide Grundsicherung der IT vorgeschrieben. Trotzdem können Fehlfunktionen vorkommen und müssen schnell erkannt werden. Klassische IDS-Lösungen sind jedoch wegen der teils proprietären Protokolle im Bereich Industriesteuerungen wenig geeignet.

Indi setzt auf maschinelles Lernen

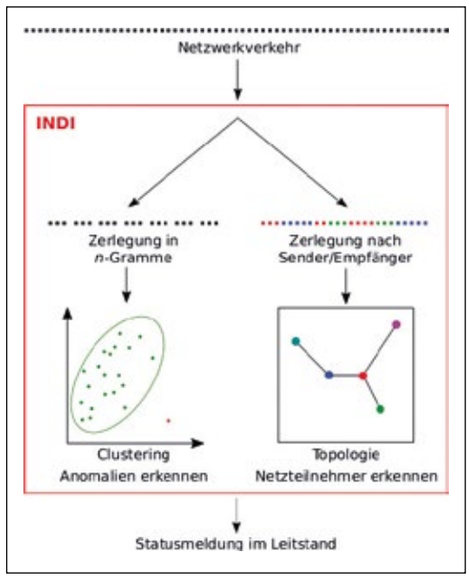
An diesem Punkt setzt das Forschungsprojekt Intelligente Intrusion Detection-Systeme für Industrienetze (INDI) an. Der Kerngedanke ist, maschinelles Lernen einzusetzen, um Normalbetrieb und Störungen unterscheiden zu können, denn die Wiederholung ähnlicher Datensequenzen ist eine typische Eigenschaft von Industriesteuerungen. Dabei wird der Netzwerkverkehr rein passiv mitgelesen und im Demonstrator an drei Analyse-Module weitergeleitet:

- Protokollspezifische Anomalie-Erkennung: Die eingehenden Datenpakete werden zerlegt und samt ihrer Metadaten (z.B. Sender, Empfänger, Protokolltyp) mittels eines Klassifizierungsalgorithmus analysiert, der die Unterscheidung zwischen Normalzustand und Anomalie durchführt.
- Protokollunabhängige Anomalie-Erkennung: Diese ist vor allem dann interessant, wenn undo-

Das Indi-Projektteam von der TU Braunschweig, BTU Cottbus-Senftenberg, der Leag und Genua GmbH

kumentierte Protokolle zum Einsatz kommen. Sie betrachtet den rohen TCP-Datenstrom und zerlegt ihn in kurze Datensequenzen, mit denen dann ebenfalls eine Klassifizierung in Normalzustand und Anomalie mittels eines Clustering-Algorithmus durchgeführt wird.

- Topologie-Erkennung: Aus dem Netzwerkverkehr werden die Kommunikationspartner extrahiert und daraus eine Baumstruktur aufgebaut. So kann man sehen, welche aktiven Geräte im Netzwerk vorhanden sind, wer mit wem auf welche Weise kommuniziert und – im Falle einer Anomalie – deren Verursacher. So erhält man eine grafische Visualisierung des Netzwerkzustands und gleichzeitig eine Bestandsaufnahme, die man mit dem Netzplan vergleichen kann.



Anomalie-Erkennung im Netzwerk-Verkehr

Separationstechnologie

Diese Verfahren laufen auf einer gemeinsamen Hardware-Plattform, auf der ein Microkernel als Separationsschicht dient. Dieses isoliert die Analyse-Software von direktem Hardwarezugriff und stellt so die Rückwirkungsfreiheit auf das Anlagennetz sicher. Die kleine Codebasis und die klar definierten Schnittstellen eines Microkernels minimieren die Angriffsfläche. Dieselbe Technolgie kommt bei Produkten des IT-Sicherheitsherstellers Genua zum Einsatz, die die hohen Anforderungen im staatlichen Geheimschutzbereich erfüllen.

Universitäten und Unternehmen arbeiten zusammen

In dem Projekt haben mehrere Partner zusammengearbeitet: die TU Braunschweig, die BTU Cottbus-Senftenberg, der Energieversorger Leag sowie der IT-Sicherheitshersteller Genua. Gefördert wurde das Projekt vom Bundesministerium für Bildung und Forschung.

Bei Genua sind die Erfahrungen mit dem Indi-Projekt bereits in die Entwicklung des Industrial Gateways GS.Gate eingeflossen, das eine hochsichere Anbindung von Maschinenanlagen an die Außenwelt bietet und die Integration kundenspezifischer Software-Lösungen ermöglicht. ■

Weitere Informationen zum Projekt Indi:
http://indi-project.org/

Autor

Christoph Moder,
Forscher und Microkernel-Entwickler bei Genua

Kontakt

Genua GmbH,
Kirchheim bei München
Tel.: +49 89 991 950 0
www.genua.de

INTERVIEW

Digitales Neugeschäft

Sicherheit für die digitale Transformation: Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit

„Informationssicherheit in digitalen Produkten und Dienstleistungen erfordert den Einsatz von Kryptografie und zunehmend auch physischer Sicherheit in den Produkten vor Ort.“

Dirk Rosenau, Software Engineering/Postal & Security Approval, FP Inovolabs

FP Inovolabs ist Entwickler elektronischer und mechanischer Geräte – als Teil der FP-Unternehmensgruppe und auch für dritte Kunden. Neben Mess- und Wiegetechnik befasst sich das Unternehmen hauptsächlich mit Sicherheitstechnologie. GIT SICHERHEIT sprach mit Dirk Rosenau, zuständig für Software Engineering/Postal & Security Approval bei dem Unternehmen.

GIT SICHERHEIT: Herr Rosenau, Ihr Unternehmen gehört zur FP-Unternehmensgruppe und befasst sich unter anderem mit Sicherheitstechnologie. Geben Sie uns zum Einstieg einmal einen Überblick und das eine oder andere typische Beispiel aus diesem Bereich?

Dirk Rosenau: Der FP-Konzern betreibt weltweit über 200.000 Frankiermaschinen, die für unsere Kunden Geldtransaktionen im Wert von über 1.5 Milliarden US-$ im Jahr absichern. Den durch die Regulierungsbehörden vorgegebenen Standards folgend, setzen wir in diesen Maschinen Hardwaresicherheitsmodule (HSM) ein, die zur Umsetzung von kryptografischen Methoden die dafür relevanten kritischen Betriebsparameter wie Schlüssel oder in unserem Fall auch Geldwerte vor unautorisiertem Zugriff und Manipulation schützen. Ein HSM bietet hier physischen Zugriffsschutz auf einem hohen Niveau, um auch einen sicheren Betrieb an öffentlich zugänglichen Betriebsorten mit adäquater Sicherheit zu gewährleisten. In unseren Produkten zur digitalen Kommunikation setzen wir ebenfalls Kryptografie ein, um die Nachweisbarkeit von Ereignissen und die Authentizität oder Vertraulichkeit von Dokumenten gewährleisten zu können.

Sie befinden sich wie viele Unternehmen mitten in einem Prozess der Transformation, die von der Digitalisierung, dem Internet der Dinge und der Vernetzung geprägt ist. Was bedeutet das in Ihrem Fall?

Dirk Rosenau: Digitale Transformation bedeutet zunächst Veränderung von Prozessen und Einsatz digitaler Produkte und Dienstleistungen. Wir passen hier sowohl unsere eigenen Geschäftsprozesse an, entwickeln aber auch neue digitale Produkte für unsere Kunden. Wir setzen bei uns im Haus unser eigenes FP-Sign-Produkt ein, um diverse interne Geschäftsprozesse zu digitalisieren (z. B.: digitale Bestellung oder Unterschriftenmap-

pe). Dadurch erzielen wir neben der schnelleren Abwicklung auch mehr Transparenz, da alle an diesen Geschäftsprozessen beteiligten Personen ihre Dokumente und den Zustand der Bearbeitung einsehen können. Digitale Transformation ist aber auch mit viel Aufklärung verbunden. Veränderung muss mit Überzeugung durch Vertrauensbildung und Verbindlichkeit der digitalen Lösungen eingeführt werden. Wir glauben, dass unsere fast hundertjährige Erfahrung hier auch in Zukunft überzeugen und andere ebenfalls inspirieren kann. In unserem IoT-Geschäftsfeld können wir bei unseren Kunden bereits neue Bedürfnisse nach Transformation erkennen. Es gibt einen zunehmenden Wunsch nach dem Einsatz von Pay-per-use-Modellen, die wir mit unseren Produkten abbilden können. Dies bedeutet: Anbieter verändern ihre Geschäftsmodelle vom Verkauf von Hardware zum Verkauf von lösungs- und serviceorientierten Produkten.

Zu Ihrer Strategie zählt auch die Verstärkung des Geschäftsbereichs Sichere digitale Kommunikationsprozesse. Was bedeutet das im Einzelnen?

Dirk Rosenau: Sicherheit in diesem Zusammenhang umfasst Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit. Diese Kriterien sind in der digitalen Kommunikation, beim Speichern und Verarbeiten von besonderer Bedeutung für unsere Kunden – sowohl bei der Kommunikation von Person zu Person (P2P) als auch von Maschine zu Maschine (M2M). Mit Hilfe von kryptografischen Verfahren, der sorgfältigen Auswahl von Algorithmen und Schlüssellängen und einem Zertifizierungsprozess durch vertrauenswürdige Dritte können wir geeignete Lösungen anbieten. Grundsätzlich erfordert die Produktentwicklung und Pflege von Produkten in diesen Geschäftsbereich eine kontinuierliche Verbesserung und Stärkung der Sicherheit dieser Produkte, da die Bedrohungen durch Cyberkriminalität täglich zunehmen. Als Folge entstehen neue Standards und Empfehlungen von nationalen und internationalen Behörden und Standardisierungsgremien. Diese Empfehlungen und Erkenntnisse verwerten wir insbesondere in unseren neuen Produkten wie FP Sign oder den IoT-Gateways und werden zunehmend neue Dienste für Kunden in relevanten Märkten anbieten (Energiewirtschaft, Umwelttechnik, Wasserwirtschaft, Automatisierungstechnik, Gebäudetechnik).

FP im Firmenname steht ja für Francotyp-Postalia – dahinter steht der historische Kern der Unternehmensgruppe, aber auch ein technischer: Da wäre die digitale Postbearbeitung und kryptografisch geschützte Sicherheitsmodule auf Frankiermaschinen. Könnten Sie einmal nachzeichnen, welche Wege dies für die Entwicklung neuer Sicherheitssysteme für Sie eröffnet hat und eröffnet?

Dirk Rosenau: Die United States Postal Services (USPS) als nationale Postbehörde in den USA haben schon sehr früh die Digitalisierung ihrer Prozesse vorangetrieben und z. B. einen eindeutigen 2D Barcode für maschinell frankierte Briefe und Pakete eingeführt. Damit erkennen sie Betrug und ermöglichen gleichzeitig die Steuerung ihrer Geschäftsprozesse. Teil der Einführung waren hohe Schutzanforderungen an die Frankiermaschinen. FP war 1999 die erste europäische Entwicklungsgesellschaft bzw. der erste europäische Hersteller eines Hardwaresicherheitsmoduls, welches nach den nordamerikanischen Kriterien des NIST nach dem FIPS-140-Standard zertifiziert wurde. Dieser Standard beschreibt Anforderungen an kryptografische Module, die beim Einsatz von schutzbedürftigen Produkten und Prozessen vorwiegend im Behördenumfeld eingesetzt werden müssen. Die stetige Aktualisierung der Standards und Publikation von Empfehlungen hat zur Verbreitung und Anerkennung auch im europäischen und internationalen Umfeld geführt. FP hat inzwischen diverse Generationen von Hardwaresicherheitsmodulen (HSM) mit unterschiedlichen Funktionsumfang zertifiziert und im Einsatz. Die gesammelten Kenntnisse und Erfahrungen bei der Entwicklung dieser Module führen zu einer Methodik, die heute als Security by Design bezeichnet wird. Sie ist die Grundlage, um auch neuen Anforderungen gerecht werden zu können. Dabei fokussieren wir uns zunehmend neben unseren postalischen Lösungen auf die breiten Einsatzmöglichkeiten der industriellen IoT, bei denen die hohe physische Sicherheit unserer HSMs einen deutlichen USP darstellt.

. . . letztlich geht es immer um die sichere Verwaltung von Informationen?

Dirk Rosenau: Korrekt. Informationen sind heute für viele Prozesse und ganze Unternehmen die Grundlage des Geschäftsmodells. Denken Sie an die Sozialen Netzwerke oder Vertriebsportale in der Cloud. Im industriellen Bereich werden immer häufiger Informationen gesammelt und über maschinelles Lernen oder Systeme mit Anteilen künstlicher Intelligenz zur Prozessverbesserung oder Optimierung der Wartung herangezogen (predictive maintenance).

Sie waren auch ein Pionier bei der De-Mail, der nachweisbaren E-Mail mit rechtssicherer Signatur . . . ?

Dirk Rosenau: Ja, Mentana Claimsoft als 100 % Tochter der FP Holding war erster zertifizierter De-Mail Dienstanbieter. Ursprünglich als rechtssichere E-Mail mit den Attributen wie Versandbestätigung, Zugangsbestätigung, Authentifizierung und vertraulich für alle Bundesbürger gestartet, transformiert De-Mail in Deutschland insbesondere die Kommunikationsprozesse von Bundesbehörden untereinander und zu ihren Kunden. Das E-Government-Gesetz verpflichtet die Verwaltung unter anderem dazu, einen elektronischen Zugang über De-Mail zu eröffnen. Die dafür verwendete Technologie und die damit verbundene Rechtsicherheit kann aber auf andere Märkte und Produkte übertragen werden.

In welchen Märkten und Anwendungsgebieten sehen Sie hier vor allem Möglichkeiten?

Dirk Rosenau: Durch die neuen Möglichkeiten im Rahmen der europäischen eIDAS-Verordnung sind rechtssichere elektronische Signatur in Kombination mit Dokumenten und Prozessmanagement mittlerweile sehr einfach und komfortabel einsetzbar, z. B. mit dem von FP angebotenen Produkt FP Sign. FP Sign ermöglicht Transaktionen wie Vertragsabschlüsse, Freigabe- und Genehmigungspro-

FP Sign ermöglicht Transaktionen wie Vertragsabschlüsse, Freigabe- und Genehmigungsprozesse effizient, sicher und richtlinienkonform ohne Medienbrüche bei voller Transaktionskontrolle abzuwickeln ▼

zesse effizient, sicher und richtlinienkonform ohne Medienbrüche bei voller Transaktionskontrolle abzuwickeln. Die Richtlinien wie auch das Sicherheitsniveau kann der Kunde dabei in seinen Prozessen je nach Bedarf selbst festlegen.

Sie haben die manipulationssichere Abbuchung von Geldwerten genannt: Wie sieht Ihre Lösung hier aus?

Dirk Rosenau: FP betreibt diverse IT-Infrastrukturen, die unterschiedliche Abrechnungsverfahren mit Banken oder Abrechnungsservern in Kombination mit unseren Hardwaresicherheitsmodulen in den Frankiermaschinen unterstützen. Kunden können auf ein Bankkonto einen Betrag einzahlen, der dann in der IT-Infrastruktur auf den entsprechenden Kundenaccount übernommen wird. Je nach Anwendungsfall kann der Kunde dann Teilbeträge von seinem Account direkt an die Maschine manuell oder automatisiert übertragen. Auf der Maschine werden dann von dem im HSM gepflegten Budget für speziell erbrachte Leistungen Kleinstbeträge abgebucht und elektronische Belege erstellt. Diese Belegerstellung ist direkt mit der Abbuchung als Dienst im HSM implementiert, so dass keine Belegausgabe ohne Abbuchung möglich ist. Im Fall einer Frankiermaschine wird dieser Beleg als 2D-Barcode auf den Brief aufgedruckt. Ein im Barcode enthaltener Sicherheitscode kann anschließend vom Postunternehmen auf Korrektheit verifiziert werden. Damit dies technologisch für jede Maschine eindeutig möglich wird, setzen wir hier bevorzugt asymmetrische Kryptografie mit einer Public Key Infrastruktur (PKI) ein. Dies ermöglicht sowohl die individuelle Schlüsselgenerierung als auch sichere Verteilung der Schlüssel in Form von X509-Zertifikaten zur Verifikation an beliebigen Stellen. Das HSM in unseren Frankiermaschinen übernimmt hier neben der Abbuchung und Verwaltung der Geldbeträge auch die Aufgabe der sicheren Kommunikation zwischen der Maschine und der IT-Infrastruktur über Internet oder alternative Telekommunikationsnetze. Hier wird sowohl beidseitig authentisiertes TLS 1.2 auf der Basis von X509-Zertifikaten als sicherer Transport-Layer eingesetzt, als auch eine weitere beidseitige Authentisierung zwischen dem HSM und dem Kundenaccount in der Infrastruktur umgesetzt. Der Geldtransfer ist transaktionssicher implementiert, so dass Verbindungsabbrüche zu keinem Verlust von Daten führen können.

Welche Entwicklungen haben sie für das Thema Elektromobilität im Auge?

Dirk Rosenau: Bei der E-Mobilität beobachten wir derzeit die Zertifizierungsprogramme und damit verbundenen Bedarfe für Ladesäulenhersteller und -Betreiber. Hier gibt es die zweite Ladesäulen Verordnung (LSV II), das Eichrecht und diverse Bezahlsysteme und Protokolle (ISO/IEC 15118). Es ist zu erwarten, dass mit dem zunehmenden Ausbau der Infrastruktur für öffentliche Ladesäulen auch physische Sicherheit in Elektromobile und Ladesäulen integriert werden muss, um auch spontanes Laden ohne festen Vertrag zu unterstützen. Mit der Verbreitung der Ladesäulen wächst auch der Bedarf an physischer Sicherheit.

Die Normen in verschiedenen IoT-relevanten Sektoren von Smart-Cities, und -Energy bis Industrie 4.0 sind im Fluss der Entwicklung. Und seit Ende Juni gibt es den EU Cybersecurity Act, der unter anderem auch ein Rahmenwerk für die IT-Sicherheitszertifizierung von Systemen installiert. Sehen Sie das als Chance für die Etablierung neuer Produkte aus Ihrem Hause an?

Dirk Rosenau: Ja, historisch werden FP-Produkte nach nationalen und internationalen Sicherheitsstandards entwickelt, geprüft und zugelassen. Diesem Prinzip werden wir auch in Zukunft treu bleiben. Die durch diese Zulassungen erworbenen Erfahrungen und Produkteigenschaften können auch auf neue Rahmenwerke übertragen werden. Der Cybersecurity Act (CSA) listet Sicherheitsmerkmale auf, die sich auch in anderen neuen Normen und Standards (FIPS 140-3 für kryptografische Module oder DIN SPEC 27072 Mindestanforderungen an IoT-fähige Geräte) als wesentliche Anforderungen wiederfinden. Viele dieser Kriterien wie z. B. die eindeutige Identifizierung, die Update-Fähigkeit von Produkten oder vertrauliche Kommunikation sind bereits heute in unsere Produkte implementiert. Auch wenn die Erstellung von EU-weit gültigen cybersecurity schemes unter dem CSA noch am Anfang steht, so erwarten wir ein Framework, das einen innerhalb der EU allgemeingültigen Rahmen für diverse Produktklassen schafft. Dieser wird mehr Transparenz für Kunden ermöglichen, indem z. B. das Sicherheitsniveau (basic, substantial und high) klar beschrieben sowie der Zulassungsprozess überwacht wird.

Was wird in nächster Zukunft aus Ihrem Hause auf uns zu kommen?

Dirk Rosenau: Der Bereich Mail-Business wird neue international verfügbare digitale Dienste anbieten, die sowohl den Paketversand als auch das Dokumentenmanagement komfortabler und schneller ermöglichen werden. Neben den digitalen Produkten wird FP im Geschäftsfeld Secure IoT ganzheitliche Lösungen vom Gateway bis zur Visualisierung und Auswertung von Ereignissen inklusive Alarmierung in der Cloud anbieten. Wir zielen insbesondere auf die Zielmärkte Infrastrukturautomatisierung, Energieverteilung (erneuerbare Energien) und Fabrikautomatisierung. Die Lösungen werden mit den Anforderungen der Kunden wachsen und in der Zukunft insbesondere durch das Einbringen physischer Sicherheit ausgezeichnet sein. ■

Kontakt

FP Inovolabs,
Berlin
Tel.: +49 30 220 660 601
info@inovolabs.com
www.inovolabs.com

VdS-Fachtagung Cyber-Security

Am 7. November 2019 präsentiert das VdS-Bildungszentrum in Köln erstmals die Fachtagung „Cyber-Security", die sich mit einem effektiven und bedarfsgerechten Cyber-Schutz, insbesondere für kleine und mittelständische Unternehmen, beschäftigt. Neben Brand- und Einbruchschutz ist der Schutz vor Cyber-Gefahren heutzutage ein wichtiger Aspekt der Unternehmenssicherheit.

VdS-Fachtagung_Cyber: Cyber-Angriffe gehören zu den größten Geschäftsrisiken deutscher Unternehmen. Auf der ersten VdS-Fachtagung Cyber-Security wird das brisante Thema von führenden Experten beleuchtet und es werden konkrete Lösungswege aufgezeigt.

„Unsere Fachtagung bietet wichtige Impulse für einen angemessenen Cyber-Schutz in kleinen und mittelständischen Unternehmen", erklärt Andrea Schriewer, im VdS-Bildungszentrum verantwortlich für das Thema Cyber-Security. VdS hat in den letzten Jahren ein Verfahren für KMU entwickelt, mit dem die Informationssicherheit eines Unternehmens verbessert, auditiert und zertifiziert werden kann. Diese Veranstaltung richtet sich an bereits VdS-anerkannte Berater für Cyber-Security oder VdS-zertifizierte Unternehmen nach VdS 10000 sowie IT-Dienstleister und Versicherer. Das gesamte Tagungsprogramm sowie die Möglichkeit zur Anmeldung ist abrufbar auf www.vds.de/cyber19 ■

Industrie-Router mit zweistufigem Sicherheitskonzept

Eine Fernwartungslösung wird heute oft nur dann akzeptiert, wenn das Anlagenpersonal die Hoheit über sämtliche Online-Verbindungen hat. Dafür bietet der Industrie-Router „MB Net Rokey" von MB Connect Line ein zweistufiges Sicherheitskonzept. Über den integrierten Schlüsselschalter des Routers wird vom Personal vor Ort gesteuert, ob nur Datenerfassung – oder zusätzlich Fernwartung und Routing – möglich sind. Die Erfassung der Anlagendaten, beispielsweise zum Visualisieren, Überwachen oder Archivieren, sind damit von der Fernwartung unabhängig. Im Modus „Datenerfassung" (ONL) ist der Router im Portal sichtbar, jedoch nicht konnektierbar. Der Fernzugriff mit Routing muss durch die Bediener der Anlage per Schlüsselschalter (REM) autorisiert werden.

Erst dann sind die Fernwartung und der Zugriff auf das Netzwerk hinter dem Router möglich. Nach dem Abschluss der Fernwartung sollte der Schalter wieder auf die Stufe „Datenerfassung" gestellt werden. Durch das zweistufige Sicherheitskonzept lässt sich die Fernwartung an der Anlage sperren, wenn sie nicht benötigt wird. Das bietet zusätzliche Sicherheit und erhöht die Akzeptanz der Fernzugriffslösung. ■

it-sa, Halle 11.0. Stand 212

ENDPOINT SECURITY

Schutz vor USB-Angriffen

Honeywells Secure Media Exchange adressiert USB-Angriffsmethoden

Die Secure Media Exchange (SMX)-Lösung für die Cyber-Sicherheit industrieller Betriebe dient dem Schutz gegen neue und zunehmende Universal Serial Bus (USB)-Bedrohungen. Das neue SMX enthält zum Patent angemeldete Funktionen zur Abwehr eines breiten Spektrums schädlicher Angriffe auf USB-Geräte, mit denen der Betrieb durch Missbrauch legitimer USB-Funktionen oder durch unberechtigte Geräteaktionen gestört wird.

Die erweiterten Schutzmechanismen vervollständigen die zusätzlich eingebrachten SMX-Verbesserungen zur Erkennung von Schadsoftware unter Verwendung von maschinellem Lernen und Künstlicher Intelligenz (KI). Gemäß einer Honeywell-Studie verbessert das die Problemerkennung um bis zu 40 Prozent im Vergleich zu traditionellen Antivirus-Lösungen. Insgesamt bietet diese Aktualisierung der SMX-Plattform umfassenden, unternehmensweiten USB-Schutz sowie Transparenz und Kontrolle bezüglich der herausfordernden technischen Anforderungen industrieller Umgebungen.

USB-Geräte umfassen Flash-Laufwerke und Ladekabel sowie viele weitere über USB angeschlossene Geräte. Diese stellen ein wesentliches Einfallstor in die Umgebungen industrieller Leitsysteme (ICS) dar. Bisherige Security-Überwachungen richten dabei den Fokus auf die Erkennung von Schadsoftware an den USBs. Obwohl auch das wichtig ist, belegen Untersuchungen einen wachsenden Trend zu neuen Kategorien von USB-Bedrohungen, mit denen die Funktionalität der Gerätestandards verändert wird, um gängige Security-Mechanismen zu unterlaufen und die Systeme der Leittechnik direkt anzugreifen. Diese schädlichen Übergriffe auf USB-Geräte umfassen 75 Prozent der gegenwärtig bekannten Kategorien an USB-Angriffen, ein eindeutiges Indiz für das Aufkommen neuartiger Angriffsmethoden. Da diese Attacken gängige USB-Peripherien wie Tastaturen oder Lautsprecher als Angriffsmedium verwenden können, erfordert effektiver Schutz eine ausgefeilte Gerätevalidierung und Autorisierung.

Schutz vor Schäden und Stillständen

„Schädliche USB-Angriffe mit ihren Möglichkeiten zur Emulation, Ausnutzung und Manipulation von USB-Geräten sind zunehmend bösartig und verursachen häufig Schäden und Betriebsstillstände“, sagte Sam Wilson, weltweiter Produkt Marketing Manager, Honeywell Industrial Cybersecurity.“ Honeywell ist führender Anbieter einer leistungsfähigen industriellen Lösung zur Cyber-Sicherheit, die gegen derartige Angriffe auf USB-Geräte schützt. Diese Angriffe entsprechen dem überwiegenden Anteil an USB-Bedrohungskategorien und der sich weiter entwickelnden Schadsoftware. Da die Verwendung von USBs sowie die Gerätevielfalt zunehmen, wird die personelle Verifizierung von Geräteaktionen auch weiterhin eine bedeutende Rolle spielen.“

Der SMX-Schutz enthält zusätzlich die innovative Trusted Response User Substantiation Technology (TRUST) von Honeywell, die eine personelle Validierung und Authentifizierung ermöglicht und damit die Plausibilisierung der USB-Geräte absichert. TRUST trägt dazu bei, dass unerwünschte oder verdächtige Geräte keine weiteren Bedrohungen in die industrielle leittechnische Umgebung einbringen können. Bei USB-Speichermedien kommen ergänzende technologische Ebenen zur Erkennung neuerer Schadsoftware zum Einsatz, um zusätzlich gegen derartige Angriffe zu schützen. Hierzu gehören maschinelles Lernen sowie Künstliche Intelligenz, mit denen die Erkennung zunehmend komplexer Schadsoftware verbessert wird, einschließlich der am Entdeckungstag ausgenutzten Schwachstellen (Zero Day Malware) sowie schnell angepasster Schadprogramme.

SMX hilft den Anwendern dabei, Anpassungen im Bereich Personal, Prozess und Technologie zur Verbesserung des Reifegrades ihrer industriellen Cyber-Sicherheit vorzunehmen. Es schult USB-Nutzer darin, mögliche Probleme nach Ankopplung zu erkunden und zwingt Anlagenmanager zur formalen Einhaltung von Anmelde- und Abmeldeprozessen. Als technologische Überwachung ermöglicht SMX einen kontinuierlichen Schutz gegen Bedrohungen. Die aktuellen Verbesserungen stellen sicher, dass Anwender ihre USBs an jedem Ort überprüfen und so industrielle Cyber-Sicherheit einfach umsetzen können.

Die neueste Freigabe der SMX-Technologie enthält eine Reihe weiterer Funktionen. Hierzu gehören:

- Neues zentralisiertes Management: bietet Transparenz von USB-Geräten, die an industrielle leittechnische Umgebungen angeschlossen werden, sowie zentrales Bedrohungsmanagement für alle SMX-Standorte.
- Neue ICS Shield Integration: bietet zusätzliche Darstellung von USB-Aktivitäten an geschützten Endgeräten. Das schließt den Kreis zwischen zentralen Management-Funktionen und verteiltem Schutz innerhalb des Leitsystems, ohne die in der Industrie bewährte Zonen-Segmentierung zu umgehen.
- Erweiterte SMX-Möglichkeiten: bietet verschiedene Ausführungen je nach speziellem Industriebedarf, einschließlich tragbarer SMX ST-Modelle für das viel beschäftigte Betriebspersonal sowie robuste Modelle für Industrieanwendungen auch in gefährlichen Umgebungen, bei Bedingungen gemäß Militärstandard und bei Arbeitssituationen mit Handschuhen. ■

Kontakt

Honeywell Process Solutions GmbH
Offenbach
Tel.: +49 69 806 40
konstantin.rogalas@honeywell.com
www.honeywell.com

Fotos: Axis Communications

VIDEOSICHERHEIT

Video cybersecure

Cybersecurity im Unternehmen– Physikalische und digitale Sicherheit sind gleichermaßen wichtig

Daten sind das neue Öl, Informationen das neue Gold. Unternehmen sind immer mehr abhängig von der digitalen Welt. Sensible Bereiche, wie z. B. Rechenzentren, physikalisch zu schützen ist selbstverständlich. Die IT-Abteilungen stehen darüber hinaus unter immer größerem Druck, jedes im Netzwerk angeschlossene Gerät zu überwachen und vor Angriffen von innen und außen zu schützen. Dies gelingt nur mit den richtigen Tools und einem hohen Maß an Transparenz.

Im Folgenden werden Best Practices skizziert und Fragen in den Raum gestellt, mit denen sich IT-Verantwortliche, aber auch die Verantwortlichen von Sicherheitssystemen auseinandersetzen müssen. Im Zentrum steht dabei die Frage, wie man sensible Bereiche, aber auch jedes einzelne Gerät im Netzwerk am besten schützt.

Unternehmen sind einer stetig wachsenden Flut von Cyberattacken ausgesetzt. Mal aus Spaß an der Freude, meist aber mit kriminellen Absichten versuchen Hacker sich Zugang zu den Unternehmensnetzen zu verschaffen. Das wirtschaftliche Risiko ist hoch, die Gesetzeslage (z. B. die DSGVO) wandelt sich stetig.

Physikalische Sicherheit durch IP Video und IP Zutrittskontrolle

Rechenzentren liegen meist in abgelegenen Bereichen des Unternehmens und bei reibungslosem Betrieb sind Mitarbeiter eher selten vor Ort.

Mit Hilfe von IP-basierter Zutrittskontrolle und IP-Kameras kann man diesem Umstand gerecht werden. Mitarbeiter erhalten nur dann Zugang, wenn sie die entsprechenden Berechtigungen haben und mit den Videosystemen kann zum einen unbefugter Zugang überwacht und zum anderen auch der Safety-Aspekt unterstützt werden. Oftmals arbeiten gerade am Wochenende oder in der Nacht Techniker alleine in den Rechenzentren. Ein Mitarbeiter aus der Zentrale kann aus der Ferne den Einsatz überwachen und sicherstellen, dass bspw. bei einem Unfall schnell geholfen wird.

Richtig eingesetzt kann mit den Systemen im Ernstfall auch schnell und effizient ermittelt werden, wie viele Mitarbeiter sich in den geschützten Bereichen befinden und den Rettungskräften mitgeteilt werden, wie viele Personen ggf. evakuiert werden müssen.

Systeme aktualisieren – Schwachstellen schließen

Je älter ein IT-System, desto größer wird das Risiko für Cyberattacken. Eine recht simple Weisheit. Die meisten Cyberattacken machen sich die bereits hinlänglich bekannten Schwachstellen zunutze. Breit angelegte Attacken scannen dabei die zu infiltrierenden Systeme auf bekannte Sicherheitslücken. Dies passiert nicht nur bei Angriffen von außen. Immer mehr Unternehmen werden auch von innen heraus attackiert: sorglos in den PC gesteckte, infizierte USB-Datenträger; mit Viren befallene Laptops von Servicetechnikern, die sich für Administrationsarbeiten mit den Firmensystemen verbinden oder der Aufruf einer Webseite

von einem nicht durch die eigene IT beschafften Server ohne aktuellem Virenscanner – all dies sind klassische Methoden, Systeme zu infizieren.

Keine Cybersecurity ohne Management Tools!

Management-Tools sind für die IT-Sicherheit von essentieller Bedeutung. Nur mit ihrer Hilfe kann man die anfallenden Aufgaben zur Aktualisierung der Systeme effizient bewerkstelligen. Kaum ein Admin prüft zyklisch die Geräte im Netzwerk manuell auf neue Firmware-Versionen oder abgelaufene Zertifikate. Dazu fehlt schlicht die Zeit.

Ein simpler Vergleich macht den Unterschied deutlich: Das manuelle Updaten von Firmware und Analyse-Plugins in einem Kamerasystem mit 200 Geräten dauert via Einzelaufruf

Die meisten Cyberattacken machen sich die bereits hinlänglich bekannten Schwachstellen zunutze

Cybersecurity hat viel mit richtigen Prozessen zu tun – und fängt schon bei der Entscheidung für Komponenten an

der Geräte schnell in Summe über 100 Stunden. Mit dem Axis Device Management Tool lässt sich dieser Aufwand auf überschaubare 30 Minuten reduzieren.

Never change a running system!

Auf der einen Seite sollen die Systeme aktualisiert werden, aber auf der anderen fasst niemand gerne ein laufendes System an und spielt Updates ohne zwingende Notwendigkeit ein. Zu hoch ist das Risiko, dass die Systeme im Anschluss nicht mehr hundertprozentig funktionieren.

In vielen Fällen kommt es auch vor, dass eine komplexe Management Software nur mit einer bestimmten Geräte Firmware kompatibel ist und das Gerät nicht auf einfachem Weg auf eine aktuelle Firmware gebracht werden kann.

Axis bietet für diese Eventualitäten eine sogenannte LTS Firmware an. In diesen speziellen Varianten werden die Firmware Versionen nur auf bekannte Schwachstellen und Sicherheitslücken hin überarbeitet. Alle anderen Bereiche der Funktionalitäten werden nicht angetastet. So gelingt der Spagat eine sichere und kompatible Firmware, insbesondere für ältere Gerätegenerationen, bereitzustellen.

Ohne Transparenz geht es nicht

Warum setzt die IT auf die Zusammenarbeit mit bekannten Markenherstellern, wenn man die meisten Komponenten auch von No-Name-Anbietern wesentlich günstiger bekommen kann? Einer der Gründe dafür ist das Cybermanagement. Namhafte Hersteller geben zugleich auch das Versprechen ab, sich im Falle einer auftretenden Sicherheitslücke um deren Behebung zu kümmern und einen entsprechenden Patch bereitzustellen.

Und das Versprechen geht sogar noch weiter: Die Kunden werden über die Problematik informiert und aufgefordert, ihre Systeme entsprechend upzudaten. Es wird nichts verschleiert oder ausgesessen.

Auch die White-Hat Hackers konzentrieren sich meist auf die großen Anbieter. Diese Hacker versuchen mit Penetrationstests und Testmethoden Schwachstellen zu finden, ohne einem Unternehmen damit einen Schaden zuzufügen. Große Unternehmen loben immer höhere Preisgelder für das Auffinden von Schwachstellen aus. Diese gehen inzwischen schnell in den 6- oder 7-stelligen Bereich.

OEM und ODM – Ein großes Cyberrisiko

In der Sicherheitsbranche ist es leider nur allzu üblich, den eigentlichen Hersteller einer Komponente zu verschleiern. Dieses sogenannte OEM- oder ODM-Geschäft macht das Thema Cybersecurity zu einem Glücksspiel.

Was bedeutet OEM oder ODM? Bei diesen Geräten ist der verwendete Markenname nicht gleich dem Hersteller. Eine ganze Zuliefererindustrie hat sich darauf spezialisiert, selbst in Kleinserien von wenigen 100 Geräten jedes gewünschte Logo und jeden gewünschten Produktnamen möglich zu machen. Auch das Webinterface wird schnell und einfach mit entsprechenden Logos angepasst.

Die OEM-Anbieter sparen sich Entwicklungs- und Herstellungskosten und können auf diesem Weg sehr einfach ein umfangreiches „eigenes" Portfolio vorgaukeln. Selbst etablierte Hersteller greifen inzwischen darauf zurück, bspw. zur Erweiterung des Portfolios um Einstiegsprodukte.

Wenn es um die Cybersecurity-Aspekte des Systems geht, dann macht genau diese Verschleierung die Arbeit kompliziert. Security Patches des ursprünglichen Herstellers finden entweder gar nicht oder nur mit erheblichem Zeitversatz den Weg in die OEM Geräte. Sicherheitslücken, die der Hersteller für seine eigenen Geräte veröffentlicht, werden nur äußerst selten auch von den OEM Anbietern übernommen.

Aus gutem Grund ist der Einsatz von OEM Komponenten in der IT verpönt. Die mangelnde Transparenz und fehlenden Garantien im Cyber-Kontext wiegen den Preisvorteil in keinem Fall auf.

Sensibilisierung der Hersteller, Errichter und Endkunden

In der IT-Industrie hat sich das Thema Cybersecurity über die vergangenen Jahrzehnte immer weiterentwickelt. Unternehmensprozesse sind entsprechend gestaltet, Wartungsverträge für Soft- und Hardware sind gängige Praxis - und sogar jeder Privatanwender kann mit dem Begriff Virenscanner etwas anfangen und führt regelmäßig ein Update auf seinem Smartphone aus.

Die Sicherheitsindustrie ist vielerorts leider noch nicht ganz so weit. Das fehlende IT Know-how bei vielen Herstellern, die fehlende IT-Qualifizierung auf Seiten vieler Errichter und auch die gewachsenen Strukturen bei Endkunden sind kein besonders guter Nährboden für Veränderungen.

Wie wird man Cyber secure?

Cybersecurity hat sehr viel mit den richtigen Prozessen zu tun. Dies fängt schon bei der Entscheidung für die Komponenten an. OEM-Geräte gilt es auf jeden Fall zu vermeiden, einschlägig bekannte Seiten wie bspw. www.ipvm.com geben Auskunft zu diesem Thema und machen die Gebaren der Branche transparenter.

Neben Features und Funktionen der Geräte muss ein Management Tool für administrative Aufgaben vorhanden sein.

Die IT-Abteilung gilt es grundsätzlich mit einzubeziehen, egal ob die Geräte im Firmennetz betrieben werden oder ein separates Netzwerk aufgebaut wird.

Und natürlich müssen Hardware und Software zyklisch aktualisiert werden. Wartungsverträge helfen die Kosten kalkulierbar zu halten und sorgen dafür, dass das Thema nicht in Vergessenheit gerät.

Cybersecurity funktioniert nur, wenn alle daran mitarbeiten.

Autor:

Timo Sachse,
Product Analyst EMEA bei
Axis Communications

it-sa, Halle 10.0, Stand 423

Kontakt

Axis Communications, D-Ismaning
timo.sachse@axis.com
www.axis.com

PHYSIKALISCHE SICHERHEIT

Cyber Security für Sicherheitsanbieter

Sicherheitstechnik gegen Angriffe schützen – BHE gibt Support

Auch Sicherheitsanbieter müssen sich mit dem Thema Cyber Security auseinandersetzen und ihre Techniken schützen. Welchen Support der BHE seinen Mitgliedern in Sachen Cyber Security gibt, lesen Sie in diesem Artikel.

Dem 1974 gegründeten BHE Bundesverband Sicherheitstechnik e.V. sind heute über 1.000 Mitgliedsunternehmen aus ganz Deutschland angeschlossen, die vorbeugende Sicherungstechnik herstellen, planen und/oder installieren.

Als Kommunikations- und Informationsplattform für alle, die sich mit Sicherheitsfragen beschäftigen, hält der BHE seine Mitglieder über alle relevanten Themen und Neuerungen auf dem Laufenden und bietet entsprechende Hilfestellungen und Unterstützung an.

So auch bei einer der größten Herausforderungen des 21. Jahrhunderts, der Cyber-Security.

Cyber-Security und IT-Sicherheit haben gewerkeübergreifend immer größere Auswirkungen auf die Sicherheits-Branche. Sowohl betriebsintern als auch bei Kunden sind in Sachen Digitalisierung und Vernetzung viele Aspekte zu beachten.

Dabei liegt die Hauptaufgabe nicht nur darin, dass die Anwendungen problemlos funktionieren, sondern dass sie gegen Angriffe abgesichert sind. Denn bei allen Systemen und Geräten, die mit dem Internet verbunden sind, besteht die Gefahr, dass unbefugte Dritte die Daten ausspähen oder manipulieren. Deshalb müssen grundlegende datenschutzrechtliche Standards eingehalten und Vorkehrungen für eine sichere Datenspeicherung, -übertragung und -zugriff umgesetzt werden. In diesem Punkt unterscheidet sich professionelle Sicherheitstechnik – wenn man sich zum Beispiel den Privatbereich vor Augen hält – von gängigen „Smart Home-Produkten".

Der BHE-Fachausschuss IT führt die Kompetenzen der Hersteller von IT-Geräten (Überwachungseinheiten, Kameras usw.) und IT-Strukturen (Switche, Router usw.) zusammen mit den praktischen Erfahrungen der BHE-Errichter. Aus diesem Fachwissen und Erfahrungsschatz werden zu allen wichtigen IT-Themen Informationen für die BHE-Mitglieder erstellt.

Sicherheitsanbieter, die in diesem sich dynamisch weiterentwickelnden Themenfeld mit den aktuellen Entwicklungen Schritt halten möchten, lädt der BHE zu einer Mitarbeit im FA-IT ein. Der Fachausschuss trifft sich zweimal pro Jahr, die nächste Sitzung findet am 10. Oktober 2019 in Fulda-Künzell statt. Nähere Informationen erhalten Interessenten in der BHE-Geschäftsstelle (b.brill@bhe.de; Telefon +49 6386 9214-12).

Der „IT-Blog" unter www.bhe.de/it-blog bietet außerdem aktuelle Nachrichten und Informationen aus der IT-Welt. Hier werden u.a. aktuelle Meldungen des BSI oder von Heise-Security veröffentlicht sowie interessante Beiträge verschiedener Zeitungen.

Auch der neue BHE-Praxis-Ratgeber Informationstechnik (IT) greift das Thema IT auf – insbesondere die Netzwerktechnik in Verbindung mit diversen sicherheitstechnischen Anlagen. Der Ratgeber ist zur Unterstützung bei der täglichen Arbeit, als Nachschlagewerk für den Errichter, für Planer, aber auch für den Betreiber von sicherheitstechnischen Anlagen konzipiert.

Detaillierte Informationen finden Interessenten unter www.bhe.de/praxisratgeber-it. ■

Kontakt

BHE Bundesverband Sicherheitstechnik e.V.
Brücken
www.bhe.de

56 Prozent der Incident Response Requests erfolgen nach spürbaren Folgen einer Cyberattacke

Eine aktuelle Analyse von Kaspersky zeigt, dass Unternehmen mehrheitlich (56 Prozent) Unterstützung im Bereich Vorfallreaktion anfragen, wenn das Kind bereits in den Brunnen gefallen ist – wenn also bereits offensichtliche Folgen eines Cyberangriffs aufgetreten sind, wie durch Ransomware verschlüsselte Workstations, nicht-autorisierte Finanztransaktionen oder Dienste nicht mehr verfügbar sind. 44 Prozent gehen dagegen aus Perspektive der IT-Sicherheitsprävention den besseren Weg: Sie reagieren schon in einem sehr frühen Stadium des Angriffs, so dass die Organisation potenziell schwerwiegenden Konsequenzen entgehen kann.

Der aktuelle Kaspersky-Report zeigt die Analyse von Incident Responses, an denen Experten des Cybersicherheitsanbieters im Jahr 2018 beteiligt waren. Dabei wurden 22 Prozent der Vorfallreaktionen eingeleitet, nachdem potenziell schädliche Aktivitäten im Netzwerk festgestellt wurden, weitere 22 Prozent nachdem eine schädliche Datei gefunden wurde.

Beides kann ohne weitere Anzeichen auf Sicherheitsverstoße auf einen anhaltenden Angriff hindeuten. Das Problem: Nicht jedes Unternehmenssicherheitsteam ist in der Lage festzustellen, ob automatisierte Sicherheitstools diese schädlichen Vorgänge schon erkannt und ihnen Einhalt geboten haben; oder aber ob es sich um den Beginn eines größeren, unsichtbaren Vorgangs im Netzwerk handelt und externe Spezialisten erforderlich sind. ▼

it-sa, Halle 9, Stand 430

Kaspersky-Sicherheitsempfehlungen

- Ein eigenes Team einsetzen, das für IT-Sicherheitsvorfälle im Unternehmen zuständig ist.
- Backup-Systeme für wichtige Assets implementieren.
- Um frühzeitig auf einen Cyberangriff zu reagieren, eine Kombination aus dem firmeninternen Incident-Repsonse-Team als erste Verteidigungslinie und einem externen Dienstleister für komplexere Vorfälle wählen.
- Einen Plan zur Vorfallreaktion mit detaillierten Anleitungen und Verfahren für verschiedene Arten von Cyberangriffen aufstellen.
- Schulungen und Trainings helfen dabei, Mitarbeiter für Cyberbedrohungen wie Spam zu sensibilisieren.
- Patch-Management-Prozesse implementieren, um Software stets aktuell zu halten und so Sicherheitslücken zu vermeiden.
- Regelmäßig Sicherheitsbewertungen der IT-Infrastruktur durchführen.

Zeitaufwendige Erkennung von Schadcode spielt Hackern in die Karten

Das Zeitfenster vom Auftauchen bis zur Erkennung neuer Malware – und seien es nur Minuten – reicht aus, um Schaden anzurichten. Nur auf Detektion zu setzen, kann folglich nicht der Heilige Gral der IT-Sicherheit sein, meint Bromium.

Bis neue Schadsoftware überhaupt erkannt wird, vergeht immer Zeit. Bromium hat diese Problematik am Beispiel eines Kunden detailliert untersucht. Im Juni 2019 wurden bei ihm mit der Bromium-Lösung Secure Platform, die Applikations-Isolation mittels Micro-Virtualisierung bietet, genau 35 Threats isoliert. Davon waren 29 definitiv bösartig, die restlichen entweder noch unbekannt oder Alarmierungen aufgrund eines verdächtigen Verhaltens. Konkret wurden 25 verschiedene Malware-Typen identifiziert, wobei bei 8 zum Zeitpunkt der Isolation eine Hash-basierte Erkennung noch nicht möglich war. Bis sie letztlich überhaupt erkennbar waren, vergingen dann nach Bromium-Untersuchungen zwischen 27 Minuten und 31 Stunden.

„Und genau an diesem Punkt zeigt sich das ‚Window of Opportunity' für die Angreifer, die sehr wohl wissen, dass sich viel zu viele Unternehmen und Behörden immer noch hauptsächlich mit der Detektion von Angriffen beschäftigen", erklärt Jochen Koehler, Regional VP Sales Europe bei Bromium in Heilbronn. „Die logische Konsequenz lautet, potenziell gefährliche User-Aktivitäten strikt zu isolieren, anstatt weiterhin nur auf Erkennung zu setzen."

Die derzeit effektivste Möglichkeit für die Isolation von Gefahren bietet die Micro-Virtualisierungstechnologie. Diesen Ansatz verfolgt Bromium seit Einführung seiner Software Secure Platform. Die Lösung schließt die zeitliche Lücke zwischen Auftreten und Erkennung von Schadsoftware. ■

it-sa, Mitaussteller bei Computacenter in Halle 10.0, Stand 216

Baramundi Management Suite

Die Baramundi Software AG veröffentlichte bereits im Mai das neue 2019er Release der Baramundi Management Suite (bMS). Die umfassende Unified-Endpoint-Management-Lösung (UEM) bietet den Nutzern mit dem neuen Release neben einem Customization Tool für Windows-Installation auch für Android Enterprise deutlich erweiterte Management-Möglichkeiten sowie eine Erweiterung der Self-Service-Funktion und ein neues Monitoring Feature. Wie in den Vorgängerversionen wurden zudem auch in der neuen Version 2019 die bestehenden Module mit dem Input der Kunden aus der baramundi Community weiterentwickelt. ■

it-sa, Halle 11.0, Stand 110

LastPass mit Identitätsmanagement aus der Cloud

Auftritt für LastPass auf der it-sa in Nürnberg: Vom 8. bis 10. Oktober 2019 präsentiert der Passwortmanager seine neue LastPass Identity Lösung, die Unternehmen aller Größen ein vollständiges, sicheres Identitätsmanagement aus der Cloud zu einem erschwinglichen Preis ermöglichen soll. Die neue LastPass Business-Lösung reflektiert die aktuelle IT-Realität in Unternehmen: Mitarbeiter bringen Hunderte von Cloud-Anwendungen in ihren beruflichen Arbeitsalltag mit. Das setzt IT-Teams unter Druck, ein hohes Sicherheitsniveau zu erreichen, ohne komplexe Authentifizierungsprozesse einzuführen, die die Produktivität der Mitarbeiter verringern. Auf diese Herausforderungen bei der Verwaltung von Zugriff und Identitäten ist LastPass Identity ausgerichtet. Die Software bietet drei Lösungsansätze: Die neue SSO-Technologie sichert Zugangspunkte für mehr als 1.200 Anwendungen, MFA bietet eine adaptive, biometrische Authentifizierungslösung - und schließlich sei LastPass Identity eine clevere Komplettlösung, die Enterprise Passwortverwaltung, SSO und MFA in einer einzigen Lösung kombiniert. Damit können Unternehmen, so der Anbieter, unabhängig von ihrer Größe und verfügbaren Ressourcen schnell und einfach eine erschwingliche, flexible Identitätslösung einsetzen und den Sicherheitsstandard eines modernen Arbeitsplatzes deutlich verbessern. Das entlaste auch IT-Teams. ■

it-sa, Halle 9, Stand 444

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

Commercial Manager
Jörg Wüllner +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
Iris Biesinger +49 6201 606 555

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

Verlagsvertretung
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

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

JEDER SPRICHT ÜBER DAS IIOT

... wir setzen es einfach um.

Netzwerke und Computer für eine „smartere“ Industrie.

- Cybersecurity-Lösungen für alle Ebenen und Topologien
- Leistungsstarke Computer, verlässliche Netzwerke
- Vertikale Integration von SCADA bis zu Feldgeräten

Moxa. Wo Innovation passiert.

www.moxa.com

MOXA®
Reliable Networks ▲ Sincere Service