Sebastian Rohr

INDUSTRIAL IT SECURITY

EFFIZIENTER SCHUTZ VERNETZTER PRODUKTIONSLINIEN

Ein Fachbuch von

elektro technik
INDUSTRY OF THINGS
Security Insider

VOGEL COMMUNICATIONS GROUP

SIEMENS

Ingenuity for life

SIMATIC IOT2020

Ihr Vorsprung in der Bildung

Mit dem IOT2020 bietet Siemens eine Lösung für Open-Source-Anwendungen für Lehrende und Lernende im Bildungssektor an. SIMATIC IOT2020 ermöglicht Auszubildenden und Studierenden praxisnahe Erfahrungen mit Hochsprachenprogrammierung bis hin zu anspruchsvollen Projekten zu sammeln.

SIEMENS
Global Industry Partner of WorldSkills International

worldskills

siemens.de/sce/iot2020

Dipl.-Ing. Sebastian Rohr

Industrial IT Security

Effizienter Schutz vernetzter Produktionslinien

VOGEL COMMUNICATIONS GROUP

Dipl.-Ing. oec. Sebastian Rohr
2001 erhielt Sebastian Rohr seinen Abschluss als Wirtschaftsingenieur, Fachrichtung Produktionswirtschaft, an der TU Hamburg-Harburg. Über Stationen als Sicherheitsberater bei der Siemens AG, Forscher für Mobilfunk und Netzwerksicherheit am Fraunhofer Institut für Sichere Informationstechnik (SIT) sowie als Solution Strategist für die Sicherheitslösungen von CA (Computer Associates) kam Rohr als Chief Security Advisor zu Microsoft. Nach seiner Tätigkeit bei Microsoft gründete er die accessec GmbH und ist dort als Geschäftsführer aktiv. Seit 2017 ist er zusätzlich als CTO im Vorstand der APIIDA AG tätig, die er ebenfalls mitbegründete. Rohr ist Spezialist für IT- und Informationssicherheit mit besonderem Fokus auf Industrielle IT-Sicherheit und das Identity & Access Management. Zudem ist er Mitglied der ISACA, bei (ISC)2 sowie im TeleTrust e.V. und vertritt seine Unternehmen in den Branchenverbänden VDMA und Bitkom. Darüber hinaus ist er Referent und Schulungsleiter für diverse Organisationen und tritt bei zahlreichen Fachveranstaltungen als Moderator und Vortragsredner auf.

Weitere Informationen:
www.vogel-fachbuch.de
http://twitter.com/vogelfachbuch
www.facebook.com/vogel-fachbuch
www.vogel-fachbuch.de/rss/buch.rss_

ISBN 978-3-8343-3382-7
1. Auflage. 2019

Geleitworte

Wesentliche Änderungen in der industriellen Fertigung

Im Zeitalter einer globalen Digitalisierung ist die industrielle Fertigung von wesentlichen Änderungen betroffen. Der Begriff der 4. Industriellen Revolution (Industrie 4.0) umfasst nicht nur die Produktionstechnik, sondern auch die Unternehmensprozesse, die Organisation und natürlich den Menschen in seinem Arbeitsumfeld im Unternehmen. Die übergreifenden Änderungen der Unternehmensprozesse und der Wertschöpfung in einem Netzwerk statt in einer linearen Kette haben zur Folge, dass es einen durchgängigen Informationsfluss geben muss, der dabei helfen kann, die Anforderungen an neue Geschäftsmodelle umzusetzen. Als direkte Konsequenz dieser komplexeren Daten- und Informationsströme wird die bislang oft etablierte Sicht auf die Produktion als «Daten-Insel» innerhalb des Unternehmens sich hin entwickeln zu einer vermehrt unternehmensübergreifenden Kommunikation, die Fertigungsschritte in vielen Organisationen verbindet – insbesondere, wenn die vielfach propagierten selbst-organisierenden Wertschöpfungsnetze sich weitgehend autark anpassen sollen. Dieser vermehrte Bedarf nach Kommunikation hat direkte Auswirkungen auf die notwendigen Schutzmaßnahmen für IT, Produktion und Produktionsdaten. Ohne eine ausreichende Umsetzung dieser Security-Maßnahmen werden die vorgelegten Umsetzungskonzepte nicht realisierbar sein, da zu hohe Risiken für Manipulation an Prozessen, Daten und Maschinen und damit für die Produktionsmittel und Produkte entstehen.

Eine sichere Kommunikation basiert vor allem auf sicheren, vertrauenswürdigen Identitäten (für Mensch, Maschine, Produkte, zusammengefasst als «Industrial IAM») und verlässlichen Informationen zum Werkzeug und Werkstück (digitaler Zwilling). Dabei ist nicht nur eine sichere Technologie notwendig, sondern es ist besonders auf einen hohen Reifegrad der Organisationsprozesse und eine gute Aus- und Weiterbildung der Mitarbeiter zu achten. Nicht zuletzt muss das Unternehmen seine Produktion und deren IT-Komponenten auch im Rahmen eines umfassenden **I**nformations**s**icherheits-**M**anagement-**S**ystems (ISMS) abbilden.

Die bekannt gewordenen Angriffe auf Unternehmen haben Ziele, die von Wirtschaftsspionage bis zur Sabotage reichen – und viele der kolportierten Vorfälle konnten an den organisatorischen Grenzen weder erkannt noch gestoppt werden. Das Problem existiert folglich sowohl firmenintern als auch über die Unternehmensgrenzen hinweg. Hier wird deutlich, dass neben einer nach innen gewandten Sicht auch eine partnerschaftliche Zusammenarbeit mit der Lieferkette (neu: dem Liefer-Netzwerk) und/oder den Kunden(Unternehmen) erforderlich ist. Wie so oft beobachtet, attackieren die professionellen Angreifer die schwächsten Glieder der Kette – und diese können sich durchaus «jenseits des eigenen Vorgartens» befinden. Klare Absprachen zu Meldewegen und einheitliche sowie prüfbare Vorgaben zu Sicherheitsstandards sollten in der industriellen Produktion zum guten Ton gehören!

Neben dem Schutzziel der Verfügbarkeit der Produktion (Ausfallzeiten in der Fertigung) ist die Integrität der Daten wichtiger geworden (Produziere ich das qualitativ richtige Produkt für den Kunden?). Umso mehr gilt es, ein durchgehendes Security-Konzept zu etablieren, das einen hinreichenden Schutz gegen Angriffe ermöglicht und zudem wirtschaftlich tragbar ist. Das bedeutet, dass ein Unternehmen weiß, welche wichtigen Informationswerte (oder neudeutsch «Assets») es in der Produktion hat und wie diese durch das Security-Konzept zu schützen sind. Eine umfassende Risikoanalyse und Risikobewertung sind dabei die Basis für weitere Entwicklungen. Letztlich wird das Thema Resilienz in der IT-Sicherheit der Produktion an Bedeutung zunehmen, da eine Kompromittierung aufgrund der Komplexität nicht mehr ausgeschlossen

werden kann – eine 100%ige Sicherheit wird es auch in der Fertigung nie geben. Eine Anpassung an dieses neue Paradigma erfordert auch ein Umdenken bei der Gestaltung bzw. Fokussierung der Maßnahmen vom Vorbeugen (*prevent*) und Abwehren (*deter*) hin zum Erkennen (*detect*) und Eingrenzen (*contain*). Insgesamt bedeutet dies, die Organisation besser auf einen Ernstfall im Bereich der Cyber Security vorzubereiten und mehr Maßnahmen für die Erkennung von und Wiederherstellung nach solchen Incidents zu treffen.

Das vorliegende Buch ermöglicht sowohl Einsteigern in die Materie einen leichten Zugang und verschafft Orientierung, während Fortgeschrittene wertvolle Hinweise aus der Praxis zu vielen Themen wie etwa Verzeichnisdiensten und Netzwerkarchitektur erhalten. Auch der Exkurs zum Risikomanagement hilft dabei, die Anfangshürden zu überwinden und nutzbare Ergebnisse zu erzielen.

Dr. Ernst Esslinger
Abteilungsleiter der Abteilung «Methods / Tools Systems» bei der HOMAG GmbH

IT-Sicherheit als Führungsaufgabe

Chancen und Risiken fürs Unternehmen einzuschätzen und richtige Entscheidungen zu treffen gehört zu den Grundaufgaben eines Managers. Das fällt ihm nicht immer leicht, denn oft fehlen ihm dazu die nötigen Spezialkenntnisse. Ein Vertriebsmann wird sich vielleicht mit Fragen der Buchhaltung schwer tun – trotzdem muss er eine ordentliche Jahresplanung zustande bringen. Als Geschäftsführer wird er womöglich gezwungen sein, einem unehrlichen Buchhalter auf die Schliche zu kommen, weil er ja fürs gesamte Unternehmen verantwortlich ist und dafür sogar haftet. Freiberufler müssen ohnehin alles können, was sich nicht an Externe, zum Beispiel an den Steuerberater, abwälzen lässt.

Manager müssen also ohnehin ständig dazulernen, und zwar nicht immer Dinge, die ihnen liegen oder die ihnen sonderlich Spaß machen. So ein Thema ist zum Beispiel die IT-Sicherheit. Dabei geht es gar nicht darum, aus einem guten Kaufmann einen mittelmäßigen EDV-Techniker zu machen oder aus einem gelernten Betriebswirt einen Computer-Freak. Ein guter Manager muss heute allerdings wenigstens in der Lage sein, seinen eigenen IT-Fachleuten oder seinen externen Dienstleistern die richtigen Fragen zu stellen und sich auf diese Weise genügend Sicherheit zu verschaffen, um Entscheidungen zu treffen, die auf mehr als nur einem vagen Bauchgefühl basieren.

Vor allem muss der Manager oder Unternehmer imstande sein, das Risiko abzuschätzen, das er und seine Firma im Zeitalter des «Internet of Things» eingeht – einer Welt, in der alles mit allem verbunden sein wird – und infolgedessen riskiert, Opfer eines Cyberangriffs zu werden, der sozusagen die Kronjuwelen des Unternehmens bedroht – und damit seine Existenz!

Es wäre logisch anzunehmen, dass Führungskräfte hier ebenso sorgfältig zu Werke gehen, wie sie es in anderen Bereichen zu tun gewohnt sind. Jeder gute Manager versucht doch, sein Risiko bei Wechselkursen, Insolvenzen oder Lagerhaltung durch intelligentes Risikomanagement möglichst gering zu halten. Man sollte also meinen, dass dieses kleine Einmaleins des verantwortungsbewussten und vorausschauenden Wirtschaftens auch in der IT genauso eingesetzt wird.

Leider sieht es in der Praxis bis heute aber ganz anders aus. Im Juni 2017 stellte die Hamburger Unternehmensberatung Sopra Steria Consulting nach der Befragung von mehr als 500 Führungskräften aus den Branchen Banken, Versicherungen, Sonstige Finanzdienstleister, Energieversorger, Automotive, Sonstiges verarbeitendes Gewerbe, Telekommunikation und Medien sowie öffentliche Verwaltung ernüchtert fest: «Der harmlose Umgang in den Chefetagen bleibt ein

Problem!» Demnach kümmern sich nur 46 Prozent der Firmen regelmäßig darum, dass alle Mitarbeiter über die Gefahren der IT-Sicherheit aufgeklärt werden. 21 Prozent konzentrieren ihre Maßnahmen nur auf die Mitarbeiter in der IT-Abteilung.

Nicht, dass den Managern hierzulande nicht klar wäre, was für einen wilden Ritt sie da hinlegen. Im Juli 2017 veröffentlichte das Analystenunternehmen Thales eine Studie, in der der Frage nachgegangen wurde, wie deutsche Manager selbst den Stand der Sicherheitsmaßnahmen ihrer IT beurteilen. 95 Prozent gaben an, nicht ausreichend gegen Cyberangriffe geschützt zu sein. 45 Prozent meinten sogar, dass die Sicherheit ihrer IT sehr oder extrem anfällig sei. Damit liegen die Deutschen im internationalen Vergleich übrigens auf Platz 1: In keinem anderen Land glauben Manager, dass ihre IT-Systeme so schlecht geschützt sind wie hier. Und das Problem wird immer schlimmer: Im Vorjahr waren nur 90 Prozent der Ansicht, sie seien nicht ausreichend geschützt.

Sicherheit mit Konzept

Die Reaktion der meisten nichttechnischen Führungskräfte ist es, in dieser Situation in noch mehr Technik zu investieren. 2017 stiegen laut Thales derartige Investitionen um 80 Prozent gegenüber dem Vorjahr. Im Geldausgeben für IT-Sicherheit sind die Deutschen inzwischen Weltmeister!

Aber IT-Sicherheit ist keine Frage der Technik, oder zumindest nicht in erster Linie. Natürlich müssen Systeme geschützt sein, denn die Gegenseite rüstet ja auch ständig auf. Es wäre aber ein Irrtum zu glauben, dass man sich nur hinter die Burgmauern seiner Firewall zurückziehen muss, und schon wäre das Problem gelöst.

Worum geht es bei IT-Sicherheit wirklich? Nicht um den Schutz der Systeme selbst, sondern um den Schutz der Informationen, die darin gespeichert liegen und die von ihnen ständig verarbeitet werden. Daten sind das Erdöl des 21sten Jahrhunderts, und Informationen sind ein wichtiger Teil des Betriebsvermögens! Da Informationen im Unternehmen hin und her wandern und im Zeitalter von IoT auch bis weit über die Unternehmensgrenzen hinaus, gibt es nur einen Weg, sie wirklich wirkungsvoll und dauerhaft zu schützen: Es muss ganz klar festgelegt sein, wem welche Daten «gehören» und wo die Verantwortung für sie liegt. Auch in diesem Punkt ist Sicherheit mit jedem anderen Geschäftsvorgang innerhalb eines Unternehmens vergleichbar. Die Zuständigkeit kann im Einzelfall delegiert werden, so wie der Finanzvorstand eines Unternehmens seine Verantwortung zum Beispiel für das Rechnungswesen an einen Buchhalter abgeben kann. Es muss aber jederzeit klar sein, wer welche Daten wofür verwenden kann. Und es muss klar zurückverfolgbar sein, wer wann was mit den Daten gemacht hat. Und hier wird modernes ***I****dentity and* ***A****ccess* ***M****anagement* (IAM) in Zukunft eine zentrale Rolle spielen.

Das Delegieren von Sicherheitsaufgaben ist leider nicht ganz so einfach, denn Daten verändern sich auf dem Gang durch die Unternehmensinstanzen. Es ist deshalb ganz wichtig festzulegen, wer zu welchem Zeitpunkt die Verantwortung für die Korrektheit der Informationen trägt.

Doch was heißt schon «korrekt»? Damit Informationen im Unternehmen eingesetzt werden können, müssen sie nämlich fünf durchaus unterschiedliche Anforderungen erfüllen:

Unversehrtheit: Daten dürfen nur im Rahmen genau definierter Geschäftsprozesse verändert werden. Die Veränderungen müssen autorisiert und nachvollziehbar sein. Manipulierte oder manipulierbare Daten sind praktisch wertlos. Gerade im Online-Zeitalter ist die Integrität von Daten aber ein Problem. Im Internet gibt es keine Gewissheit, dass eine empfangene Nachricht mit der gesendeten identisch ist, da sie ein Netzwerk mit Millionen angeschlossener Computer durchläuft. Jeder kann dabei potenziell Änderungen durchgeführt haben.

Vertraulichkeit: Der Zugriff auf Firmendaten muss auf denjenigen Personenkreis beschränkt bleiben, der von Verantwortlichen bestimmt worden ist. Jeder nachgewiesene Zugriff von

Fremden auf Firmendaten muss sofort Zweifel an deren Unversehrtheit und entsprechende Überprüfungsmechanismen auslösen. Im Internet ist Vertraulichkeit ein Problem, weil das verwendete Übertragungsprotokoll TCP / IP vor allem auf Fehlertoleranz hin entwickelt wurde. An Abhörsicherheit dachte damals niemand. Vertraulichkeit muss deshalb heute durch Verschlüsselung sozusagen nachträglich hergestellt werden.

Verfügbarkeit: Daten, auf die nicht (oder nicht mehr) zugegriffen werden kann, sind für das Unternehmen wertlos. Das mag banal klingen, aber angesichts der Sorglosigkeit in vielen Unternehmen gegenüber dem Thema Sicherheitskopien und Backup-Strategien kann es sich schnell zum Problem auswachsen.

Authentizität: Es ist schwer, zweifelsfrei festzustellen, wer eine fragliche Information in einem Computersystem tatsächlich erzeugt oder verändert hat. Beim Datenaustausch per Internet potenziert sich das Problem, denn die Beteiligten können sich ja nicht sehen und kennen sich im Zweifelsfall auch nicht gegenseitig. Es geht also nicht nur darum zu verhindern, dass irgendjemand beim Datenaustausch unerkannt «mithört», sondern darum: Wie stelle ich fest, dass sich mein Computer wirklich mit dem richtigen Partner unterhält?

Verbindlichkeit: Keiner der Beteiligten soll bestreiten können, dass eine Übertragung stattgefunden hat. Im Internet kann jeder behaupten, eine Nachricht nicht erhalten zu haben. Umgekehrt kann jeder behaupten, eine bestimmte Nachricht nicht geschickt zu haben. Beweisbar ist nichts. Industrie und Wissenschaft haben verschiedene Verfahren entwickelt, um die Sicherheit unter den oben aufgeführten Aspekten bei der Nachrichtenübermittlung im Internet zu gewährleisten. Das bekannteste Verfahren ist ein sogenannter digitaler Zeitstempel, der nachweisbar nicht nur die Authentizität des Absenders, sondern auch den Absendezeitpunkt dokumentieren soll. Daneben gibt es die Einrichtung der «digitalen Signatur», deren praktischer Einsatz aber noch ganz am Anfang steht.

In diesem Buch geht es immer wieder auch um IAM und seine Anwendung im Unternehmen. Mein Freund Sebastian Rohr ist ja auch ein ausgewiesener Experte auf diesem Gebiet. Es geht aber auch um die Frage, wie sich IT-Sicherheit so organisieren lässt, dass der Manager wieder nachts schlafen kann. Es ist deshalb ein wichtiges Buch – aber es ist nur ein Anfang. Bis IT-Sicherheit ebenso zum Basisrepertoire deutscher Führungskräfte gehört, mit dem sie so zielsicher und vorausblickend umgehen können wie mit allen anderen Bereichen, in denen sie Verantwortung tragen, braucht es einen Kulturwandel. Und der ist, wie jeder weiß, viel schwerer zu bewerkstelligen als der rein technische Wandel.

Wenn Deutschland die Digitale Transformation und den Einstieg in die Welt der totalen Vernetzung meistern soll, führt allerdings kein Weg daran vorbei.

Tim Cole
Internet-Publizist, Kolumnist und Autor

Vorwort

Industrial IT Security ist ein weites Feld, das man einerseits nicht mit Samthandschuhen anfassen darf, weil schon viel zu lange auf IT-Sicherheit in der Fertigung verzichtet wurde. Andererseits sind besondere Vorsicht und Achtsamkeit geboten, da unbedachte Handlungen schnell das Schutzziel der Verfügbarkeit gefährden könnten. Es sind also Taten gefragt, die mit Sinn und Sachverstand geplant und umgesetzt werden. Deren oberstes Ziel muss es sein, die Stabilität der IT in den Produktionsanlagen zu sichern und die IT vor Schadwirkung durch Angreifer zu schützen. Dazu gehört in erster Linie die Erkenntnis, dass wir alle künftig in einer vernetzten Welt leben werden, die leider auch neue Gefahren mit sich bringt.

Diesen Gefahren sollte mit der Identifikation und Umsetzung von nachhaltig wirksamen Lösungen und Methoden begegnet werden. Jene müssen die Industrial IT schützen – ohne die Produktion an sich zu beeinträchtigen. Mit diesem Buch möchte ich das Bewusstsein schärfen, dass Schnellschüsse und eine Insel-orientierte Herangehensweise – wie sie heute noch in vielen Industrieunternehmen häufig auf der Tagesordnung stehen – den Cyberattacken von morgen nicht standhalten werden. Sicher ist auch: Es gibt nicht *den einen* Königsweg. Es werden immer mehrere, individuell passende und aufeinander abgestimmte Sicherheitsmaßnahmen erforderlich sein, die in Zeiten des digitalen Wandels Zukunftssicherheit schaffen. Ich freue mich, wenn ich meinen Lesern mit diesem Buch auf dem Weg zu *ihrer* Lösungsfindung ein Stück Orientierung und die Möglichkeit einer ersten Selbsteinschätzung geben kann, um die wichtigen ersten Schritte hin zu einer eigenen Industrial-IT-Security-Strategie erfolgreich meistern zu können.

Dass dieses Buch entstanden ist, verdanke ich einer ganzen Reihe von Menschen. Meinen besonderen Dank spreche ich aber meiner Frau und meiner Tochter aus, die selbst nach langen Tagen im Büro und auf Dienstreisen akzeptiert haben, dass ich in meiner Dachstube an diesem Buch weitergearbeitet habe. Danken möchte ich auch der Vielzahl an liebgewonnenen Kollegen und Freunden aus dem Volkswagen-Konzern, wie zum Beispiel Michael Sander, Hans-Werner «Hansi» Vogel, Michael Schweiger, René Puppe von Volkswagen Nutzfahrzeuge, Yvonne Mihaylov aus dem Werk Emden und den vielen Instandhaltern und Sicherheitsexperten der Audi AG, von Skoda, MAN Truck & Bus sowie den Produktions-IT-Experten des VDMA für ihre Expertise und Unterstützung. Hervorzuheben ist auch das besondere Engagement von Michael Jochem von Bosch, Ernst Esslinger von der Homag-Gruppe, Tim Cole, Steve Kolumbus und Jörg Ringmeir von Hirschvogel, Thorsten Hamers von Trützschler sowie den unzähligen Kollegen von Phoenix Contact, der Siemens AG, Bosch und Bosch Rexroth sowie der Nobilia und natürlich Herrn Dr. Detlef Houdeau von Infineon. Die Experten des GA5.22 unter Leitung von Heiko Adamczyk haben ebenfalls ihren Anteil an dem Gelingen dieses Buches, ebenso wie die Mitglieder der AG «Sicherheit vernetzter Systeme» der Plattform I4.0. Ihnen allen danke ich recht herzlich. Last but not least gilt mein Dank auch meinem Team der accessec GmbH, Nadine Sinner, Caleb Ketcha, Iratxe Garrido, Sven Feuchtmüller, Janis Kinast, Valdet Camaj, Young-Hwan Kim, Laura-Ann Hauger, Vladimir Stefanov, meinen Gründungspartnern Stefan Schaffner und Claus Mink – ohne ihre Unterstützung und Entlastung wäre dieses Projekt nie zustande gekommen!

Für den letzten Schliff am Inhalt danke ich der Vogel Communications Group, meiner Lektorin und meinem PR-Team der Fuchskonzept GmbH, die mich immer wieder motiviert und angespornt haben – DANKE!

Sebastian Rohr

Der **Onlineservice** InfoClick bietet unter https://vogel-fachbuch.de/infoclick/ nach Codeeingabe zusätzliche Informationen und Aktualisierungen zu diesem Buch.

InfoClick

In 2 Schritten zum Onlineservice

1. Einfach https://vogel-fachbuch.de/infoclick/ aufrufen.
2. Den unten stehenden Zugangscode in die Suchleiste eingeben und bestätigen.

   Sofern Aktualisierungen oder Zusatzinformationen zu Ihrem Buch bereitstehen, werden diese anschließend unterhalb der Eingabemaske aufgeführt.

Ihr persönlicher Zugang zum Onlineservice ⇨ 338200870001

Inhaltsverzeichnis

1 Einleitung

Spätestens seit den Medienberichten im Jahr 2010 über die sogenannten «Stuxnet»- Angriffe auf iranische Atomanlagen und die erfolgreiche Manipulation eines deutschen Hochofens zur Stahlerzeugung im Jahr 2014 reifte in der Fachwelt die Erkenntnis heran, dass die vormals abgeschottete Automatisierungstechnik in der heutigen Welt des «Internet der Dinge» vernetzt, erreichbar und somit angreifbar geworden ist. Weitere ausgefeilte Angriffe über neuere Ausspäh-Malware wie Havex (2014) und den «Industroyer», der von der Firma ESET im Zusammenhang mit dem Zusammenbruch des Stromnetzes in der Ukraine gebracht wurde, steigerten die Aufmerksamkeit der Verantwortlichen. Im Jahr 2016 wurde auf der BlackHat Asia dann ein experimenteller Wurm namens «PLC-Blaster» vorgestellt, der sich nur auf Siemens S7 vermehrt und ganze Netzwerke lahmlegen konnte. Im Sommer 2018 warnte das ***B****undesamt für* ***S****icherheit in der* ***I****nformationstechnik* (BSI) dann öffentlich, dass die Unternehmen der Energiewirtschaft in Deutschland massiven Angriffen ausgesetzt seien, aber bisher noch keine kritischen Infrastrukturen betroffen wären, sondern lediglich deren Büro-Netzwerke.

Parallel zu den erschreckenden Erkenntnissen über die mangelnde Sicherheit der ICS-/SCADA-Systeme in Produktionsnetzen hat der zunehmende Einsatz von Standard-Informationstechnologie in Produktion, Fertigung und Entwicklung zur Prägung des Begriffs der «Industrial IT» für eben diese nun angreifbaren Systeme geführt, der in klarer Abgrenzung zur «klassischen» Office IT steht. Diese Abgrenzung im Rahmen dieser Einleitung ist wesentlich, denn einer der Kardinalsfehler früher Bemühungen zu mehr (IT-) Sicherheit für Produktionsanlagen war es, die für die Bürokommunikation erstellten Regeln und Technologien unverändert in der Produktion umzusetzen.

Je nach Reifegrad der eigenen Sicherheitsorganisation sowie deren Prozesse und dem generellen Stellenwert der Informationssicherheit im Unternehmen haben sowohl große Konzerne als auch kleine und mittelständische Unternehmen erheblichen Nachholbedarf bei der Bestimmung der eigenen Gefährdungslage, der Exposition kritischer Anlagen, Maschinen oder Produktionsprozesse, der Einschätzung des eigenen Risikopotenzials und der gezielten Bedarfsanalyse für Gegenmaßnahmen. Selbst solche Organisationen, die durch aufgedeckte Angriffe eine hohe Sensibilität für den gesamten Themenkomplex haben, kämpfen mit der Unterscheidung zwischen wirklich nachhaltig sinnvollen und nur kurzfristig medienwirksamen Maßnahmen. Das vorliegende Buch soll auf der einen Seite das notwendige Problembewusstsein schaffen – und auf der anderen Seite sowohl Orientierung geben als auch eine bessere Selbsteinschätzung ermöglichen. Ein Weg dorthin kann über die Anwendung bekannter Ansätze wie etwa des «AKV-Dreiecks» aus der engen Verknüpfung von Aufgaben, Kompetenzen und Verantwortlichkeiten sowie der aus dem Qualitätsmanagement bekannten kontinuierlichen Verbesserungsprozesse (KVP) mit der wiederkehrenden Bewertung der eigenen Risikosituation führen. Eine wichtige Erkenntnis dieses Buches soll es daher sein, dass viele Wege zu einer Verbesserung der IT-Sicherheit in der Produktion führen können – wenn der hierfür notwendige Wandel unter Zuhilfenahme von im Unternehmen bekannten Methoden und Werkzeugen gelingt. Dass diese Aussage mehr ist als eine These, zeigt an geeigneter Stelle ein prägnantes Beispiel einer Adaption der FMEA-Methodik bei der Risikobewertung.

1.1 Zweck und Zielgruppe

Da nach Erkenntnissen des Autors in vielen Organisationen weder die Rolle eines «Production Security Officers» oder «Automation Security Officers» bekannt oder gar besetzt ist, sollten zu-