Mit Security zu mehr Sicherheit

Schutz von Personen, Umwelt und Infrastruktur gegen Cyber-Bedrohungen

Die Vernetzung von Betriebsabläufen schreitet immer weiter voran. Unternehmen investieren daher beträchtliche Summen in Sicherheit, um ihre Marke, ihren Betrieb und das geistiges Eigentum zu schützen. Die sicherheitsrelevanten Auswirkungen von Cyber-Risiken werden dabei jedoch häufig übersehen. Mit der Integration von Safety-/Security-Programmen und den folgenden Schritten können Unternehmen die Auswirkungen von Sicherheitsrisiken abschätzen, managen und minimieren.

Einleitung

Industrielle Sicherheit hat oberste Priorität bei der Implementierung vernetzter, informationsfähiger Architekturen, mit denen Unternehmen ihre Produktivität, Effizienz und Sicherheit steigern wollen.

Ob es um den dezentralen Zugriff auf Produktionsmaschinen, den drahtlosen Zugriff auf Pumpenstationen oder die Anbindung von Fertigungsanlagen an die IT-Infrastruktur geht – eine höhere Konnektivität kann zu deutlichen Verbesserungen von Produktivität und Sicherheit führen. Doch auch die Risiken nehmen zu – nicht nur für geistiges Eigentum, Gewinne und systemkritische Produktionsressourcen, sondern auch für Personen und Umwelt.

Sicherheitssysteme sind so konzipiert, dass sie Fehler erkennen, Bediener warnen und automatisch eingreifen. Bei einer Änderung am oder einem Angriff auf das Sicherheitssystem können die entstandenen Sicherheitslücken dazu führen, dass ein Standardsteuerungssystem jenseits seiner Sicherheitsparameter arbeitet. Als Folge können Schäden an der Ausrüstung oder für die Umwelt entstehen oder sogar Mitarbeiter und die Allgemeinheit einer Gefahr ausgesetzt sein.

Konnektivität birgt Chancen und Risiken

Ein Connected Enterprise verbindet Personen, Prozesse und Dinge. Es bringt die Informationstechnologie (IT) auf der Unternehmensebene mit der Automation (OT) der Werksebene in einer gemeinsamen Netzwerkinfrastruktur zusammen. Außerdem zieht es Nutzen aus neuen Technologien, von Daten- und Analyse-Software bis hin zu intelligenten Geräten, die das Internet der Dinge (IdD) bilden.

„Die für den Betrieb, die Sicherung und die Wartung von Industriesteuerungssystemen verantwortlichen Mitarbeiter müssen die wichtige Verknüpfung zwischen Sicherheit und Security verstehen. Eine Security-Maßnahme, die die Sicherheit beeinträchtigt, ist inakzeptabel."

Guide to Industrial Control Systems (ICS) Security, NIST

Was bedeutet das für Hersteller und Industriebetriebe? Es bedeutet Produktionsintelligenz zum Messen und Verbessern nahezu sämtlicher Aspekte des Betriebs, wie Qualität, Produktivität, Betriebszeit und Gesamtanlageneffektivität (OEE). Es bedeutet unternehmensweite Konnektivität für den unmittelbaren Datenaustausch und die nahtlose Zusammenarbeit im gesamten Unternehmen. Es bedeutet dezentrale Überwachung kritischer Produktionsanlagen und auf dezentrale Standorte verteilter Systeme.

Neben all diesen Chancen sind aber auch die Risiken ein Thema. Mehr Anschlusspunkte bedeuten mehr Zugangspunkte und somit auch mehr Sicherheitsbedrohungen. Diese Bedrohungen können physisch oder digital sein, intern oder extern, böswillig oder unbeabsichtigt. Und sie können eine Gefahr in vielerlei Hinsicht darstellen, z. B. der Verlust geistigen Eigentums, Betriebsunterbrechungen und Einbußen bei der Produktqualität.

Sicherheit ist vielleicht die am wenigsten diskutierte Folge von Sicherheitsbedrohungen.

Wenn Security die Sicherheit bedroht

Angegriffene Maschinen- oder Prozesssicherheitssysteme können eine Kettenreaktion hervorrufen.

Wenn ein angegriffenes Sicherheitssystem die Maschine beim Erreichen eines gefährlichen Zustands oder beim Auslösen eines Sicherheitsgeräts nicht stoppt, kann es dazu kommen, dass das Werkspersonal genau den Gefahren ausgesetzt wird, die verhindert werden sollten. Sicherheitssysteme, die nicht in der Lage sind, die Produktion bei Erreichen bestimmter Betriebsbedingungen zu stoppen, können darüber hinaus Mitarbeiter oder die gesamte Anlage Gefahren wie Feuer, Chemikalienaustritt oder Explosionen aussetzen.

Die Risiken sind besonders hoch in Industriezweigen, in denen mit gefährlichen oder flüchtigen Stoffen gearbeitet wird, zum Beispiel in der Chemieproduktion. Und auch mit der zunehmenden Verbreitung von Robotik steigt das Risiko, da Menschen und Roboter Seite an Seite an den Fertigungsstraßen arbeiten.

Angegriffene Sicherheitssysteme können aber auch Verbraucher gefährden. Stellen Sie sich einmal die möglichen Auswirkungen eines Cyberangriffs vor, der Verfahrensabläufe in der Lebensmittel- oder pharmazeutischen Fertigung verändert. Dabei kann es zu schädlichen oder gar tödlichen Verunreinigungen kommen. Selbst wenn der Angriff bemerkt wird, bevor das jeweilige Produkt das Werk verlässt, könnte die Lieferung dringend benötigter Produkte wie z. B. lebenserhaltender Medikamente verzögert werden.

Hinzu kommt, dass manipulierte oder unterbrochene Prozesse in kritischen Infrastruktureinrichtungen verheerende Auswirkungen auf die Wasser- und Energieversorgung der Bevölkerung haben können.

„Hersteller und Distributoren in der Lebensmittel- und Getränkeindustrie setzen Steuerungssysteme ein, um Zutaten zu mischen, Produkte zu verpacken und Produkte für Konsumenten zu transportieren. Diese Systeme können manipuliert werden, um die Lebensmittelversorgung zu sabotieren oder eine Lebensmittelknappheit herbeizuführen."

Critical Control System Vulnerabilities Demonstrated And What to Do About Them, SANS Institute

Sicherheitsverstöße sind bereits Realität

Sicherheitsverstöße und Schwachstellen, die zu Sicherheitsrisiken führen, sind nicht nur theoretischer Natur. Sie sind bereits Realität:

- Ein Cyberangriff auf ein deutsches Stahlwerk führte zum Ausfall ganzer Systeme der Anlage und ein Hochofen konnte nicht mehr mit den üblichen Methoden heruntergefahren werden. Das Werk erlitt massive Schäden. Der Vorfall zeigt die destruktiven und potenziell schädlichen Auswirkungen, die Sicherheitsbedrohungen auf Industriebetriebe haben können.[1]
- Die FDA gab eine Warnung an Medizinprodukthersteller und Gesundheitseinrichtungen über die Anfälligkeit bestimmter medizinischer Geräte für Sicherheitsverletzungen heraus. Eine der genannten Schwachstellen bestand darin, dass die Geräte durch Malware infiziert oder deaktiviert werden könnten.[2]
- Verizon berichtete über eine mutmaßliche Verletzung der Cybersicherheit in einer Einrichtung zur Wasserversorgung und Messung des Wasserverbrauchs. Bei Verizon wurden unerklärliche Ventil- und Kanalbewegungen festgestellt, einschließlich der Manipulation von speicherprogrammierbaren Steuerungen zur Verwaltung der Menge an Chemikalien, die zur Trinkwasseraufbereitung eingesetzt werden.[3]
- Die Explosion einer Ölpipeline in der Türkei wurde von staatlicher Seite auf eine Fehlfunktion zurückgeführt, doch in den Nachrichten wurde gemeldet, dass dies das Werk von Hackern war. Die Explosion führte zum Auslaufen von 30 000 Barrels Öl. Nach Berichten von Bloomberg hatten Hacker die Alarmfunktionen abgeschaltet, die Kommunikation unterbrochen und das Erdöl in der Pipeline unter hohen Druck gesetzt.[4]

Hauptrisikotypen

Security-Risiken, die sicherheitsrelevante Auswirkungen haben, können in vielen verschiedenen Formen auftreten. Einige der Hauptrisikotypen sind:

Mitarbeiterfehler: Nicht immer steckt böse Absicht hinter Security-Risiken. Tatsächlich stellen unbeabsichtigte Fehler das häufigste Security-Risiko dar. Dabei sind es Mitarbeiter oder Auftragnehmer, die unwissentlich Fehlanschlüsse am Netzwerk vornehmen, das falsche Programm auf eine Steuerung laden oder ein infiziertes Gerät am System anschließen. Diese scheinbar kleinen Fehler können allerdings schwerwiegende Folgen haben, wenn sie dazu führen, dass Systeme abseits sicherer Parameter betrieben werden.

Verärgerte Mitarbeiter: Auch aktuelle oder frühere Mitarbeiter, die sich mit dem Steuerungssystem und dem industriellen Netzwerk eines Unternehmens auskennen, stellen eine Gefahr für die Sicherheit dar. Ein gutes Beispiel dafür ist ein Arbeitnehmer in Australien, der sich Zugang zum Steuerungssystem der Abwasseranlage seines früheren Arbeitgebers verschaffte und dafür sorgte, dass 800 000 Liter Rohabwasser in öffentliche Parks und Flüsse abgelassen wurde.[5]

Hacker mit politischen oder finanziellen Zielen: Das geistige Eigentum eines Herstellers kann ein lukratives Ziel für Hacker sein. Abgesehen davon versuchen Hacker, den Betrieb von Fertigungs- oder Industrieunternehmen aus finanziellen, Wettbewerbs- oder politischen Gründen zu stören.

Wirtschaftsspionage: Staatlich gelenkte Spionage, die auf wichtige Infrastruktur und Produktionsanlagen abzielt, stellt eine konstante Bedrohung dar. Beamte des US-amerikanischen Justizministeriums berichteten von zahlreichen Unternehmen, die das Ziel solcher Aktivitäten wurden. Für die nationale Sicherheit stellt dies eine ersthafte Bedrohung dar.[6]

Cyber-Terrorismus: Böswillige Handlungen können darauf ausgelegt sein, kritische Infrastruktureinrichtungen zu stören, zu infizieren oder lahmzulegen. Potenzielle Ziele sind Nuklearanlagen, Wasserversorgungen und Ölraffinerien. Bei einem dieser angeblichen Angriffe versuchten Hacker, einen Kleinstaudamm in New York unter ihre Kontrolle zu bringen. Der Angriff war jedoch erfolglos, weil der Damm für Wartungszwecke offline geschaltet war.[7]

Mit Security zu mehr Sicherheit

Regierungen, die besorgt über disruptive und gefährliche Angriffe auf die Cybersicherheit von Anlagen und kritischen Infrastrukturen sind, arbeiten bereits mit Herstellern und Industriebetrieben zusammen.

„Nahezu die Hälfte der befragten Sicherheitsfachkräfte glauben, dass es wahrscheinlich oder sehr wahrscheinlich ist, dass ein erfolgreicher Cyberangriff in den nächsten drei Jahren die Infrastruktur lahm legen und zu einem Verlust von Menschenleben führen wird."

Critical Infrastructure Readiness Report, The Aspen Institute and Intel Security, 2015

Das Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reagierte beispielsweise auf 295 Cybersicherheit-Zwischenfälle im Jahr 2015 in 16 kritischen Infrastruktursektoren.[8]

Die drei Sektoren, in denen es zu den meisten Vorfällen kam, waren:

- Kritische Fertigung (97 Vorfälle)
- Energie (46 Vorfälle)
- Wasser und Abwasser (25 Vorfälle)

Es bleibt jedoch weiterhin viel Arbeit. Unternehmen müssen bei der Gewährleistung von Sicherheit durch Security proaktiver vorgehen. Sie sollten vier Hauptelemente in ihre Strategie einarbeiten:

- Einhaltung von Standards
- Integration von Sicherheit und Security
- Risikoanalyse
- Maßnahmen zur Risikominderung

Eine Frage der Konformität

In den Sicherheitsstandards sind einige Anforderungen enthalten, um Hersteller und Industriebetriebe dabei zu unterstützen, Sicherheit durch Security zu erreichen:

- Abschnitt 7.4 der Norm **IEC 61508 („Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme")** leitet Unternehmen dazu an, eine Analyse der Sicherheitsbedrohung durchzuführen, wenn ihre Gefahrenanalyse eine absehbare „böswillige oder unbefugte Aktion" ergibt, die eine Sicherheitsbedrohung darstellt. Leider wird dieser Forderung selten Folge geleistet.
- Die zweite Ausgabe der Norm **IEC 61511 („Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie")**, die für 2016 geplant ist, fordert die Durchführung von Bewertungen des Security-Risikos bei Sicherheitssystemen (SIS). Das SIS muss so ausgelegt sein, dass die notwendige Ausfallsicherheit bei erkannten Security-Risiken gegeben ist.

Diese Anforderungen mögen nicht detailliert ausgearbeitet sein, doch sie bieten formale Compliance-Richtlinien für die Adressierung von Security-basierten Risiken. Es ist wichtig, sie zu befolgen. In der Zwischenzeit prüfen Normungsorganisationen zusätzliche Updates, die weiter ins Detail gehen könnten, um festzulegen, wie die Industrie Risiken bestimmen und Sicherheit durch Security gewährleisten muss.

Integration von Sicherheit und Security

Sicherheit und Security wurden traditionell als getrennte Einheiten betrachtet, es gibt jedoch Gemeinsamkeiten im Hinblick auf die angewandten Konzepte zur Analyse und Verminderung von Risiken.

Das Konzept der „Zugriffskontrolle" ist zum Beispiel bei Sicherheit und Security gleich. In beiden Fällen bauen Richtlinien und Verfahren auf Geschäftspraktiken, Risikomanagement-Ansätzen, Anwendungsanforderungen und Industriestandards auf. Beide zielen darauf ab, die Ressourcen eines Unternehmens zu schützen, d. h. Personen, Prozesse, Ausrüstung und geistiges Eigentum.

Wenn sie die Wahrscheinlichkeit von Security-basierten Zwischenfällen reduzieren wollen, werden Hersteller und Industriebetriebe das Thema Sicherheit neu überdenken müssen. Insbesondere ist ein Umdenken im Hinblick auf das Zusammenspiel von Sicherheit und Security erforderlich.

Um diesen Ansatz zu verstehen, sollten Unternehmen sich zuerst mit den „drei Cs der Sicherheit" auseinandersetzen. Es handelt sich hierbei um eine Reihe von Vorgehensweisen führender Hersteller:

- **Kultur (verhaltensorientiert):** Verhaltensweisen von Mitarbeitern und Unternehmen – wie Werte, Prioritäten, Einstellungen, Anreize und Überzeugungen – anhand derer definiert werden kann, in welchem Maße ein Unternehmen Sicherheitsstandards umsetzt.
- **Compliance (verfahrensorientiert):** Richtlinien und Verfahrensvorschriften, mit denen ein Unternehmen die Übereinstimmung mit den anwendbaren Sicherheitsnormen erreichen kann.
- **Kapital (technisch):** Moderne Sicherheitstechnologien und -techniken, die zur Optimierung von Sicherheit und Produktivität gleichermaßen beitragen.

Als Nächstes sollten Unternehmen sich darüber Gedanken machen, wie Security in jedem dieser Grundpfeiler für Sicherheit verankert werden kann. Beispiel:

Kultur: Zusätzlich zum Schutz des geistigen Eigentums, der Prozesse und der Anlagen, muss das Sicherheitspersonal den Schutz der Sicherheitssysteme in das Zentrum ihres Handelns stellen. Auch eine Ausweitung der Zusammenarbeit zwischen den Bereichen EHS (Sicherheit, Gesundheit und Umweltschutz), Operations und IT ist wichtiger denn je. Alle drei Teams sollten zum Beispiel bei der Entwicklung gemeinsam verwalteter Ziele für Sicherheit und Security und der Festlegung der Anforderungen für kritische Sicherheitsdaten von Produktionssystemen zusammenarbeiten. Nicht zuletzt bezieht eine starke Sicherheitskultur jeden einzelnen Mitarbeiter ein. Deshalb ist ein unternehmensweites Verständnis der Beziehung zwischen Security und Sicherheit notwendig.

Compliance: Compliance-Bemühungen sollten den in Sicherheitsnormen (beispielsweise IEC 61508 und 61511) festgelegten Security-Anforderungen entsprechen. Im Gegensatz dazu sollten alle Sicherheitsbemühungen einem Defense-in-Depth-Konzept folgen. Dies wird in der Normenreihe IEC 62443 („IT-Sicherheit für industrielle Automatisierungssysteme") (auch bekannt als ISA-99) und in anderen Regelwerken empfohlen. Sicherheitsbezogene Risiken sollten auf allen Ebenen einer Organisation adressiert werden.

Kapital: Unternehmen sollten Sicherheitstechnologien mit integrierten Sicherheitsfunktionen einsetzen. Darüber hinaus sollten Sicherheitstechnologien verwendet werden, die sowohl Schutz vor Sicherheitsverletzungen bieten als auch eine rasche Wiederherstellung nach einem Komplettausfall gewährleisten.

Umfassende Risikoanalyse

Unternehmen sollten eine unternehmensweite Risikomanagementstrategie umsetzen, um mit Sicherheitsbedrohungen und Schwachstellen sowie ihren potenziellen Auswirkungen auf die Sicherheit fertig zu werden. Bei dieser Strategie sind zwei Bewertungen unentbehrlich:

- Eine **Sicherheits-Risikobeurteilung** ist notwendig, um die Übereinstimmung mit bestehenden Sicherheitsnormen, wie z. B. den Sicherheitsanforderungen von IEC 61508 und 61511, zu bestätigen. Diese Beurteilung sollte sich nicht nur auf standardmäßige Bedienerfunktionen, sondern auf alle Mensch-Maschine-Interaktionen beziehen, wie Maschineneinrichtung, Wartung, Reinigung und Hygiene sowie Schulung und Administration. Unternehmen sollten ihre bestehenden Verfahren zur Durchführung von Sicherheitsrisikoanalysen um die Analyse der Risiken durch Cyberangriffe erweitern.
- Bei einer **Beurteilung des Security-Risikos** sollte der aktuelle Security-Zustand einer Organisation insgesamt dargelegt werden. Dazu gehören Software, Netzwerke, Steuerungssystem, Richtlinien und Verfahren sowie das Mitarbeiterverhalten. Auch die Maßnahmen zur Erreichung der gewünschten Sicherheitsebene sollten beschrieben werden.

Diese Bewertungen werden zwar getrennt voneinander durchgeführt, sie sollten jedoch auf Unternehmensebene in dieselben Risikomanagementziele zum Schutz von Mitarbeitern, Kunden und Umwelt einfließen.

Unternehmen, die Drittanbieter mit der Durchführung dieser Bewertungen beauftragen, sollten sich einen Anbieter mit guter Sachkenntnis in den Bereichen Sicherheit und Security suchen. So kann die Übereinstimmung und Harmonisierung beider Bewertungen sichergestellt werden.

Maßnahmen zur Risikominderung

Die jeweiligen Maßnahmen zur Risikominderung, die ein Unternehmen implementiert, hängen von den spezifischen Security-Risiken und den potenziellen Auswirkungen auf die Sicherheit ab. Es gibt jedoch einige zentrale Maßnahmen, die von den meisten Herstellern und Industriebetrieben als Best Practice umgesetzt werden sollten:

- **Segmentierung in Zonen:** Dies ist die wichtigste Best Practice im Hinblick auf Security. Die Segmentierung in Zonen sollte in jeder Anlage als Bestandteil eines ganzheitlichen Defense-in-Depth-Sicherheitskonzepts Anwendung finden, um den Zugriff auf Sicherheitssysteme zu begrenzen. Eine Industrial Demilitarized Zone (IDMZ) mit Firewalls und Data Brokern kann das werksweite Netzwerk sicher vom Unternehmensnetzwerk abgrenzen. Auch durch Verwendung virtueller LANs (VLAN) und einer Layer-2 oder Layer-3-Switch-Hierarchie können Funktionsunterbereiche erstellt werden, um so kleinere Vertrauensstufen einzurichten und die Durchsetzung von Sicherheitsrichtlinien zu erleichtern.
- **Physischer Zugang:** Viele Organisationen verwenden RFID-Karten für die Zutrittskontrolle in eine Einrichtung. Doch die Sicherung des physischen Zugangs sollte über den Schutz der Sicherheitssysteme hinausgehen. Es empfiehlt sich der Einsatz von Geräten zur Verriegelung (Lock-in) und Absperrung (Block-out), um ein unbefugtes Entfernen von Kabeln zu verhindern und nicht verwendete oder nicht benötigte Ports zu schließen. Darüber hinaus sollten Steuerschaltschränke verriegelt werden, um den Walk-up- und Plug-in-Zugriff auf industrielle Automatisierungs- und Steuerungsgeräte einzuschränken. Immer modernere Lösungen zur Sicherung des physischen Zugangs kommen auf den Markt, z. B. IP-Videoüberwachungssysteme, die Analytik zur Gesichtserkennung einsetzen.
- **Netzwerkintegrierte Sicherheit und Security:** CIP Safety™ und CIP Security™ sind Erweiterungen des Common Industrial Protocol (CIP) – dem Protokoll der Anwendungsebene für EtherNet/IP™. CIP Safety ermöglicht die Koexistenz von Sicherheitskomponenten und -systemen auf demselben EtherNet/IP-Netzwerk als Standardgeräte und ermöglicht ein sicheres Abschalten im Falle eines Denial-of-Service-Angriffs. CIP Security baut Datenintegrität und Vertraulichkeit in die EtherNet/IP-Kommunikation ein. Arbeiten Geräte, die mit CIP Safety und CIP Security ausgestattet sind, zusammen, bieten sie Schutz vor Datenkorruption und böswilligen Angriffen auf Sicherheitssysteme.

- **Sicherheitsprodukte mit integrierter Security:** Sicherheitssysteme und andere Hardware sollten über integrierte Security-Funktionen verfügen. Mit einer Sicherheitssteuerung, die codierte Software verwendet, kann beispielsweise sichergestellt werden, dass Firmware nur von einer vertrauenswürdigen Quelle heruntergeladen werden kann. Eine Zugangstür schränkt den physischen Zugang zur Steuerung ein. Ein industrieller Managed Switch mit Access Control Lists (ACL) dient ebenfalls dazu sicherzustellen, dass der Zugriff auf das Netzwerk nur durch autorisierte Geräte, Anwender und zugelassenen Datenverkehr erfolgen kann.
- **Authentifizierung und Autorisierung:** Über Security-Softwarefunktionen kann der kabelgebundene und kabellose Zugriff auf die Netzwerkinfrastruktur begrenzt werden. Security durch Authentifizierung und Autorisierung ist eine Schlüsselkomponente der Bedienerschnittstellen-Software und kann den Sicherheitssystemzugriff auf autorisierte Personen beschränken. Dies bietet Schutz vor böswilligen und unabsichtlichen internen Bedrohungen. Security-Mitarbeiter können definieren, ***wer*** Zugriff auf die Software hat, ***welche*** spezifischen Aktionen auf welcher Hardware ausgeführt werden dürfen und von ***wo*** aus diese Aktionen durchgeführt werden können.
- **Asset und Change Management:** Mit Asset Management-Software lässt sich die Erkennung neuer Ressourcen automatisieren und Konfigurationsänderungen können zentral über die gesamte Einrichtung hinweg und innerhalb der Sicherheitssysteme zurückverfolgt werden. Die Software erkennt böswillige Eingriffe in Echtzeit, protokolliert diese Aktivitäten und sendet Berichte an das zuständige Personal. Werden unerwünschte Änderungen vorgenommen, kann die Software auf archivierte Kopien eines Geräteprogramms zugreifen, um für eine schnelle Wiederherstellung zu sorgen.
- **Schwachstellen-Management:** Prozesse und Verfahrensvorschriften sollten entwickelt werden, um schnell auf die Veröffentlichung von Sicherheits- und Security-Mitteilungen reagieren zu können. Dies umfasst Vorgehensweisen zur unmittelbaren Sichtung von Meldungen und Ermittlung der möglichen Auswirkungen. Auch Verfahren zum Patch-Management betroffener Produkte zählen dazu.

Zusammenfassung:

Security bezieht sich nicht nur auf den Schutz von Daten und Betriebszeit. Security umfasst auch den Schutz von Personen und der Umwelt sowie den Schutz von Infrastruktur- und Versorgungseinrichtungen, von denen die Bevölkerung abhängig ist. Organisationen, die gegen diese Risiken gewappnet sein wollen, müssen für die Einhaltung der neuesten Standards sorgen, Sicherheit und Security ganzheitlich integrieren, eine umfassende Risikoanalyse durchführen und Maßnahmen zur Risikominderung unter Verwendung der neuesten Technologien umsetzen.

Ressourcen:

Rockwell Automation unterstützt Unternehmen bei ihren spezifischen Sicherheitsbelangen mit der richtigen Mischung aus Know-how zu den beiden Bereichen Sicherheit und Security. Wir bieten Ihnen ein in der Branche einmaliges Portfolio an Sicherheitslösungen, das auch Sicherheitsdienstleistungen wie beispielsweise Beurteilungen beinhaltet. Unser Angebotsspektrum für industrielle Sicherheit umfasst Netzwerkprodukte, kostenlose Tools und Ressourcen sowie eine große Bandbreite von Sicherheitsdienstleistungen. Für den Aufbau sicherer Systemen müssen auch sichere Produkten eingesetzt werden. Deshalb stellen wir mit unserem Entwicklungsprozess für zuverlässige Security-Lösungen sicher, dass Security von Anfang an in unsere Produkte integriert wird.

Wir arbeiten dabei auch eng mit strategischen Allianzpartnern wie Cisco, Panduit und Microsoft zusammen, um Ihnen industrielle Sicherheitslösungen aus einer Hand bieten zu können. Zum Beispiel entwickelten Cisco und Rockwell Automation gemeinsam ein Sicherheitsframework für industrielle Netzwerke im Rahmen des Converged Plantwide Ethernet (CPwE)-Programms. Über das CPwE-Programm sind auch Gestaltungsrichtlinien, Referenzarchitekturen und Schulungsressourcen erhältlich.

1) Hack attack causes 'massive damage' at steel works, BBC News, 22. Dezember 2014

2) Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication, FDA, 13. Juni 2013

3) Data Breach Digest, Verizon, 2016

4) Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar, Bloomberg, 10. Dezember 2014

5) Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australien, NIST, 23. Juli 2008

6) The Great Brain Robbery, 60 Minuten, 17. Januar 2016

7) U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam, New York Times, 24. März 2016

8) NCCIC/ICS-CERT Year in Review, ICS-CERT, 2015

www.rockwellautomation.com

Hauptverwaltung für Antriebs-, Steuerungs- und Informationslösungen

Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Naher Osten/Afrika: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asien/Australien/Pazifikraum: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, China, Tel: +852 2887 4788, Fax: +852 2508 1846

Deutschland: Rockwell Automation GmbH, Parsevalstraße 11, 40468 Düsseldorf, Tel: +49 (0)211 41553 0, Fax: +49 (0)211 41553 121
Schweiz: Rockwell Automation AG, Industriestrasse 20, CH-5001 Aarau, Tel: +41(62) 889 77 77, Fax: +41(62) 889 77 11, Customer Service – Tel: 0848 000 277
Österreich: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61

Publikation SAFETY-WP035A-DE-P – Dezember 2016