Inhaltsverzeichnis

Resonanzen der Verbände

A Cybersicherheit als Voraussetzung für erfolgreiche Digitalisierung

B Regelkonformität mit Normen und Richtlinien

C Fabrik als Anwendungsdomäne / Industrial Control Systems

D Mobile und intelligente Komponenten / Smart Devices

F Unternehmensorganisation

G Risikomanagement

Resümee

Management-Statement

Grußwort

Es ist in aller Munde: Wie andere Gesellschaftsbereiche revolutioniert Digitalisierung auch die Industrie rasend schnell. Das bietet vor allem für den Innovations- und Wirtschaftsstandort Deutschland enorme Potenziale, sei es Effizienz- und Qualitätssteigerung oder vollkommen neue, datenbasierte Geschäftsmodelle. Gleichzeitig gehen aber mit der Digitalisierung auch Herausforderungen in puncto Sicherheit einher. Wie sollen sensible Kundendaten sicher verwahrt und kritische Infrastrukturen vor dem Zugriff Unbefugter geschützt werden?

Insbesondere kleine und mittlere Unternehmen fühlen sich von Sicherheitsfragen überfordert. Cybersicherheit wird als trocken, teuer und aufwendig wahrgenommen. Dabei wird der Wert von durchdachten Sicherheitskonzepten für die Industrie 4.0 im Buch eindeutig herausgestellt: Cybersicherheit ist nicht nur sinnvoll, sondern absolute Grundvoraussetzung für erfolgreiche Digitalisierung. Standardisierte Sicherheitsarchitekturen werden zum «Enabler» für Industrie 4.0. Erst das Vertrauen in IT-Sicherheit ermöglicht datenbasierte Geschäftsmodelle und neue Partnerschaften. Die Autoren machen klar, dass Security als Qualitätsmerkmal in allen relevanten technischen Aktionsfeldern verankert werden muss – egal ob Smart Devices, Cloud Computing oder Industrial Control Systems.

Das Buch erklärt nicht nur die Bedeutung von IT-Sicherheit, sondern bietet auch die nötige Unterstützung. Durch eine umfangreiche Analyse des Themas fügen sich Beiträge der Experten und Praktiker zu einem Leitfaden für industrielle Anwender.

Damit Sicherheit umfassend und dauerhaft eintritt, bedarf es «Security by design». Eine vorausschauende Sicherheitskultur muss sich im Bewusstsein der Verantwortlichen sowie im Portfolio der Unternehmen widerspiegeln. Genauso wichtig ist jedoch die internationale Zusammenarbeit, denn die Bedrohungslage kennt keine Grenzen und Nationalitäten. Nur eine globale, standardisierte und vertrauenswürdige Sicherheitsinfrastruktur über gesamte Wertschöpfungsnetzwerke und industrieller Lebenszyklen ermöglicht es, die Potenziale der Industrie 4.0 voll auszuschöpfen. Hier geht das Buch auch auf die Rolle der Plattform Industrie 4.0 und ihrer Arbeitsgruppe «Sicherheit vernetzter Systeme» ein, die globale Key Player zusammenbringt, um Lösungsansätze, Handlungsempfehlungen und konkrete Anwendungsbeispiele für eine sichere, vernetzte Industrie zu entwickeln.

In diesem Sinne des Austausches und Know-how-Transfers bieten die folgenden Seiten viel Wissenswertes rund um das Thema Cybersicherheit – egal ob für Privatpersonen, Großkonzern oder Mittelstand.

Viel Spaß beim Lesen und Lernen!

Henning Banthien, Secretary General der Plattform Industrie 4.0

Vorwort des Herausgebers

Mehr als sechs Millionen Cyberangriffe finden jeden Tag weltweit statt. Anzunehmen ist, dass sich die Anzahl und Intensität hochspezialisierter Cyberangriffe in Zukunft weiter steigern werden. Die steigende Anzahl von «Smart Factories» mit neuen digitalen Technologien und vernetzten Objekten, wie sie Industrie 4.0 mit sich bringt, wird die Anfälligkeit für Cyberangriffe dynamisieren und die Angriffsfläche weiter erhöhen. Eine ständig steigende Angriffskomplexität und Angriffsqualität heben die Gefährdungslage zusätzlich auf ein neues Niveau.

Die Auswirkungen von Cyberattacken im Bereich der Industrie sind gravierend und können ernste Folgen haben: illegaler Wissens- und Technologietransfer durch Datendiebstahl und technische Spionage (streng vertrauliche Informationen zur Produktherstellung werden ausspioniert), Wirtschaftssabotage (sensible Produktionsdaten werden manipuliert oder das gesamte Wertschöpfungsnetzwerk wird komplett zum Stillstand gebracht) und nicht zuletzt leidet das Gesamtimage eines Unternehmens nach außen bei Geschäftspartnern und Kunden erheblich. Angesichts solcher Szenarien stellt sich immer drängender die Frage: Wie können wir die Digitalisierung so gestalten, dass die zu erwartenden Vorteile nicht durch den nächsten Cyberangriff zunichte gemacht werden?

Jedes industrielle Unternehmen ist dafür selbst verantwortlich, seine Unternehmensdaten und den laufenden Betrieb der Wertschöpfung sicher vor Cyberangriffen zu machen. Dies im Sinne des Unternehmenserfolges strategisch und nachhaltig umzusetzen ist Chefsache. Großunternehmen haben dabei im Laufe der letzten Jahrzehnte gegen Cyber-Sicherheitsvorfälle durch entsprechende Maßnahmen ein sehr hohes Absicherungsniveau erreicht. Doch wo ein international operierendes Großunternehmen erhebliche Summen investieren kann, um sich vor dubiosen Machenschaften Cyberkrimineller zu schützen, muss sich ein mittelständisches Unternehmen mit weitaus geringeren Mitteln helfen.

Eigenes Wissen ist dabei immer noch die beste Verteidigung. Mit dem vorliegenden Buch möchte ich als Herausgeber einen Beitrag dazu leisten, dass mittelständische Unternehmen einen leichteren Zugang zu dem Thema Cybersicherheit für vernetzte industrielle Anwendungen erlangen. Mit diesem Werk adressiere ich bewusst auch neue digitale Entwicklungen, wie sie Industrie 4.0 und die Digitalisierung mit sich bringen, und spreche den fachinteressierten Leser an, der sich grundlegend in die Thematik einarbeiten möchte und dafür praxisbezogene, allgemein verständliche Informationen benötigt.

Das Thema wird umfassend und in vielen Facetten beleuchtet und analysiert. Dabei liegt das Hauptaugenmerk der Beiträge nicht nur auf dem möglichen Gefahrenpotenzial, sondern auch in konkreten Handlungsanweisungen und Schutzmaßnahmen. Somit wird dem interessierten Leser ein praxisbezogener Leitfaden an die Hand gegeben, mit dessen Hilfe er das Konzept Cybersicherheit für vernetzte industrielle Anwendungen verstehen und umsetzen kann.

Dazu erarbeiteten wir mehrere sich ergänzende und ineinandergreifende Themenblöcke, die aus Expertensicht in ihrer Gesamtheit für die Entwicklung von Cybersicherheit bei Industrie 4.0 von zentraler Bedeutung sind. Durch einen abwechslungsreichen Mix wurde darauf geachtet, dass Einblicke aus Großkonzernen, Mittelstand, Start-ups sowie Meinungen von Forschungs- und Bildungseinrichtungen vermittelt werden. Das Werk besitzt eine sinnlogische Reihenfolge, aber einzelne Kapitel können auch unabhängig voneinander gelesen werden.

Der Mittelteil dieses Buches orientiert sich an den drei für die Praxis von Cybersicherheit für vernetzte industrielle Anwendungen besonders relevanten technischen Aktionsfeldern: die Informationstechnik auf den lokalen Servern und in den Datenzentren (IT – Information Technology), die industriellen Steuerungs- und Leitsysteme (OT – Operational Technology) und die in

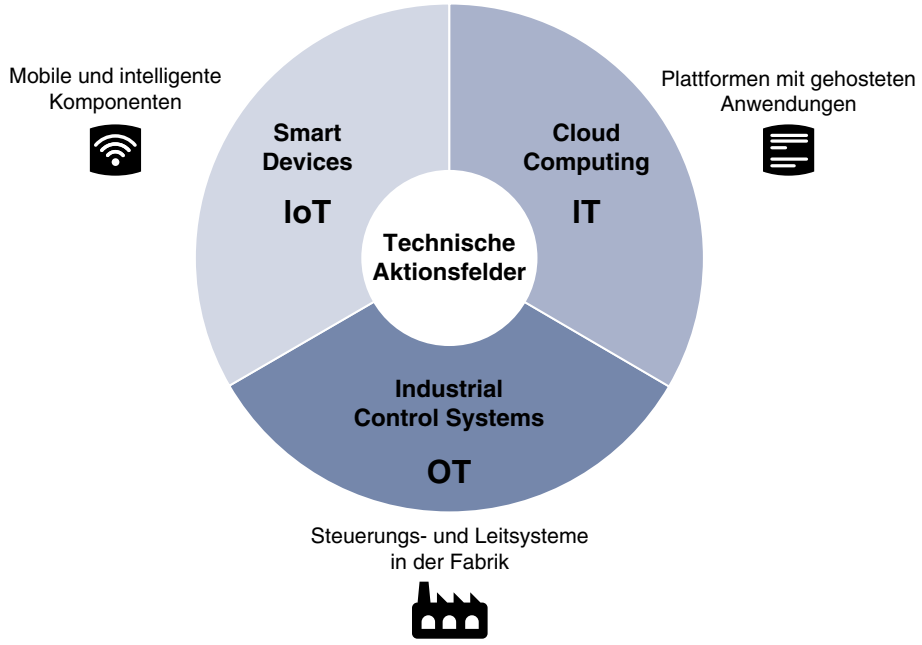

Bild 1 *Technische Aktionsfelder der Cybersicherheit bei Industrie 4.0*

industriellen Anwendungen verwendeten Komponenten des Internets der Dinge (IoT – Internet of Things).

Bild 1 fasst diese drei technischen Komponenten der Cybersicherheit zusammen. Die Sicherheitsarchitektur dieser drei technischen Systeme und Komponenten muss grundlegend neu gedacht werden. Dabei muss die Sicherheit durch «Security by Design» und «Security by Default» von vornherein gewährleistet sein.

Im Teil C «Fabrik als Anwendungsdomäne / Industrial Control Systems» wird der Unterschied zwischen Information Technology und Operational Technology herausgearbeitet. Cyberangriffe auf industrielle Anlagen und kritische Infrastrukturen können ernste Folgen haben und lassen sich nicht einfach durch übliche Sicherheitsmaßnahmen wie bei Anwendungen in der Büro- und IT-Umgebung vermeiden. Es werden typische Schwachstellen und das daraus resultierende grundlegende Bedrohungspotenzial für industrielle Steuerungssysteme, ergänzt durch Praxisbeispiele aus dem Monitoring von verschiedenen ICS, vorgestellt. Es erfolgt eine detaillierte Betrachtung technischer und organisatorischer Maßnahmen mit einzelnen Aspekten der Sicherheitskonzepte für ICS-Systeme. Insbesondere werden Besonderheiten automatisierter Sicherheitseinrichtungen (SIS) aus Sicht der Manipulierbarkeit bzw. Kompromittierbarkeit durch Cyberangriffe dargestellt und wesentliche Elemente eines dedizierten SIS-Cyber-Security-Managements beschrieben und Aspekte der praktischen Umsetzung erörtert.

Im Teil D «Mobile und intelligente Komponenten / Smart Devices» geben wir eine Einführung und einen Überblick über Cyber Security für Industrie-4.0-Komponenten als wichtigen Bestandteil vieler Industrie-4.0-Anwendungen. Diese Komponenten zeichnen sich dadurch aus, dass sie sich mit anderen Komponenten vernetzen und über Systemgrenzen hinweg kommunizieren, um so im Zusammenspiel mit Backend-Diensten die Industrie-4.0-Anwendungen zu realisieren. Die Teilnehmer in einem Industrie-4.0-System müssen sich in zunehmendem Maße auf die Korrekt-

heit, Vollständigkeit und Unverfälschtheit ihrer Daten, Systeme und Prozesse verlassen können. Insbesondere sind lokale Schnittstellen, Wartungs- und Administratorzugänge, die Datenspeicherung und die Netzwerkkommunikation zu schützen. Grundlegende Sicherheitsmaßnahmen umfassen den Schutz der ausgeführten Firmware und Software, den Schutz von kryptographischem Material, sichere Kommunikationsverbindungen sowie sichere Identitäten durch Identitätszertifikate. Mögliche Angriffe auf solche Geräte werden in praktischer Hinsicht analysiert und diskutiert.

Im Teil E «Plattformen mit gehosteten Anwendungen / Cloud Computing» befassen wir uns mit den wichtigsten Sicherheitsrisiken und Bedrohungsszenarien virtualisierter IT-Ressourcen wie Rechenkapazität, Datenspeicher, IoT-Plattformen und Software durch einen Service Provider über das Internet. Grundprinzipien des Datenschutzes und Prinzipien für die Sicherheit industrieller IoT-Plattformen werden beschrieben. Eine IoT-Plattform ist eine wiederverwendbare Basis an Technologien, Diensten und Realisierungen von Prozessen, auf denen aufbauend weitere Technologien, Dienste, Realisierungen von Prozessen und Anwendungen entwickelt werden können. Sicherheitsmechanismen, die bereits bei der Konzipierung der Plattform integriert sind, und Sicherheitsstrategien im Prozess der Anwendungsentwicklung spielen neben dem kontinuierlichen Monitoring mit intelligenter Detektion und schneller Reaktion auf Systemanomalien eine wesentliche Rolle.

In der Gesamtheit bedarf die offene, vernetzte Wertschöpfung der Industrie 4.0 einer durchgängigen, geschlossenen Lösung der Cybersicherheit zur Bewältigung der Gefahren durch neue digitale Technologien im industriellen Umfeld. Cybersicherheit ist dabei keine Innovationsbremse, sondern vielmehr ein wichtiger Garant für zukünftigen unternehmerischen Erfolg. Neben den drei technischen Aktionsfeldern beschreiben wir wichtige Einflussfaktoren, deren Kenntnisse für die Cybersicherheit vernetzter Industrie-4.0-Anwendungen in Unternehmen unterstützend oder zwingend notwendig sind (Bild 2).

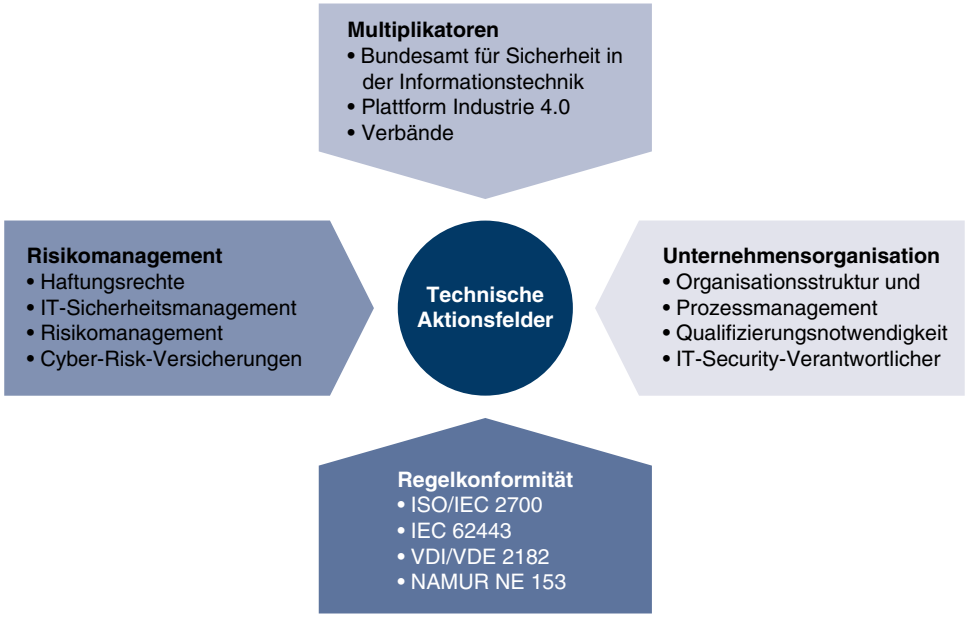

Bild 2 *Einflussfaktoren auf die technischen Aktionsfelder der Cybersicherheit*

Welche Multiplikatoren unterstützen die Industrie bei der Verbreitung und Akzeptanz von Cybersicherheit? Zum einen gilt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentraler Ansprechpartner für den Ausbau der Beratung für die Wirtschaft zum Thema Informationssicherheit in der Digitalisierung. Weiterhin befassen sich mit dem Thema Cybersicherheit für vernetzte Anwendungen in der Industrie 4.0 der Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (BITKOM), der Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA), der Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI), der Cyber-Sicherheitsrat Deutschland e.V. sowie die deutsche und die österreichische Plattform Industrie 4.0; sie haben dazu eigene Arbeitsgruppen gebildet, um ihren Mitgliedern aktive Unterstützung bei der Umsetzung dieser Thematik zu gewähren. Eine Vielzahl von Publikationen, größtenteils frei verfügbar im Internet, sind daraus hervorgegangen.

Im Teil A «Cybersicherheit als Voraussetzung für erfolgreiche Digitalisierung» gehen wir der Frage nach, welche Bedrohungen sich generell durch die Digitalisierung der Industrie ergeben. Das Vorgehen der Angreifer bei gezielten Angriffen wird beschrieben sowie die Auswirkungen von Angriffen auf Produktionssysteme und welche Veränderungen Industrie 4.0 mit sich bringen wird. Cybersicherheit wird als ein inhärenter Bestandteil der Digitalisierung definiert. Die steigende Komplexität verstärkt zunehmend die Verletzlichkeit der installierten Systeme. Neben vielfältigen bekannten Angriffsmethoden wird auch «Cyber Crime as a Service» als neuer Trend erläutert. Es wird die Schlussfolgerung gezogen, dass Digitalisierung und Cybersicherheit einer neuen Kultur des Miteinanders mit erweiterten Formen der Kooperation sowie neue Schutz- und Verteidigungsstrategien bedürfen.

Im Teil B «Regelkonformität mit Normen und Richtlinien» werden ausgesuchte, wichtige Standards vorgestellt. Die Normenreihe ISO/IEC 27000: IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme (ISMS) gibt die Möglichkeit, eine unternehmensweite Strategie im Hinblick auf Informationssicherheit zu etablieren. Mögliche Anwendungsbereiche und der Anwendernutzen von Umsetzungen werden aufgezeigt. Die Normenreihe IEC 62443: Industrielle Kommunikationsnetzte – IT-Sicherheit für Netze und Systeme hat sich zwischenzeitlich mit ihrem Umfang und ihrer Komplexität als der Security-Standard für die Automatisierungstechnik etabliert. Anwendungsbereiche und Umsetzungen werden erläutert. Die Richtlinienreihe VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung stellt ein allgemeines Vorgehensmodell zur Berücksichtigung von Security bei der Herstellung, Integration und Betrieb von industriellen Automatisierungskomponenten bzw. -anlagen vor. Die Anwendung des Vorgehensmodells wird aus Sicht des Herstellers, Integrators bzw. Maschinenbauers und Betreibers beschrieben. Das NAMUR-Arbeitsblatt NA 163: IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen beschreibt ein Verfahren, mit dem die IT-Sicherheit von Prozessleittechnik-Sicherheitssystemen schnell und einfach analysiert werden kann.

Im Teil F «Unternehmensorganisation» definieren wir die Sicherheit als eine feste Säule der Grundsätze der Unternehmensführung. Technik allein bringt noch keine Sicherheit. Deshalb gehen wir der Frage nach, wie nun die Etablierung und das Management von Informationssicherheit und Cyber-Security-Grundsätzen im Unternehmen erfolgen kann. Ein großer Teil aller Cyberbedrohungen kann schon mit gut koordinierten technisch-organisatorischen Methoden abgewehrt werden. Ein Informationssicherheits-Managementsystem (ISMS) dient dabei der Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit in einer Unternehmung. Dazu müssen die Risiken, die die Informationssicherheit bedrohen, identifiziert, bewertet und ihnen mit geeigneten Maßnahmen entgegengewirkt werden. Ein wichtiger Punkt ist dazu ein Identitäts- und Berechtigungsmanagement. Es regelt den unkontrollierten Informationsfluss und den generellen Zugang zu Informationen.

Im Teil G «Risikomanagement» befürworten wir, Risiken durch umfassende Analysen frühzeitig aufzudecken, um sich rechtzeitig auf mögliche Schadensfälle vorzubereiten. Durch systematische Risikomanagementprozesse sowie die Bereitstellung geeigneter Ressourcen für die Cyberabwehr können die Gefahren von Cyberangriffen und mögliche Verwundbarkeiten systematisch reduziert werden. Im Folgenden wird die Integration der operativen Cybertechnologien in das Risikomanagement des Unternehmens dargelegt. Ziel dabei ist es, die sich ergebenen Anforderungen effizient in existierende Risiko-Management-Systeme (RMS) einpassen zu können. Praktische Handlungsanweisungen zur Umsetzung des Risikomanagements für vernetzte industrielle Anwendungen werden vermittelt und die Auswirkungen des Risikomanagements auf den operativen Betrieb aus dem Blickwinkel der Betreiberverantwortung betrachtet. Cyberversicherungen können ebenso als ein Element eines ganzheitlichen Risikomanagements dienen. Sinn und Zweck einer Cyberversicherung für Produktionsbetriebe werden betrachtet.

Mein ganz besonderer Dank gilt Niels Bernau, der durch motivierenden Zuspruch, fachliche Diskussionen und konstruktive Anregungen in hohem Maße zum Gelingen der Arbeit beitrug. Dank sagen möchte ich dem gesamten Team der Vogel Communications Group für ihre freundliche Art und tatkräftige Unterstützung sowie die zahlreichen guten Ideen.

Thomas Schulz

Resonanzen der Verbände

I Zentrale Enabler einer erfolgreichen digitalen Transformation

Durch die Digitalisierung können Unternehmen ihr Produkt- und Serviceportfolio erweitern. Gleichzeitig werden Geschäftsmodelle sowie Kundenbeziehungen neu definiert. Die Dynamik der Entwicklungen befähigt aufstrebende, innovative Player, bereits etablierte Akteure herauszufordern, und erzeugt somit sektorenunabhängig einen wettbewerbsbedingten Digitalisierungsdruck. Zusammen mit den Versprechen der digitalen Transformation hinsichtlich höherer und effizienterer Produktivität schreitet somit nicht nur die intelligente Vernetzung einzelner Elemente der Wertschöpfungskette voran, sondern wächst auch die digitale Angriffsfläche. Um gleichzeitig der fortschreitenden Professionalisierung und Industrialisierung von Cyberkriminalität in allen Erscheinungsformen – Datenmanipulation und -diebstahl oder Sabotage – entgegentreten zu können, sind verschiedene Maßnahmen, sogenannte «Prozess-Enabler», unabdingbar.

Cybersicherheit beruht bisweilen vor allem auf Selbsthilfe und liegt in der Eigenverantwortung der Unternehmen. Hierbei sind angemessene technische Sicherheitsvorkehrungen zwar Grundvoraussetzung, doch Cyberkriminellen genügt in der Regel die Identifikation einer einzigen Schwachstelle, um Netzwerke erfolgreich zu infiltrieren. Aufgrund dieser asymmetrischen Ausgangslage ist es folglich ebenso wichtig, ein konsistent hohes Level an Cyberhygiene – also ein cybersicherheitskonformes Onlineverhalten der Mitarbeiter – durch Kommunikation und Schulungen sicherzustellen. Insgesamt muss Cybersicherheit als der Verantwortungsbereich aller Abteilungen – und nicht nur der IT-Beauftragten – wahrgenommen werden.

Darüber hinaus muss Cybersicherheit aktiv umgesetzt und vorgelebt werden. Oftmals werden Projekte aufgrund sicherheitstechnischer Bedenken verzögert oder sogar abgebrochen, so dass Cybersicherheit als Spielverderber und Hemmnisfaktor interner Prozesse wahrgenommen wird. Zudem stehen entsprechende Ausgaben diametral zu den Wirtschaftlichkeits- und Produktivitätszielen der Geschäftsführung. Dementsprechend muss Cybersicherheit von Anfang an in Entwicklungsprojekte integriert sowie als Wettbewerbsvorteil verstanden werden (Security by Design) und ein offener Dialog zwischen operativer und technischer Ebene zur Vermittlung entsprechender Interessen etabliert werden.

Cyberangriffe richten sich des Weiteren nicht gegen einzelne Einheiten eines Wirtschaftsökosystems. Vielmehr ist die Bedrohungslage transnational und gesamtstaatlich. Privatpersonen, Behörden und Unternehmen, egal ob Großkonzern oder KMU, sind betroffen. Zur Sicherung eines starken Wirtschaftsstandortes braucht es demnach eine flächendeckende Cybersicherheitsarchitektur, die nur durch eine vertrauensvolle sektorenübergreifende Kooperation sichergestellt werden kann. Als zentraler Enabler einer nachhaltig erfolgreichen digitalen Transformation gilt neben angemessenen technischen Sicherheitsvorkehrungen, unternehmensinterner Cyberhygiene und dem Verständnis von Cybersicherheit als Wettbewerbsvorteil zuletzt auch ein Netzwerk der Köpfe. Denn nur durch gemeinsames Handeln, regen Austausch und Know-how-Transfer kann Cybersicherheit nachhaltig verbessert werden.

Hans-Wilhelm Dünn
Präsident – Cyber-Sicherheitsrat Deutschland e.V.

II Modulares Bausteinsystem der Security

Security! Viel zu trocken ist das Thema für die meisten. Viel zu aufwendig und kompliziert für den Anwender. Viel zu teuer für den Controller. Regelrecht muffelig reagieren selbst manche Kollegen im VDMA auf das Thema. Alles übertrieben und bitteschön doch bereits erledigt, Safety macht Security einfach mit. Punkt, aus. Alles darüber hinaus – braucht man nicht, lohnt sich nicht.

Doch doch, Security ist wichtig! Aber: «Security wird erst dann wichtig, wenn was passiert ist», sage ich gerne. Keine Neuigkeit, aber immer noch Realität in den Unternehmen und Amtsstuben weltweit. Spätestens mit Industrie 4.0 eine gefährliche Einstellung, doch peppig aufbereitet kann man sogar ausgesprochene Security-Muffel überzeugen. Dabei hole ich mir gerne die Hilfe von kleinen viereckigen LEGO-Bausteinen, denn die kennt und mag nun wirklich jeder.

12 Gründe, warum LEGO wie Security ist:

- Man braucht keine Superkräfte um es zusammenzubauen.
- Man braucht einen Plan!
- Es geht schneller, wenn man es im Team macht.
- Bei anderen sieht es so großartig aus, bei einem selbst wie bei einem Anfänger.
- Es gibt gefühlte 10 000 verschiedene Bausteine.
- Wenn es drauf ankommt, fehlt genau der eine Baustein.
- Wie viel es kostet, weiß man meist erst nach ein paar Jahren.
- Manchmal muss man kreativ sein.
- Die Herausforderung steigt mit dem Grad der Digitalisierung.
- Am Ende lässt sich alles auf ein paar Basics reduzieren.
- Es gibt Helden auf beiden Seiten.
- Lösungen der Community sind sehr gefragt.

Mein Beitrag bietet nicht genug Platz um jeden einzelnen der zwölf Punkte zu beleuchten. Für den sicheren und zuverlässigen Betrieb von Industrie-4.0-Anlagen kommt es nicht nur auf die Auswahl passender Bausteine an. Vielmehr steht das Zusammenspiel aller Beteiligten im Fokus, angefangen bei Zulieferern von Kommunikationskomponenten über Produktentwickler im Maschinenbau bis hin zu Anlagenbetreibern, Plattformanbietern und Servicegebern. Die Aufgabe: «Shared Responsibilities» – Gemeinsame Verantwortung. Wie in einem Uhrwerk hat jedes Rädchen Aufgaben und Funktionen. Das muss nicht kompliziert sein. Oft geht es darum, die richtigen Dinge zur rechten Zeit anzugehen. Zum Beispiel sollten Produktentwickler Security bereits im Design ihrer Produkte berücksichtigen. Der Aufwand hierfür ist geringer als das Stopfen von Löchern im laufenden Betrieb bei Kunden. Dabei geht es nicht darum, ein hundertprozentig sicheres System zu schaffen, sondern darum, grundsätzliche Funktionalitäten und Geschäftspraktiken zu etablieren.

Der VDMA entwickelt auf Basis der IEC 62 443 das Einheitsblatt 66 418 zur Industrial Security, in dem die Anforderungen an die Produktentwicklung zum Zeitpunkt des Inverkehrbringens von Maschinen und Anlagen nach dem Stand der Technik beschrieben werden. Mit den im Einheitsblatt beschriebenen Bausteinen wird der Maschinen- und Anlagenbau seiner Verantwortung für Industrie 4.0 und darüber hinaus gerecht.

Mein lieber Kollege Peter Früauf hat einmal gesagt, dass Safety der Schutz des Menschen vor der Maschine ist und Security der Schutz der Maschine vor dem Menschen. Diesem Schutz vor den

handwerklichen Fähigkeiten eines Angreifers oder einer Angreiferin ein Gesicht zu geben, war das Ziel dieses Buches. Nun liegt es an Ihnen, liebe Leser, sich Ihrer Verantwortung bewusst zu werden und das Richtige zur richtigen Zeit zu tun.

Steffen Zimmermann
Leiter Competence Center Industrial Security – VDMA Verband Deutscher Maschinen- und Anlagenbau e.V.

III Etablierung einer Sicherheitskultur

Das Verständnis von «Sicherheitskultur» wird oft auf den Aspekt Awareness-Steigerung verkürzt. Im ZVEI verdeutlichen wir daher immer wieder drei Fragen, denen man sich stellen muss, will man eine Sicherheitskultur aufbauen und stärken. Erstens: Was sind der Treiber und Nutzen? Zweitens: Wer sind die zu beteiligenden Partner? Und drittens: Woran erkenne ich Fortschritte und Hindernisse?

Warum braucht es eine Sicherheitskultur überhaupt? Rein betriebswirtschaftlich ist die Antwort eindeutig: Investitionssicherheit. Jede technische Anschaffung für Cybersicherheit wird ihre Wirkung verlieren, wenn die Nutzer und Betroffenen nicht aufmerksam und angemessen damit umgehen. Nimmt man an, dass angesichts der dauerhaften Risikolage Anschaffungen erfolgen werden, braucht es immer den «Faktor Mensch», damit diese Investitionen überhaupt ihre Wirkung erzielen. Zusätzlich ist das Management der Cybersicherheit in einer Organisation im Sinne des «Plan-Do-Check-Act» ohne eine Sicherheitskultur de facto unmöglich. Denn eine etablierte Sicherheitskultur unterstützt alle drei Kernfähigkeiten:

1. Angemessenes Verhalten und Beachtung der Policies (= Prävention)
2. Aufmerksamkeit bei Auffälligkeiten und Verdachtsfällen (= Detektion)
3. Richtiges und schnelles Handeln bei einem Vorfall (= Reaktion)

Bisher betreffen die Punkte vor allem Mitarbeiter innerhalb einer Organisation. Doch es müssen noch mehr Kreise einbezogen werden. Denn insbesondere Geschäftspartner und Gäste sorgen für Security-Herausforderungen, wie z.B. Präsentation über USB-Sticks, keinerlei Security-Vorkehrungen für die E-Mail-Kommunikation, Ablegen von (wichtigen) Dokumenten in öffentlichen Cloudsystemen usw. Achtsame Führungskräfte und Mitarbeiter können in diesen Situationen Hinweise geben, Alternativen anbieten und Grundprinzipien einhalten. Andernfalls werden technische Maßnahmen wieder schnell Makulatur. Darüber hinaus ist der Austausch mit anderen Verantwortungsträgern elementar. IT- oder Sicherheitsbeauftragte können im Kontakt mit Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), anderen externen Kollegen oder Netzwerken wie der Allianz für Cyber-Sicherheit einen realen Mehrwert für die eigene Arbeit und die Organisation als Ganzes gewinnen. Allein der Austausch muss gelebt werden.

Wie geht man eine Sicherheitskultur an? Fakt ist: Sie entsteht nicht von allein. Zunächst braucht es ein klares *Commitment* der Leitung. Zum einen braucht es den Auftrag, die Zeit und das Budget,

die Mitarbeiter bei Cybersicherheit mitzunehmen. Zum anderen müssen meist verschiedene Unternehmensbereiche – bzw. deren Verantwortliche – zusammengebracht werden: z.B. die IT mit der Produktion. Es braucht dauerhaft feste Security-Ansprechpartner und Abstimmungsformate. Das Mandat für eine Sicherheitskultur kommt *top-down*, die Erfahrungen und Praxis jedoch *bottom-up*. Das braucht Formate, Zeit und gegenseitiges Verständnis. Zusätzlich ist Kreativität gefragt. Einfache Webinare oder passive Vortragsrunden zur Cybersicherheit einmal im Jahr bringen die Mitarbeiter selten weiter. Awareness-Kampagnen dürfen nicht nerven und müssen verständlich bleiben. Inzwischen stehen zahlreiche Angebote über *Gamification*, d.h. die spielerische Vermittlung von Inhalten, oder ansprechende Workshops zur Verfügung. Die Einbeziehung von Mitarbeitern ist kein Punkt zum Abhaken auf der Checkliste. Ziel muss es sein, dass die Kollegen Verdachtsmomente erkennen, auch eigene Fehltritte frei melden und stets einen Ansprechpartner finden.

Alle diese Punkte werfen sicherlich weitere Fragen auf. Doch bietet der vorliegende Band einen hervorragenden Einblick in die Rahmenbedingungen und umsetzbaren Maßnahmen – insbesondere für Produktionsunternehmen. In diesem Sinne ist er auch ein Aufruf zum Austausch und Vernetzen. Verbände und andere Plattformen bieten dafür gute Gelegenheiten. Entscheidend ist nun, die hier skizzierten Inhalte aufzugreifen, *Security Lessons Learned* abzufragen und eigene frei zu teilen – das ist gelebte Sicherheitskultur.

Lukas Linke
Senior Manager Cybersecurity – ZVEI Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

IV Wirtschaftsschutz in der digitalen Welt

Das Internet of Things und speziell die Industrie 4.0 haben das Potenzial, der deutschen Wirtschaft sehr große Vorteile zu bringen – Vorteile, die im weltweiten Konkurrenzkampf entscheidend sein werden. Die herausragende Position, die Deutschland im Bereich der produzierenden Industrie innehat, kann nur durch den Einsatz von Industrie 4.0 gesichert werden. Darüber hinaus ermöglicht Industrie 4.0 nicht nur die Sicherung der Position, sondern auch deren Ausbau. Werden Outsourcing und Offshoring-Prozesse umgekehrt, so sichert dies die Arbeitsplätze von heute und ermöglicht die Schaffung neuer Arbeitsplätze von morgen.

Allerdings dürfen bei der Umsetzung wichtige Sicherheitsmechanismen nicht vernachlässigt werden. Fehlende Sicherheit kann schnell zum Bremsklotz der Digitalisierung werden. Beispielsweise gaben in der letzten vom Bitkom durchgeführten Industrie-4.0-Anwenderstudie mehr als 50 Prozent der befragten Unternehmen auf die Frage «Welche Hemmnisse sehen Sie beim Einsatz von Industrie-4.0-Anwendungen in Ihrem Unternehmen?» als Antwort «Anforderungen an die Datensicherheit» an. Unzureichendes Vertrauen in die Datensicherheit ist damit das größte Hemmnis beim Einsatz von Industrie 4.0, direkt hinter Datenschutz und hohen Investitionskosten. Das Ergebnis überrascht nicht, da durch Industrie 4.0 und die erforderliche Vernetzung auf einmal Zugriff von außen auf Maschinen, Systeme und Daten möglich ist, die bis dato abgeschnitten und hinter Firmenmauern sicher verwahrt waren.

Die Auswirkungen, die mangelnde Sicherheit in diesem Kontext verursacht, können unvorstellbar groß sein und können somit sehr schnell die Vorteile überwiegen. Noch ist die Anzahl der dokumentierten Hackerangriffe auf produzierende Unternehmen gering, ihre Zahl wird jedoch im gleichen Verhältnis zum Vernetzungsgrad der Unternehmen steigen. Die Angriffe können vielfältig sein. So können falsche oder veränderte Auftrags- oder Maschinenparameterdaten chargenweise Fehlteile verursachen, die aussortiert werden müssen. Noch schlimmer trifft es Unternehmen, die vernetzt mit anderen Unternehmen arbeiten. Angriffe auf in der Wertschöpfungskette vorgelagerte Unternehmen könnten Kettenreaktionen hervorrufen, die das Potenzial haben, ganze Branchen durcheinander zu bringen.

Die grundlegenden Herausforderungen beginnen jedoch schon viel früher und liegen im Detail. Auch wenn nur eine einzelne Firma betrachtet wird, wachsen zwei Welten zusammen: Office- und Produktions-IT; zwei Welten und zwei Systeme, die bislang streng getrennt wurden, werden nun miteinander vernetzt. Daher muss auch die Sicherheit beider Systeme als Gesamtkonzept betrachtet werden.

In seinem neuen Buch zu Industrie 4.0 legt Thomas Schulz den Schwerpunkt genau auf dieses Thema. Während das erste Buch den Industrie-4.0-Ansatz in einer generellen Art und Weise beleuchtete, spezialisiert sich das vorliegende Werk komplett auf den Sicherheitsaspekt vernetzter Industrie-4.0-Lösungen. Das Thema wird umfassend und aus unterschiedlichen Blickwinkeln von Experten und Praktikern im Leitfaden-Stil analysiert und gibt dem industriellen Anwender die Möglichkeit, Cyber Security für Industrie 4.0 zu verstehen und umzusetzen. Damit leistet es einen wichtigen Beitrag gerade auch für mittelständische Unternehmen, die sich in die Thematik einarbeiten möchten.

Lukas Klingholz
Referent Big Data & Künstliche Intelligenz – Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.