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

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-

mindest der oftmals etablierte (Chief) Information Security Officer (CISO) und vor allem IT-affine Instandhalter, Inbetriebnehmer sowie Lieferanten von Automatisierungstechnik dieses Werk lesen. Im Grunde sollte jeder mit der Produktion direkt oder indirekt befasste Mitarbeiter – vom auszubildenden Mechatroniker über den Maschinenbauer und Techniker bis hin zum Ingenieur für Automatisierungstechnik – «seinen» Zugang zu diesem wichtigen und zukunftsbestimmenden Thema finden. Dieses Buch soll deshalb auch einen Beitrag zur fachübergreifenden Kommunikation zwischen diesen Personen leisten und für mehr gegenseitiges Verständnis der Beteiligten werben.

1.2 Aufbau des Buches

Der Einstieg in die Thematik erfolgt nach Abschluss dieser Einleitung im nichttechnischen respektive soziotechnischen Bereich der Organisation, der Prozesse und Abläufe der Industrial IT Security. Hier werden insbesondere der stetige Fortbildungsbedarf und die Notwendigkeit zur Anpassung von organisatorischen Strukturen adressiert, ohne die eine sichere IT für Produktionsanlagen unmöglich ist.

Im Fokus stehen dabei insbesondere die Risikomanagement-Ansätze, die nur ganzheitlich betrachtet einen wirklichen Mehrwert liefern können (Kapitel 8).

Als erster technisch geprägter Abschnitt führt Kapitel 3 in automatisierte Produktionssysteme und Anlagen ein, die zusammen mit mehr und mehr an Office IT angelehnten Client-Rechnern die Basis für die vernetzte Produktion stellen. Neben einem kurzen Blick auf Whitelisting-Lösungen wird vor allem der Blick für die Dokumentation und die Gesamtsicht der Produktions-IT geschärft – frei nach dem Motto: Man kann nur managen, was man auch kennt!

Kapitel 4 thematisiert dann konkret die übergreifende Vernetzung der Produktion und welche Maßnahmen zur Netzsegmentierung sinnvoll umgesetzt werden können, um gezielt Bedrohungspotenziale zu reduzieren. Hierbei kommt dem Abschnitt «Remote Access» eine besondere Bedeutung zu.

Das fünfte Kapitel gibt eine Einführung in die Sicherheit von SCADA/ICS-Komponenten (***S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition / **I**ndustrial **C**ontrol **S**ystems*). Es sei erwähnt, dass die Sicherheit dieser Systeme in den vergangenen Jahren durch die Hersteller verbessert wurde, aber weiterhin ein hoher Bedarf für die Absicherung der Bestandssysteme erkennbar ist. Hier sind vor allem Instandhaltung und Automatisierungsspezialisten gefragt.

Insbesondere vor dem Hintergrund eines hohen Bedarfs für die Verwaltung von Assets, Personen und Berechtigungen diskutiert der Autor in Kapitel 6 Verzeichnisdienste und ihre Eignung und Mehrwerte für den Einsatz in Produktionsanlagen. Der Fokus in diesem Kapitel liegt auf dem Einsatz von Microsoft-Active-Directory-Technologien.

Kapitel 7 gibt einen Überblick zur Sicherheit von industriellen Softwareprodukten und Anwendungen und stellt Auswahlkriterien und Hinweise zur Beschaffung und Entwicklung eigener Software bereit. Abschließend werden in diesem Kapitel auch beispielhafte Anwendungsszenarien und besondere Herausforderungen für das Management der Industrial IT und ihrer Sicherheitsrisiken dargestellt. Kapitel 7 betrachtet Besonderheiten und Ausnahmefälle in der Industrial IT, wie sie etwa durch die Safety-Zertifizierungen und die Abnahmen sowie die in der Vergangenheit üblichen Verbote von Änderungen an abgenommenen Systemen entstanden sind.

Das Risikomanagement wird dann in Kapitel 8 im Rahmen einer Einführung thematisiert, um einen Einstieg zu ermöglichen. Für weitergehende Ausführungen empfiehlt sich die umfangreiche Fachliteratur zum Thema Enterprise Risk Management und ein Blick in die Standards

der IEC 62 443 sowie der ISO 27 000 für die Umsetzung im Rahmen eines Informationssicherheits-Management Systems.

Das im Jahr 2018 nahezu allgegenwärtige Thema Industrie 4.0 wird im abschließenden Kapitel 9 kurz umrissen, und einige Highlights und neuere Erkenntnisse der Plattform Industrie 4.0, der Verbände Bitkom, VDMA und ZVEI sowie aus dem Forschungsprojekt IUNO des BMBF, an dem der Autor beteiligt war, finden hier Einfluss.

1.3 Abgrenzung

Einige der folgenden Kapitel beschreiben konkrete technische Ansätze, deren Wirksamkeit und Sinnhaftigkeit in Abhängigkeit von Branche, Größe und Maturität der betreffenden Organisation jedoch stark differieren kann. Eine Reihe der organisatorischen Hinweise und Forderungen sind durch die damit verbundenen Personalkosten nur bedingt in kleinen oder mittelständischen Unternehmen anwendbar. Der Leser ist dennoch eingeladen, sich von den teilweise recht konkret vorgestellten Beispielen inspirieren zu lassen und die Anwendbarkeit und Zielführung der beschriebenen Maßnahmen für die eigene Organisation zu prüfen. Auch gibt der Autor zu bedenken, dass die Umsetzung rein technischer Lösungen oder der Kauf von Produkten im Schnellverfahren oftmals ihre Wirkung verfehlen, wenn die begleitenden Prozesse nicht optimal ausgerichtet sind, keine Verantwortlichkeiten benannt und Aufgaben zusammen mit den entsprechenden Kompetenzen verteilt werden. Die Schlüsselposition nehmen hier erneut befähigte, motivierte und engagierte Mitarbeiter ein, die über Schulungen das notwendige Wissen vermittelt bekommen, in Labors und Testumgebungen ihre Kenntnisse erweitern und im Anschluss in funktional übergreifend arbeitenden Teams ihr Wissen mit anderen Fachbereichen, Standorten und Funktionen teilen. Der beste Schutz vor erfolgreichen Angriffen auf die Industrial IT sind und bleiben nun einmal das Wissen und die Erfahrungen derjenigen, die die Systeme planen, akquirieren, installieren, integrieren und bis zu ihrer Abschaltung instand halten und betreiben. Dieses relevante Wissen in einem notwendigen Maße zu teilen, schafft die Basis für ein tiefes IT-Sicherheitsverständnis der Mitarbeiter in einer Organisation.

2 Organisationsanforderungen für den Aufbau einer Industrial IT Security

Die größte auf Produktionsanlagen der Industrial IT Security übertragbare Erkenntnis der IT-Sicherheit der vergangenen 20 Jahre ist wahrscheinlich die, dass die Bemühung um mehr Sicherheit eher einer Reise gleicht als einem Ziel – wobei sich den längerfristig mit IT-Sicherheit befassten Experten in der Regel schnell zeigt, dass sich selbst das Ziel dieser Reise ständig ändert. Hieraus abzuleiten, dass das Erreichen von mehr Sicherheit einer Reise ohne Ziel gleicht, verfehlt die Realität jedoch deutlich. Vielmehr muss derjenige (oder diejenigen, falls es eine Gruppe ist), der für mehr IT-Sicherheit im Unternehmen die Verantwortung trägt, seine Bemühungen so weit wie möglich an der IT-Strategie des Unternehmens ausrichten. Folglich muss auch der Zielkanon der Informationssicherheit einer Organisation an ihren strategischen Zielen ausgerichtet sein. Oder kurz: Die Unternehmensstrategie setzt Ziele und Rahmen für die Informationssicherheits-Strategie und die IT-Strategie. Die Ziele der IT und der Informationssicherheit bereiten wiederum den Rahmen für die Ziele der Industrial IT und der IT-Sicherheit im Unternehmen.

TIPP

Eine genauere Erklärung zum direkten Zusammenhang und zur Ableitung von fest zuordenbaren Sicherheitszielen und deren Ableitung aus den Unternehmenszielen bieten die SABSA®-Kurse zur Sicherheitsarchitektur.

Wer sich der Informationssicherheit aus Sicht der Auditoren nähern will, dem sei die Fortbildung zum ***C****ertified* ***I****nformation* ***S****ystems* ***A****uditor* (CISA) empfohlen – wer eher die Sicht des internen Planers für Informationssicherheit einnehmen möchte, dem sei der ***C****ertified* ***I****nformation* ***S****ecurity* ***M****anager* (CISM) – beides Angebote der ISACA – nahegelegt. Eher technisch orientierte Personen werden durch den ***C****ertified* ***I****nformation* ***S****ystem* ***S****ecurity* ***P****rofessional* (CISSP) der $(ISC)^2$ oder die einschlägigen Fortbildungen von SANS oder etwa des VDI-Wissensforums bedient.

Sich mit den Zusammenhängen und Einflussfaktoren im Feld der IT-Sicherheit zu befassen, ist längst keine Kür mehr, sondern eine Pflicht geworden. Immerhin stellt die globalisierte Welt nahezu alle Organisationen vor bisher ungeahnte Herausforderungen, was die Adaption an die sich immer schneller verändernde Umwelt und die globalgeografisch «regionalen» Märkte angeht. Infolge dessen müssen sie in immer schnellerer Abfolge ihre Strategie anpassen. Und dies hat im Bereich der Informationstechnologie mit Verbreitung des Internets, der mobilen Revolution, der eintretenden digitalen Transformation und der Schaffung des Internets der Dinge (***I****nternet* ***o****f* ***T****hings*, IoT) erhebliche Auswirkungen auf die Dynamik der (Industrial) IT.

Hier als CISO oder Sicherheitsverantwortlicher Schritt halten zu können, erfordert neben persönlichen Fähigkeiten und umfangreichem Wissen und Erfahrungen auch ein hohes Maß an Adaptionsfähigkeit, persönlicher Lernbereitschaft sowie ein ebenso adaptives Netz abgestimmter Prozesse, die diesen schnellen Wandel abfedern und in geordnete Bahnen lenken. Dieses einführende Kapitel beschreibt die Anforderungen an ein Prozessgeflecht der Informationssicherheit für die Industrial IT und zeigt auf, an welchen Stellen die «etablierten» Prozesse und Regelungen der Office IT nicht auf die Industrial IT übertragbar sind und folglich angepasst oder gar neu definiert werden müssen.

Um IT-Sicherheitsprozesse für diese komplexe Umgebung erfolgreich planen, umsetzen und aufrechterhalten zu können, muss eine geeignete Organisationsstruktur für die Informationssicherheit vorhanden sein. Es bedarf also der Definition von Rollen, die die verschiedenen Aufgaben für die Erreichung der im Vorfeld vereinbarten Sicherheitsziele wahrnehmen. Außerdem müssen Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen.

Die bereits in Abschnitt 1.1 dargestellten Unterschiede zwischen Office IT und Produktion führen dazu, dass auch das Informationssicherheits-Management (ISMS) für die Produktion sich vom ISMS der Office-Welt unterscheidet. Um diese Abweichungen jedoch sinnvoll einordnen zu können, werden im folgenden Abschnitt zunächst die Unterschiede zwischen Office IT und Industrial IT herausgearbeitet.

DEFINITION

ISMS = **I**nformations**s**icherheits-**M**anagement-**S**ystem; Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

2.1 Abgrenzung Office IT–Produktion

Die größten Abweichungen zwischen Office und Produktion ergeben sich durch die Rahmenbedingungen, wie beispielsweise:

- Die hohen Verfügbarkeitsanforderungen der Produktion erschweren das in der Office IT übliche Einspielen von Updates, falls diese nicht durch Vorgaben der Lieferanten oder Hersteller zu Garantie und Gewährleistung ausgeschlossen sind;
- die lange Lebensdauer von Produktionsanlagen im Vergleich zur Office IT;
- mangelnde Berücksichtigung der IT Security und Informationssicherheit bei der Konzeption der eingesetzten Systeme, Protokolle und Technologien;
- mangelnde (Sicherheits-) Vorgaben für Genehmigungen und Betrieb der Anlagen oder Komponenten;
- Zielkonflikte zwischen Safety und Security – «abgenommene Anlagen» können bzw. sollen nicht durch Software Updates verändert werden.

Begrifflichkeiten und Bezeichnungen

Neben der eher übergeordneten Bezeichnung der Industrial IT haben sich Begriffe wie Shopfloor IT (für IT-Komponenten «in der Werkhalle» – oder auf Englisch «*on the shopfloor*») und «***O**perational **T**echnology*» (OT) etabliert. Die Abkürzung «OT» wird in Anlehnung an und als Abgrenzung zu «IT» gerne auch im Umfeld des Internet der Dinge (Internet of Things, IoT) verwendet und bei einer Gegenüberstellung der Bereiche als «IT / OT genutzt. Es bleibt abzuwarten, ob sich einer dieser Begriffe durchsetzen wird und ob sich zwischen ihnen eine Hierarchie etabliert.

Ein Kernpunkt der IT-Sicherheit und der Informationssicherheit wird durch die sogenannten Schutzziele gebildet. Aus dem Englischen abgeleitet, wird dabei oft von der sogenannten «CIA-Triade» gesprochen, die aus ***C**onfidentiality* (Vertraulichkeit), ***A**vailability* (Verfügbarkeit) und ***I**ntegrity* (Integrität) gebildet wird. Dazu werden ergänzend *Authenticity* (Authentizität) und

Non-Repudiation (Nicht-Abstreitbarkeit) genannt, die in einigen Standardwerken als gleichberechtigte Schutzziele genannt werden. Zu beachten ist, dass die im Office-Netz nahezu immer zuerst genannte Vertraulichkeit in den allermeisten Produktionsanlagen eine eher untergeordnete Rolle spielt. Die Produktion setzt – verständlicherweise, bei den harten Vorgaben zu Ausstoß und Stückzahlen je Zeiteinheit – ihr Augenmerk auf die Verfügbarkeit der Anlagen und Systeme und priorisiert diese zumeist sehr stark. Erst mit größerem Abstand folgt dann die Integrität (um die Korrektheit der übertragenen Daten zu sichern) und erst ganz am Ende wird sich um Vertraulichkeit gekümmert (nicht zuletzt, weil die hierfür erforderliche Verschlüsselung oft zu Verzögerungen bei der Übermittlung und Analyse der relevanten Daten führen würde – in einem von Echtzeitanforderungen dominierten Bereich ein echtes No-go!).

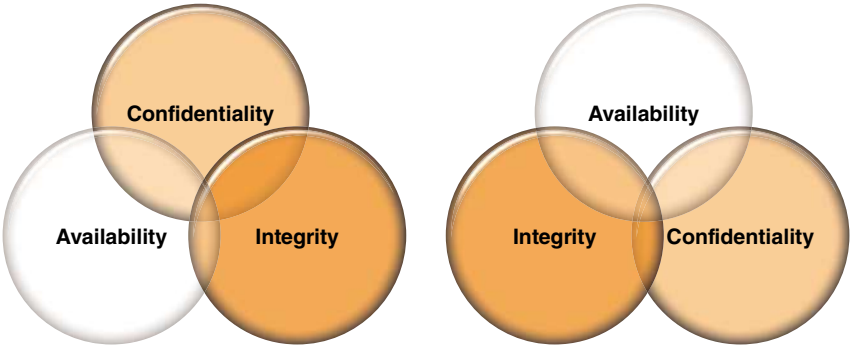

Bild 2.1 *CIA gegen AIC*

Neben den in Bild 2.1 dargestellten generellen Abweichungen bei der Priorisierung der Schutzziele muss vor allem beachtet werden, dass diverse technologische und organisatorische Rahmenbedingungen grundlegend unterschiedlich sind. Hierzu zählen unter anderem

- keine oder kaum Standardisierung der genutzten Hardware,
- keine oder kaum Standardisierung der genutzten Software,
- fehlende Standards und Technologien für Softwareverteilung und Asset Management,
- keine definierten Meldewege und Verfahren zur geregelten Annahme von Incidents,
- fehlende Zuordnung der Assets (Geräte, Peripherie, Programme) zu Verantwortlichen,
- fehlende Vorgaben für die Einkaufsbedingungen und Integrationsvorgaben für/von IT-Anteilen in Steuerungen, Maschinen und Produktionsanlage.

Insbesondere der Bedarf für Aufbau-organisatorische und personelle Änderungen zur Bewältigung dieser Unterschiede kann im Rahmen dieses Buches nur angerissen werden, da auf Basis der unterschiedlichen Unternehmensgrößen, Organisationsformen und internen Prozesse nur schwer generelle Handlungsvorschläge abzuleiten sind. Dennoch sollte sich der geneigte Leser vermehrt Gedanken um die strategische Änderung dieser Punkte machen, da jede ohne Vorgaben neu angeschaffte Anlage und jeder neue, nicht standardisierte PC in einer Maschinensteuerung erhebliche Folgekosten im Management der heterogenen Landschaft verursachen wird!

Tabelle 2.1 *Gegensätze Produktion–Office*

Kategorie	Office IT	Industrial IT
Signall-Laufzeiten und Antwort-verhalten	Keine garantierten Abarbeitungszeiten Hohe Latenz u.U. akzeptabel Ethernet-typisch «best effort»	Garantierte Abarbeitungszeiten Latenz ist zum Teil hart begrenzt Bus-Kommunikation teilweise deterministisch
Verfügbarkeit / Neustarts	Reboot von produktiven Server-Client-Systemen nicht ungewöhnlich Kurzfristig anberaumte Wartungsvorgänge möglich (z.B. kritischer Patch) Wartungsausfälle verursachen planbare Kosten	Reboot im produktivem Umfeld nicht akzeptabel Wartungszyklen nur mit langem Vorlauf, ausgerichtet an Anlagen-Instandhaltungsaufgaben IT-Wartungsausfälle verursachen hohe Kosten
Priorisierung der Schutzziele	Vertraulichkeit und Integrität von Daten stehen im Vordergrund Wesentliche Risiken betreffen die nachhaltige Störung von Geschäftsprozessen	Schutz von Mensch und Umwelt stehen im Vordergrund Wesentliche Risiken betreffen den unzureichenden Schutz von Menschen und die Zerstörung von Produktionskapazitäten. Auswirkungen auf die Umwelt sind möglich
Systemressourcen / Dediziertheit	Systemressourcen ausreichend, um Installation von IT-Security-Tools zu erlauben Interdependenzen vorhanden, aber beherrschbar	Installation fremder Softwarekomponenten auf Systemen erst nach Freigabe durch Lieferant oder nach Ablauf Gewährleistung, z.B. Virenschutz oder Whitelisting nur unter Verlust der Hersteller-Wartung
Lebenszeit der Komponenten	Wenige Jahre	Bis zu 20 oder 25 Jahre

Aus Tabelle 2.1 wird ersichtlich, dass die Unterschiede in der Betrachtung und Nutzung zwischen klassischer Office IT und der Industrial IT deutlich sind. Neben den bereits durch die Schaffung von «Industrial PC»-Hardware adressierten Problemen mit den teilweise rauen Umgebungsbedingungen für den Betrieb von IT-Komponenten blieben in den vergangenen zehn Jahren die besonderen Herausforderungen hinsichtlich Laufzeit, Stabilitätsanforderungen an die Systeme und deren Verfügbarkeit weitgehend unbeachtet.

Dies führt unter anderem dazu, dass durch fehlende Einkaufsanforderungen noch zum Zeitpunkt der Planung dieses Buches Produktionsmaschinen mit dem lange abgekündigten Betriebssystem Windows XP ausgeliefert wurden, weil die für den Betrieb der Anlagen notwendigen Softwarekomponenten nicht mit modernen Alternativen lauffähig sind und der Anlagenbauer die Migration nur langsam (oder gar nicht) vorantreibt. Hier zeigt sich ein «System-inhärentes Problem», in dessen Spannungsfeld sich die Industrial IT bewegt: Die Betreiber haben es bislang versäumt, «IT-Komponenten auf dem neuesten Stand der Technik» zu fordern (oder sie scheuen den Mehraufwand bei der Beschaffung), während die Anlagenbauer und Maschinenintegratoren die Investition in eine neue IT-Generation vermeiden wollen, da sie dies nicht mit ihren Bedürfnissen nach «mehr Funktionalität» mit höheren Preisen kompensieren können. Dass sowohl für den Anlagenbauer als auch für den Betreiber die strategischen Kosten des Betriebs solch inhärent unsicherer (und durch die o.g. Limitierungen über Jahre hinweg noch kritischer werdenden) Altlasten die Mehrkosten einer Investition in aktuelle und vor allem «aktualisierbare» IT-Komponenten bei weitem übersteigen (werden), ist offensichtlich.

2.2 Organisation und Industrial IT Security

Erst in wenigen Organisationen hat sich die Erkenntnis durchgesetzt, dass die Betrachtung der Informationssicherheit in der Produktion oder in produktionsnahen Umfeldern eine eigene Disziplin ist und entsprechende Expertise benötigt. In weiten Teilen kann beobachtet werden, dass etablierte Sicherheitsfunktionen wie beispielsweise der CISO oder der IT-Sicherheitsbeauftragte die Verantwortlichkeit für die IT-Komponente in der Produktion ablehnen oder diese aus ihrem Verantwortlichkeitsbereich heraus definieren. Diese Art der Abgrenzung führt unweigerlich zu einem Vakuum an Zuständigkeit und damit zu einer ausbleibenden Governance über diese Systeme. Ohne einen verantwortlichen Ansprechpartner bzw. verantwortliche Personen für Informationssicherheit in der Produktion können die Prozesse der Sicherheit folglich nicht ausreichend strukturiert und kontrolliert werden.

DEFINITION

Governance (frz.: *gouverner* = verwalten, leiten, erziehen; Unternehmensführung) bezeichnet allgemein das Steuerungs- und Regelungssystem im Sinn von Strukturen (Aufbau- und Ablauforganisation).

Folgende Elemente haben sich als wesentliche Bausteine für eine funktionierende IT-/Informations-Sicherheitsorganisation erwiesen:

- Die Aufbauorganisation des Unternehmens zeigt klare Governance-Strukturen und eine enge Zusammenarbeit zwischen ***O**perational **T**echnology* und ***I**nformation **T**echnology* (OT-IT-Kooperation).
- Es gibt (eine) dezidierte verantwortliche Person(en) für die OT / Industrial IT.
- Es gibt eine dezidierte verantwortliche Person für die OT-/Industrial-IT-Sicherheit.
- Die Struktur kooperiert nach Best Practices und Governance-Mechanismen, in Sonderfällen mit Ausnahmegenehmigung mit lokalen Prozessen und Sicherheitsvorgaben (etwa bei fehlendem Personal).
- In größeren Organisationen hat sich eine Verantwortlichkeitshierarchie auf Matrix-Prinzip als geeignet gezeigt, bei der die OT / Industrial IT disziplinarisch an die Werksebene berichten und eine fachliche Führung und Unterstützung von der geografischen oder zentralen IT (***C**hief **I**nformation **O**fficer*, CIO*)* erhalten. Hierbei ist zumindest eine Stabsfunktion «OT» unterhalb des CIO einzurichten, um die Belange der OT zentral vertreten zu können.
- Eine hierzu analog aufgebaute Unterstützung im Bereich der Informationssicherheit etabliert einen «***P**roduction / **A**utomation **S**ecurity **O**fficer*» (PSO, ASO), der direkt an die Werkleitung berichtet und fachlich vom CISO der Gesamtorganisation unterstützt wird. Auch hier empfiehlt sich, eine dedizierte Stabstelle für die Koordination der PSO/ASO- Angelegenheit beim CISO einzurichten.
- Die verantwortlichen Personen wurden mit denen für ihre Rollen notwendigen Schulungen und Know-how ausgestattet – die Beziehungen, Berichtswege und Prozesse wurden allen Beteiligten vermittelt und dokumentiert (Bild 2.2).

Für die Hersteller von Anlagen und Automatisierungstechnik ist es zudem wichtig, eine(n) Product Security Officer als Funktion einzurichten, der sich um die Sicherheitsanforderungen der verkauften Anlagen und Steuerungen kümmert, die Sicherheitsanforderungen aus den

Ausschreibungen und Vertriebsgesprächen mit den Kunden sammelt und koordiniert sowie für die Einhaltung der geltenden Vorschriften sorgt. Sowohl die Betreiber als auch die Integratoren benötigen umfassende Informationen über die Sicherheitseigenschaften (Security) der Komponenten und Anlagen, um diese möglichst sicher einzurichten und betreiben zu können. Im Umfeld der Safety ist dies bereits üblich und muss nun dringend für die Informationssicherheit nachgeholt werden. Verbände wie der ZVEI und der VDMA haben hierzu umfangreiches Material erarbeitet und bieten ihren Mitgliedern bereits Leitlinien mit Mindestanforderungen an. Diese sind über die Webseiten der Verbände sowie deren dedizierte Ansprechpartner leicht aufzufinden und sind zumeist auch für nicht dem Verband angehörende Unternehmen kostenfrei einzusehen.

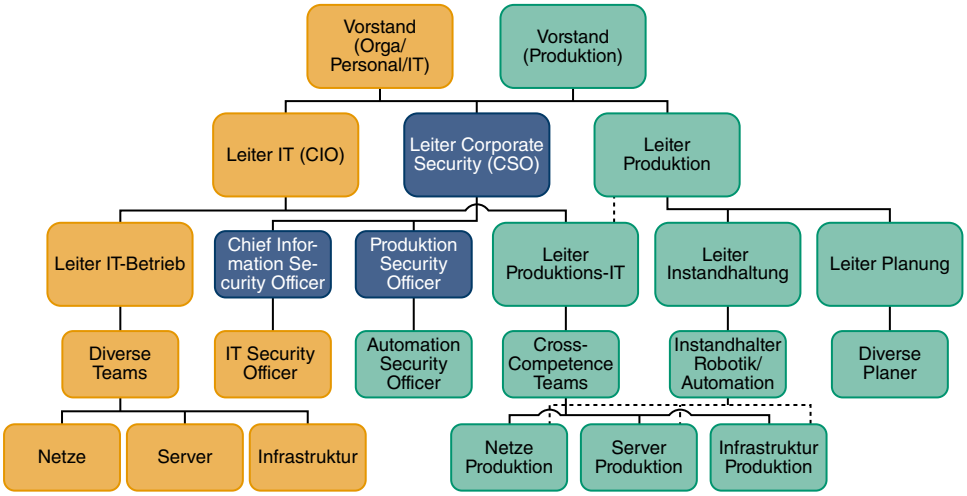

Bild 2.2 *Mögliche Organisation mit dedizierten Verantwortlichen für IT-Sicherheit*

2.3 Policies, Standards, Leitlinien und deren Anwendbarkeit

In Abwesenheit dedizierter Verantwortlichkeiten oder geeigneter Stellen in der Organisation wird nach «Entdeckung» der vielfältigen Industrial OT festgestellt, dass die vorhandenen Policies und Regelwerke gar nicht oder nur stark angepasst umsetzbar wären (Beispiel Antivirus in Steuerungs-PCs, regelmäßiges Patchen von Industrial-IT-Komponenten usw.). Es ist in den meisten Organisationen zwingend erforderlich, diese Policies und Regelwerke zumindest maßgeblich zu überarbeiten und zu ergänzen oder – mit deutlich besserer Erfolgsaussicht – direkt spezielle Regelwerke für die Industrial IT-Komponenten zu erlassen. Diese sollten unter direkter Mitwirkung der Instandhaltung, der Planungsingenieure und den Verantwortlichen für Shopfloor IT (falls vorhanden) erstellt werden, damit die Anforderungen realitätsnah aufgenommen werden.

Bild 2.3 zeigt, wie sich eine Hierarchie von Regelwerken aus Sicht der ISACA (Berufsverband der IT-Revisoren, IT-Sicherheitsmanager sowie der IT-Governance-Experten) darstellt. Hierzu muss ergänzt werden, dass die Policy der obersten Ebene durchaus unterhalb einer umfassenderen «Enterprise» Policy angeordnet sein kann. Die Policy an der Spitze der Pyramide stellt eine sehr abstrakte, kurze Anweisung dar, wie die Organisation mit Informationssicherheit umgehen will und soll. In ihr wird regelmäßig auf die darunter angesiedelten Standards und Leitlinien hingewiesen,

Bild 2.3 *Policy-Hierarchie in Anlehnung an ISACA – CISA (Certified Information System Auditor)*

die konkretere Regeln für die Nutzung bestimmter Technologien oder die Abläufe und Prozesse definieren. Daraus ergibt sich zwangsläufig, dass die Regelwerke in absteigender Reihenfolge häufiger angepasst werden müssen. Eine Corporate Policy für Informationssicherheit sollte folglich nur minimal angepasst werden, um auch die OT / Industrial IT abzudecken. Die Standards, Richtlinien und Prozeduren unterhalb bedürfen vermutlich mehr Aufmerksamkeit, bis hin zur Erstellung neuer Dokumente, die sich spezifisch auf die Komponenten der OT beziehen. Sowohl die OT / Industrial IT betreffenden Standards als auch die Leitlinien und Prozeduren müssen in einen geregelten Lebenszyklus überführt werden und benötigen jeweils einen Verantwortlichen, der für die regelmäßige Anpassung der Inhalte an den Stand der Technik sorgt. Darüber hinaus empfiehlt sich die Einrichtung einer Governance-Funktion für die Überwachung und Einhaltung der Updates und Ergänzungen. Diese kann – zumal sich hier eher Kontrollfunktionen konzentrieren – außerhalb der Produktion und innerhalb eines Enterprise Governance oder Ähnlichem befinden.

2.4 Gefährdung der Industrial IT Security und abgeleitete Anforderungen

2.4.1 Problemfeld «Fehlende Awareness der Mitarbeiter»

Die größte Herausforderung für die Sicherheit der Industrial IT ist das fehlende Bewusstsein für die Kritikalität der aktuellen Sachlage. Zwar konnten die Medienberichte über manipulierte Steuerungstechnik für Zentrifugen (Stuxnet, Busheer, Iran) und Stahlproduktion (deutscher Hochofen) sowie die offen über das Internet erreichbaren Haus-, Heizungs- und sonstigen Steuerungen (Heise Verlag 2014/2015) ein gewisses Maß an Aufmerksamkeit generieren, dies führte jedoch eher zu halbherzigen Aktionen hinsichtlich der Schließung allzu offensichtlicher Lücken, nicht jedoch zu nachhaltigem Umdenken bei der Entwicklung und der Inbetriebsetzung von vernetzen Steuerungskomponenten. Die derzeitigen (2018) Projekte rund um Industrie 4.0 sowie das Internet der Dinge und die damit einhergehende Betrachtung von Sicherheitsaspekten ist zwar ein entscheidender Schritt in die richtige Richtung, hierbei wird jedoch oftmals – bewusst oder unbewusst – auf eine Berücksichtigung der bereits vernetzten, aber schlecht gesicherten Bestandssysteme verzichtet. Folglich ist eine der wichtigsten Maßnahmen für eine Verbesserung der Sicherheitslage in der Industrial IT die Schaffung von mehr Verständnis für das Vorhandensein von Informationstechnik in der Produktion bei den Entscheidern und die klare Darstellung der mit Vernetzung und fehlenden Schutzmaßnahmen verbundenen Risiken für die Wertschöpfungsprozesse im Unternehmen.

2.4.2 Unzureichende Dokumentation der Anwendungen und Systeme («Graue IT»)

Eine besondere Schwachstelle der Industrial IT ist die oft unzureichende Dokumentation der IT-Komponenten in Produktionsanlagen und komplexen Maschinen. Im Gegensatz zur oft sehr ausführlichen und durch Qualitätsmanagement stetig verbesserten Dokumentation der mechanischen und «Safety-kritischen» Komponenten einer Anlage sind die Informationen hinsichtlich der verwendeten oder installierten IT-Systeme, Betriebssysteme, Anwendungen, Tools und Datenbanken oder Verzeichnisse oft mangelhaft, bestenfalls dürftig oder teilweise schlicht und ergreifend überhaupt nicht vorhanden. Dies erschwert maßgeblich die sinnvolle Verwaltung der vorhandenen Assets, da zunächst eine umfassende und detaillierte Erhebung erfolgen muss, um anschließend die fehlende oder unzureichende Dokumentation so zu ergänzen, dass eine Fehlerdiagnose und -behebung überhaupt möglich ist. Zwar haben die betroffenen Mitarbeiter sich die notwendigen Kenntnisse über die Anlage zumeist erarbeitet und können Fehler eingrenzen, eine Übergabe an Dritte oder eine gezielte Suche nach Details bleibt jedoch ohne diese Dokumentation nahezu unmöglich.

Durch fehlende Dokumentation kann zudem ein trügerisches Gefühl der Sicherheit entstehen, das in kritischen Situationen zu Fehlentscheidungen und falschen Informationsständen führt. Eine aus Sicht der IT-Sicherheit gute Dokumentation zeichnet sich insbesondere durch eine klare Darstellung der verwendeten IT-Komponenten und Systeme, deren Versionsstände und Konfigurationsparameter aus. Des Weiteren sind vollständige Informationen zu verwendeten Protokollen, IP-Adressen, Ports und allgemeinen Kommunikationspartnern von überragender Wichtigkeit. Im Idealfall erstellt der Errichter ein Kontextdiagramm, aus dem klar ersichtlich wird, welche Systeme mit welchen anderen Systemen über welche Sockets kommunizieren. Dies schließt eine umfassende Darstellung der Benutzer- und Systemkonten, Passwörter und deren jeweiligen Anwendungskontext ein. Insbesondere Systemkonten und technische Konten mit hohen Privilegien sind ausführlich zu dokumentieren, so dass der Betreiber jederzeit in der Lage ist, notwendige Anpassungen auch ohne die Unterstützung des Herstellers oder Lieferanten auszuführen. Falls dies aus Gründen der Gewährleistung nicht erwünscht ist, so ist zumindest eine Hinterlegung dieser Informationen bei einem Treuhänder oder ein «Escrow-Verfahren» zur Einsichtnahme in diese Daten (etwa bei Insolvenz des Lieferanten) zu vereinbaren.

i

DEFINITIONEN

Sockets ist die Bezeichnung für eine Kombination aus IP-Adresse (Schicht 3 des ISO/OSI-Modells) und (TCP/UDP-) Port (Schicht 4) zur Beschreibung der Kommunikation zwischen zwei Knoten, etwa Source 192.168.2.12:4677 – Destination 192.168.2.211:80 – der Aufruf einer Webseite auf dem Server.

Escrow-Verfahren: eine Synchronisationsmethode von Transaktionen zum Einbringen von Daten in die Datenbank.

Plain WRONG in diesem Umfeld ist ein Escrow-Verfahren – eine Möglichkeit der Einsichtnahme in den Source-Code, wenn die Firma pleite geht oder sonstwie die Software «verliert».

Ein weiteres Problemfeld sind kleinere IT-Systeme, bei denen die Zuordnung eines Verantwortlichen bzw. eines Systemeigentümers fehlt. Diese – oft als «graue IT» bezeichneten, zumeist durch interne Kräfte, Praktikanten oder Werkstudenten erstellten – unterstützenden Systeme werden durchaus von mehreren Anwendern oder Anwendergruppen genutzt, eine richtige Zuständigkeit wurde jedoch nie definiert – von einem geregelten «IT-Lebenszyklus» mit einer ordentlichen Versorgung mit Updates und Support oder Weiterentwicklung ganz abgesehen. Oftmals haben

sich jedoch starke Abhängigkeiten von oder zu dem System entwickelt, die eine intensive Betreuung und Pflege notwendig machen. Neben der «Nach-Dokumentation» solcher Anwendungen ist dann die Benennung eines «Systemeigners» die erste Maßnahme, die oftmals in die Erstellung eines koordiniert entwickelten und unterstützenden Ersatzsystems mündet, das über entsprechende Dokumentation und Zuständigkeiten verfügt.

2.4.3 Fehlende Überwachung der Infrastruktur und Anwendungen

Die Überwachung der Produktionstechnologie hinsichtlich ihrer Leistung, Abnutzung und Verbrauchsmaterialien ist eine Standardaufgabe in der Produktions- und Anlagentechnik. So werden gewöhnlich die Produktion betreffende Warnungen (z.B. bei unterschrittenen Füllständen) und technische Parameter (z.B. Temperaturen, Ventilstellungen) abgebildet. Dagegen fehlt es häufig an einer angemessenen Überwachung der unterstützenden IT-Infrastruktur [1].

Diese Beobachtung und Auswertung bietet jedoch erhebliche Mehrwerte, da die Analyse des Netzwerkverkehrs oder der Auslastungsparameter der IT-Komponenten Rückschlüsse auf möglicherweise bislang unentdeckte Angriffe oder Manipulationsversuche ermöglicht. Zu diesen Ereignissen zählen erfolglose und erfolgreiche Authentifizierungsversuche an IT-Komponenten, eine erhöhte Auslastung des Netzes an Knotenpunkten und fehlerhafte Zugriffsversuche auf Dateien oder Speicher / Verzeichnisse. Darüber hinaus kann auch eine mangelhafte, unübersichtliche Darstellung der Ereignisse dazu führen, dass Warnungen und Fehler verspätet erkannt werden. Experten raten darum dringend, zumindest grundlegende Überwachungsprozesse zu etablieren und die daraus resultierenden Log-Nachrichten und Meldungen an zentraler Stelle zu sammeln und – nach Möglichkeit – semi-automatisiert auszuwerten. Als Einstieg bieten sich als mögliche Werkzeuge Syslog-Server und Open-Source-Netzwerk-Monitoring-Lösungen wie etwa Nagios an. Darüber hinaus kann die Analyse von Daten über Werkzeuge wie Splunk (in der «Light»-Variante) erfolgen. Weitere kommerzielle Werkzeuge sind WhatsUp GOLD oder der Industrial Defender von Lockheed Martin. Mit dem Fokus auf das Risiko Management kann hier «IRMA» des deutschen Anbieters Achtwerk eine Alternative darstellen, die auch Überwachung und Reporting abdeckt. Als weiterer Vertreter der passiv lauschenden Systeme mit erweiterten Analysefunktionen hat sich das israelische Unternehmen Cyberbit mit seinem SCADA Shield einen Namen gemacht. Ebenfalls in diesem Bereich tätig, kann das deutsche Startup-Unternehmen Rhebo GmbH genannt werden, das mit seinen Produkten ebenfalls einen tieferen Einblick in die Welt der industriellen Kommunikation gibt.

DEFINITION

Syslog: ein Standard zur Übermittlung von Log-Meldungen in einem IP-Rechnernetz.

2.5 Organisatorische Maßnahmen

Dieser Abschnitt führt in mögliche organisatorische Maßnahmen für die Betreiber von Automatisierungs- bzw. Produktionsanlagen mit steigenden IT-Anteilen ein. Diese Maßnahmen sind eine Zusammenstellung erprobter Ansätze aus diversen Projekten und beziehen sich auf Standards wie etwa ISO 27 000 / IT-Grundschutz, IEC 62 443 und VDI 2182.

Die beschriebenen Maßnahmen stellen lediglich den Einstieg in einen geordneten IT-Sicherheitsprozess innerhalb der Produktion dar und setzen eine intensive Analyse der vorhandenen

IT voraus. Ohne den Aufbau eines umfassenden Managements für die Informationssicherheit auf Basis der genannten Standards wird keine Einzelmaßnahme nachhaltigen Erfolg zeigen. Es muss folglich das Bewusstsein geschaffen werden, dass die alleinige Erstellung und Verabschiedung einer Policy oder die Verschlüsselung jedweder Kommunikation weder hilfreich noch zielführend sein kann. Bei der Einführung geeigneter Maßnahmen sollten Entscheider vielmehr beachten, dass diese in für das Unternehmen oder die Standort-Organisation sinnvoller Reihenfolge durchgeführt werden. Beispielhaft kann dies wie folgt aussehen:

1. Aufbau einer Security-Organisation in der Produktion
2. Erstellen der notwendigen Dokumentationsvorlagen (für Assets, Prozesse, Verantwortlichkeiten, Aufgaben und Kompetenzen)
3. Inventarisierung aller IT-Systeme und der installierten Anwendungen in der Produktion sowie deren Eigenschaften, Besitzer usw.
4. Erstellung einer Sicherheitslinie für die Produktion / Automatisierung sowie Festlegung der Verantwortlichkeiten für Assets und Prozesse
5. Initiale Risikobewertung (rein qualitativ), ggf. Anpassung der Leitlinie an Erkenntnisse
6. Erstellen von Benutzerhandbüchern für die Administration der vorhandenen Systeme, Zuständigkeiten usw.
7. Ableitung, Definition und Implementierung der notwendigen (Pflege-) Prozesse
8. Erstellung eines Regelzyklus für die Kontrolle neuer Maßnahmen
9. Priorisierung möglicher Maßnahmen und Umsetzungsplan

Diese Aufgaben dienen dazu, eine zentrale Anlaufstelle für alle Fragen rund um die Sicherheit in der Produktion zu definieren und deren Zuständigkeitsbereich, Kompetenzen und auch Grenzen zu beschreiben. Ein sinnvoller Überblick über die eigenen Systeme und die Infrastruktur gelingt nur, wenn die Assets im Vorfeld geordnet erfasst und dokumentiert worden sind. Hierzu dienen beispielsweise Vorlagen und Templates, die den Technikern, Instandhaltern und Produktionsfachleuten helfen, systematisch vorzugehen. Je nach Situation und eigenem Ermessen kann dann die Fleißarbeit der Inventarisierung erfolgen oder der Fokus zunächst auf die Erstellung der notwendigen Leitlinie liegen. Dazu gehört in erster Linie auch, die Verantwortlichkeiten zu definieren und diese zuzuordnen, damit identifizierte Risiken ebenfalls eindeutig verteilt werden können und die Umsetzung der Maßnahmen an den zuständigen Mitarbeiter vergeben werden kann. Für die Erfassung der (Asset-) Bestandsdaten können sich auch bereits erfolgte Security Audits als nützlich erweisen, da in deren Rahmen möglicherweise bereits relevante Fragestellungen beantwortet wurden. Die vor Ort relevanten Risiken und die sich daraus ableitenden Schutzmaßnahmen gilt es bei jedem Aufbau einer Security-Organisation in der Produktion individuell zu bestimmen. Für eine angemessene Auswahl und Umsetzung der Maßnahmen ist eine ebenso individuelle Risikoanalyse zwingend notwendig. Auf deren Basis gelingt die Unterscheidung von sinnvollen und nicht zielführenden Maßnahmen, um am Ende die lokal auftretenden Gefährdungen angemessen zu entschärfen.

2.5.1 Dedizierte IT-Security-Organisation für die Produktion

Ähnlich wie die Situation in den Unternehmen Mitte des ersten Jahrzehnts dieses Jahrtausends eskalierte und erst nach und nach Stellen für Informationssicherheits-Beauftragte, Datenschutz-Beauftragte und letztlich (Chief) Information Security Officer aufgebaut werden konnten, gilt es heute zunächst einen verantwortlichen Ansprechpartner bzw. eine verantwortliche Person für Informationssicherheit in der Produktion zu benennen (Bild 2.4).

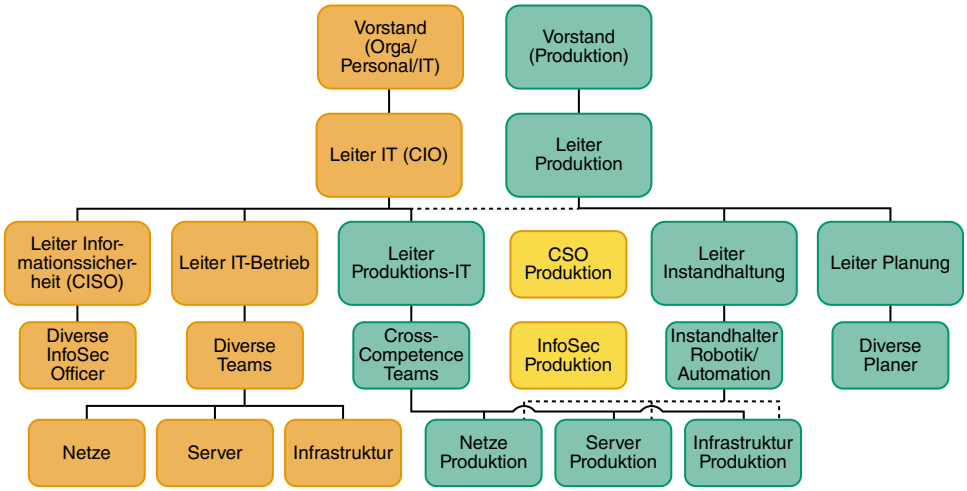

Bild 2.4 *Chief Security Officer und Produktionssicherheit*

Ohne einen solchen Ansprechpartner lassen sich die Sicherheitsprozesse nicht ausreichend strukturieren und kontrollieren. Als größter Stolperstein hat sich dabei oft erwiesen, dass das Top-Management keinen Einblick in die IT-Komponenten in der Produktion hatte oder der weitreichenden Abhängigkeit von IT in der Produktion nicht ausreichend Bedeutung beigemessen wurde. Ohne einen Ansprechpartner und Verantwortlichen für IT-Komponenten in der Produktion wird die Definition eines reinen Security-Fachmanns in der Produktion allerdings fehlschlagen. Die ideale Struktur (Bild 2.5) sieht einen direkt an den Vorstand berichtenden Corporate Security Officer vor, an den jeweils sowohl ein Chief Information Security als auch ein Production Security Officer berichten.

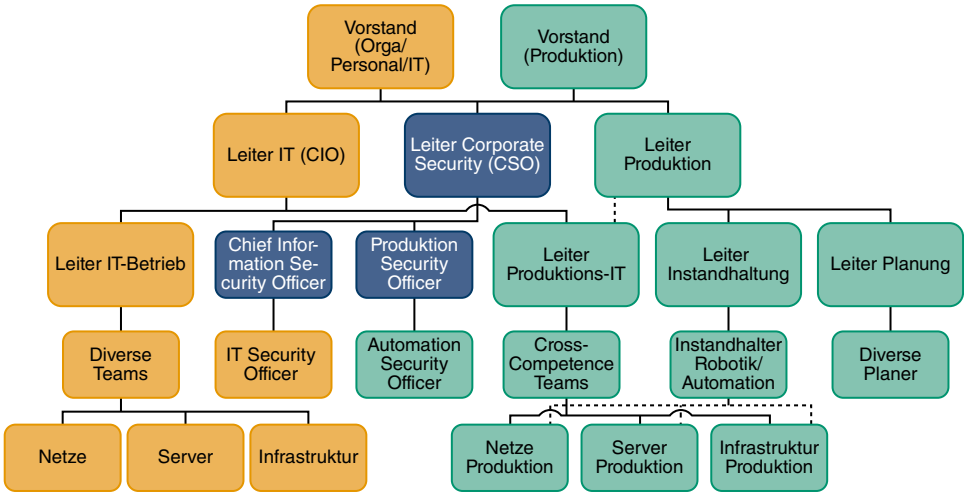

Bild 2.5 *CSO, CISO und Production Security Officer*

Unabhängig von diesen Idealbildern haben sich folgende Elemente als Bausteine für eine funktionierende Organisation bewährt:

- Es gibt eine dezidierte verantwortliche Person für die IT in der Produktion.
- Es gibt eine dezidierte verantwortliche Person für die Shopfloor-IT/OT-Sicherheit.
- Die Organisation zeigt enge Zusammenarbeit von Werksebene (OT – Operational Technology) und der IT in der Produktion und im Office.
- Es wird nach Möglichkeit nach anerkannten Best Practices und etablierten Governance-Mechanismen gearbeitet. Wo es notwendig ist, wird per Ausnahmegenehmigung die Nutzung lokal angepasster Prozesse und Sicherheitsvorgaben ermöglicht.
- Im Sinne der **A**ufgaben / **K**ompetenzen / **V**erantwortlichkeiten (AKV) (siehe auch Bild 2.7) werden alle für besondere Aufgaben verantwortlichen Personen mit den für ihre Rollen erforderlichen Schulungen und dem notwendigen Know-how ausgestattet.
- Die Beziehungen, Berichtswege und Prozesse für einen reibungslosen Betrieb müssen allen Beteiligten vermittelt werden und deren Dokumentation ist stets aktuell zu halten.

2.5.2 Sicherheitsleitlinie für die Produktion

Der Zweck einer dedizierten Sicherheitsleitlinie für die Produktion sind die Bereitstellung von allgemein gültigen Vorgaben und die Sicherstellung einer Unterstützung der Maßnahmen für die Steigerung der Informationssicherheit in der Produktion durch das Management. Die Leitlinie sollte folglich so erstellt sein, dass sowohl die geschäftlichen Anforderungen als auch die geltenden Gesetze und Vorschriften eingehalten werden.

Organisatorisch siedelt sich die Produktionsleitlinie unterhalb einer ebenfalls essenziellen Leitlinie zur Informationssicherheit für das Unternehmen an. Diese vom Management verabschiedete Leitlinie sollte im Übrigen auch einen Ansatz zur Bewältigung der Ziele für die Informationssicherheit festlegen.

Regelmäßige Prüfung und Anpassung der Leitlinie
Jede veröffentlichte Leitlinie muss regelmäßig geprüft werden (Bild 2.6), ob sie weiterhin geeignet, angemessen und wirksam ist. Im Zuge der Überprüfung sollte der Fokus auf die Identifikation von Verbesserungspotenzialen für die Leitlinie sowie auf die Methoden des Managements von Informationssicherheit in der Organisation liegen. Primär lassen sich so Antworten auf mögliche Änderungen im organisatorischen Umfeld, bei den geschäftlichen Rahmenbedingungen und bei den technischen Gegebenheiten generieren. Übrigens lehrt uns die Erfahrung: Im Sinne eines umfassenden Change-Managements sollte jede nachhaltige Änderung der Leitlinie durch das Management genehmigt und freigegeben werden.

2.5.3 Aufgaben, Kompetenzen, Verantwortlichkeiten und Prozesse

Für alle wesentlichen Aufgaben im Bereich der IT (Security) für die Produktion hat es sich bewährt, die Verantwortlichkeiten nachvollziehbar zu regeln und zu dokumentieren. Der Zuschnitt der Aufgaben sollte dabei so erfolgen, dass die vorhandenen Kompetenzen ausreichende Berücksichtigung finden oder durch dedizierte Maßnahmen zur Reduktion möglicher Kompetenzlücken kompensiert werden können. Zudem zeigt die Praxis, dass Überschneidungen zwischen ähnlichen Aufgaben ungünstig sind – Zuständigkeitslücken dürfen jedoch keinesfalls auftreten. Diese Regel sollte für alle Bereiche der Produktion eine Selbstverständlichkeit sein, für die sicherheitsrelevanten