PLATTFORM INDUSTRIE 4.0

LEITFADEN

IT-Security in der Industrie 4.0

Handlungsfelder für Betreiber

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung und Produktion
PRpetuum GmbH, München

Stand
November 2016

Druck
MKL Druck GmbH & Co. KG, Ostbevern

Bildnachweis
traffic_analyzer – iStock (Titel), zapp2photo – Fotolia (S. 5), Mimi Potter – Fotolia (S. 8), putilov_denis – Fotolia (S. 9), contrastwerkstatt – Fotolia (S. 13), Robert Kneschke – Fotolia (S. 14), Sikov - Fotolia (S. 19), industrieblick - Fotolia (S. 20), gen_A – Fotolia (S. 24), Maksim Kabakou – iStock (S. 25), maxsim – Fotolia (S. 29), jijomathai – Fotolia (S. 30), Kzenon – Fotolia (S. 33), Coloures-pic – Fotolia (S. 41)

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhaltsverzeichnis

1 Einleitung und Management Summary

Die digitale Vernetzung der weltweiten Produktion schreitet voran und wird in der vierten industriellen Revolution münden. Das Ausmaß dieser als Industrie 4.0 bezeichneten Entwicklung ist aus heutiger Sicht noch schwer abzuschätzen. Zwischen den verschiedenen Visionen dieser Revolution gibt es einen Konsens: Die weitreichende Vernetzung und fundamentale Neuordnung der klassischen Produktion werden enorme Auswirkungen auf die Gesellschaft haben, die zunehmend auf die Stabilität und das Funktionieren dieser neuen Infrastrukturen vertrauen muss. Die massive Vernetzung der industriellen Produktion kann jedoch nur dann funktionieren, wenn berechtigtes Vertrauen zwischen den Wertschöpfungspartnern besteht. Berechtigtes Vertrauen kann entstehen, wenn der Schutz gegen Bedrohungen (Security) im vereinbarten Umfang von den Akteuren gewährleistet wird, dies überprüfbar ist und den jeweiligen Partnern glaubhaft nachgewiesen werden kann. Die Schutzziele sind dabei die Verfügbarkeit, Integrität, Vertraulichkeit und der rechtskonforme Umgang (z. B. Privacy) der Ressourcen bzw. Daten. Um die Angriffsoberfläche gering zu halten und eine Grundstabilität für die neu entstehenden Infrastrukturen zu gewährleisten, muss der Sicherheitsgedanke fester Bestandteil aller Überlegungen zur Industrie 4.0 sein. Nur ein sorgfältig abgesichertes Produktionssystem ist aktuellen Angriffen gewachsen.

Die Einführung von IT-Sicherheit stellt Maschinen- und Anlagenbetreiber dabei meist vor eine enorme Herausforderung: Sind Handlungsempfehlungen und Sicherheitsmaßnahmen in der klassischen IT-Landschaft zwar hinreichend abgedeckt, so besteht große Unsicherheit in Bezug auf die Digitalisierung der Produktion. Der Anlagenbetreiber auf dem Weg zur Industrie 4.0 sieht sich mit einer großen Vielfalt an Sicherheitsfragen, -lösungen, Standards, Empfehlungen und organisatorischen Rahmenbedingungen konfrontiert, welche nicht immer auf die Bedürfnisse der vernetzten Produktion übertragbar sind. Daher besteht der Bedarf nach maßgeschneiderten Katalogen von Handlungsempfehlungen speziell für die Informationssicherheit in der Produktion.

Zwar bietet das BSI IT-Grundschutz-Handbuch allgemeine Hinweise und die IEC 62443 arbeitet für den Betreiber relevante Themen heraus – dennoch fehlen dem mittelständischen Anlagenbetreiber klare Handlungsfelder für die ersten Schritte in Richtung Sicherheit der vernetzten Produktion.

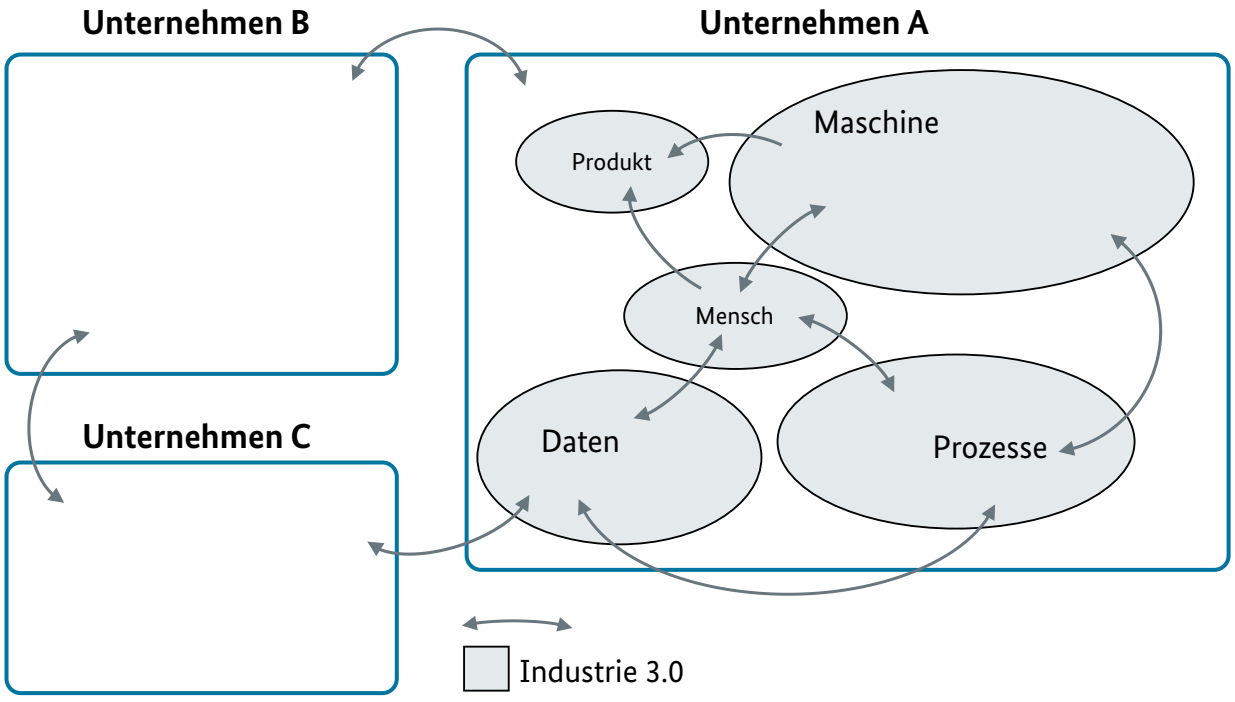
Im vorliegenden Leitfaden werden daher neben den rein technischen Schutzmaßnahmen insbesondere die notwendigen organisatorischen Rahmenbedingungen beschrieben. Dies dient dem Betreiber von Maschinen und Anlagen zunächst zur Selbsteinschätzung, auf deren Basis er die weiteren Handlungsfelder umsetzen kann. Der Betreiber kann mit der Umsetzung nachfolgend beschriebener Maßnahmen und praktischer Hinweise, beispielsweise zu möglichen Anforderungen beim Einkauf von Maschinen und Anlagen, die größten Risiken abdecken und schafft damit die Grundlage, um in Wertschöpfungsnetzwerken mitwirken zu können.

2 Besonderheiten der „vernetzten Produktion“ in Industrie 4.0

Mit der weitreichenden Vernetzung der Produktion im Kontext von Industrie 4.0 ergeben sich IT-Sicherheitsrisiken. Um die Auswirkungen der Vernetzung zu verstehen, wird zunächst auf die Besonderheiten der vernetzten Produktion in der Industrie 4.0 eingegangen. Ziel ist, ein möglichst einheitliches Bild der zu erwartenden Produktionslandschaft zu schaffen, auf dessen Basis nachfolgend Schutzmaßnahmen und Handlungsempfehlungen ausgesprochen werden. Dabei wird besonders auf drei konkrete Ausprägungen von Industrie 4.0 eingegangen: die auftragsgesteuerte Produktion in Wertschöpfungsnetzwerken, die Vernetzung der Produktionsanlagen sowie die Produkt-Maschine-Kommunikation.

Grundsätzlich impliziert Industrie 4.0 die unternehmensübergreifende Vernetzung auf allen Ebenen der klassischen Produktion. Während die Informationsflüsse der Industrie 3.0 im Wesentlichen innerhalb der einzelnen Unternehmen stattfinden (siehe Abbildung 1), kommunizieren Maschinen, Produkte, Anlagenkomponenten und Prozesse über Unternehmensgrenzen hinweg (siehe Abbildung 2).

Abbildung 1: Informationsflüsse der Industrie 3.0



Quelle: Plattform Industrie 4.0

Die klassischen Anlagengrenzen verschwimmen zunehmend. Die Etablierung und Auflösung von Komponenten-, Prozess- oder Anlagenverbünden unterliegen dabei der Dynamik des Wertschöpfungsnetzwerkes: Es können sich beispielsweise kurzzeitig entfernte Maschinen zusammenschließen, um eine geringe Stückzahl eines benötigten Produkts zu fertigen.

2.1 Auftragsgesteuerte Produktion in Wertschöpfungsnetzwerken

Die klassischen Produktionsketten, mit ihren überwiegend hierarchischen Strukturen, werden sich in Industrie 4.0 zunehmend auflösen und von flexiblen Wertschöpfungsnetzwerken zur Produktion wechselnder, kundenindividueller Produkte abgelöst. Dabei bleiben die in der Industrie 3.0 vorhandenen Kommunikationswege weitgehend erhalten, werden jedoch durch die Vernetzung der Unternehmen zum Zwecke des agilen, direkten Austauschs von Informationen ergänzt.

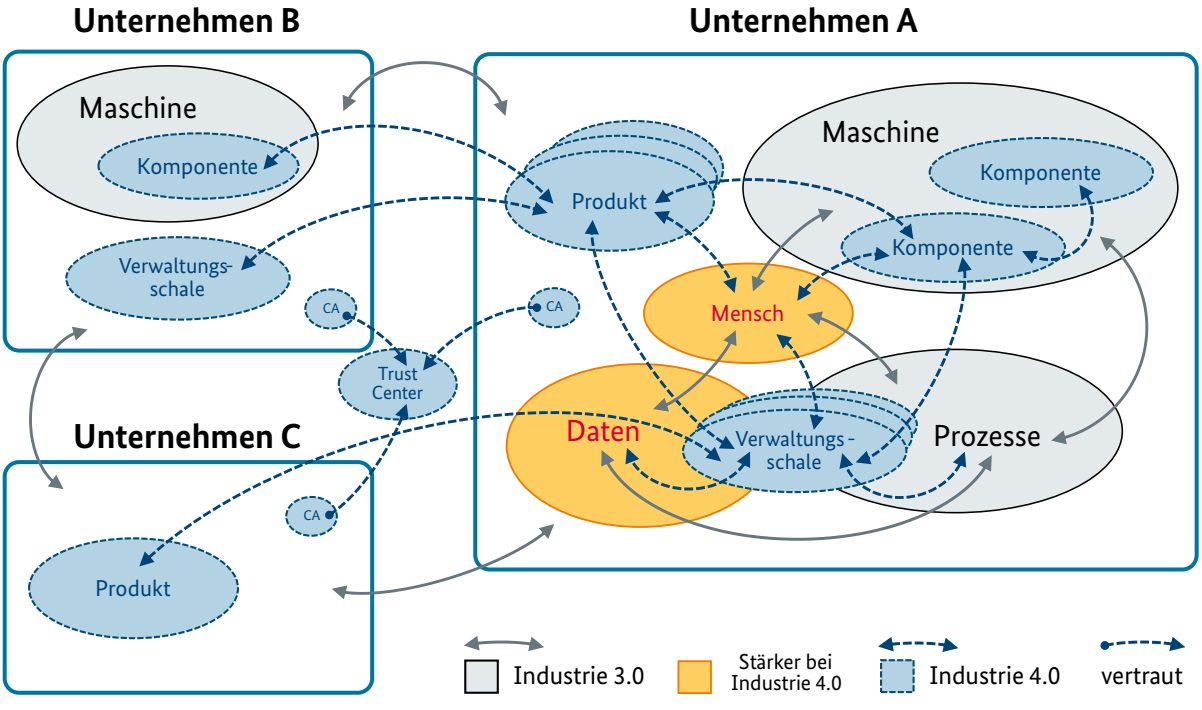
Durch die Bildung von Wertschöpfungsnetzwerken auf Basis eines intensiven, unternehmensübergreifenden Datenaustausches kann der unternehmerische Erfolg durch Effizienzgewinne optimiert werden. Zentrales Kriterium bei der Bildung und kontinuierlichen Verbesserung dieser Wertschöpfungsnetzwerke wird die Möglichkeit zur Herstellung neuer und angefragter Produkte und Dienstleistungen in der gewünschten Menge und Qualität mit der notwendigen Verfügbarkeit sein.

In der Industrie 4.0 werden dementsprechend externe Produktionsressourcen flexibel und dynamisch zur Erweiterung der eigenen Fertigungskompetenzen oder zur Erhöhung der Fertigungskapazitäten in Fertigungsnetz-Strukturen eingebunden werden. Das erfordert sowohl vermehrtes Wissen bezüglich des zu fertigenden Produkts und der notwendigen Fertigungskompetenzen als auch Änderungen in nicht produktiven Bereichen wie der Logistik und dem Lebenszyklus- oder Lieferantenmanagement.

Das Zukunftsszenario „Auftragsgesteuerte Produktion“ geht also wesentlich über die Steuerung eines Auftrages durch die eigene Produktion hinaus. Es geht vielmehr darum, ein bestmögliches Wertschöpfungsnetzwerk zur Erzeugung eines kundenindividuellen Produkts aufzubauen und den Auftrag durch dieses Netzwerk zu steuern. Dabei kann das gesamte Auftragsspektrum vom Einzelstück bis hin zur Großserie abgedeckt werden. Nicht jedes KMU muss so ein Netzwerk etablieren, aber jedes KMU muss in der Lage sein, bei solch einem Netzwerk mitzuwirken, sollen Geschäftsanteile nicht verloren werden.

Die Initiierung dieser Zusammenarbeit wird ebenso wie die dazu notwendige vertikale und horizontale Vernetzung der Produktionssysteme der Netzwerkpartner automatisiert erfolgen. Die technische Vernetzung wird auf Basis sicherer Identitäten und sicherer unternehmensübergreifender Kommunikation umgesetzt werden.

Abbildung 2: Informationsfluss in Industrie 4.0



Quelle: Plattform Industrie 4.0

Die spontane Bildung dieser Wertschöpfungsnetzwerke wird gerade für kleine und mittlere Unternehmen die Voraussetzung schaffen, bei Bedarf ihre Fertigungstiefe unter Hinzuziehung externer Fertigungskompetenzen zu erhöhen, ihre eigenen Fertigungskompetenzen und -kapazitäten in neu entstehenden Wertschöpfungsnetzwerken zu vermarkten oder größere Aufträge anzunehmen und deren Chargen mit Marge auf entsprechenden virtuellen Handelsplätzen „zu brokern“. Durch das auf diese Weise vergrößerte Produktportfolio und die höhere Auslastung der Produktionskapazitäten kann der Gewinn gesteigert und gleichzeitig die Kundenzufriedenheit erhöht werden.

2.2 Vernetzung von Maschinen und Anlagen

Die Umsetzung von Industrie 4.0 in kleinen und mittleren Unternehmen geht mit einem erheblichen Anstieg des Vernetzungsgrades zwischen allen Systemen der Produktion einher. So findet Kommunikation und Datentransfer nicht nur zwischen Geräten einer Anlage oder zwischen Anlagen und ganzen Anlagenverbünden statt, sondern es verschwimmen in zunehmendem Maße auch die vertikalen Grenzen der klassischen Automatisierungspyramide.

Im Gegensatz zur Industrie 3.0 findet unternehmensübergreifende Kommunikation nun auch zwischen den einzelnen Komponenten der gleichen Ebene der Automatisierungspyramide statt, was als horizontale Vernetzung bezeichnet wird. Es wird insbesondere eine starke Zunahme von Maschine-zu-Maschine (M2M)-Kommunikation erwartet. So können sich einzelne Maschinen in verteilten Wertschöpfungsnetzwerken einbinden, um beispielsweise eine optimale Lastverteilung zu ermöglichen. Daraus ergibt sich eine hohe Dynamik der Anlagenverbünde.

Können in der klassischen Produktion die Liefer- und Wertschöpfungsketten noch zentral abgebildet werden, wird deren gesamte Erfassung durch die verteilte Natur der zukünftigen Produktionslandschaft erschwert.

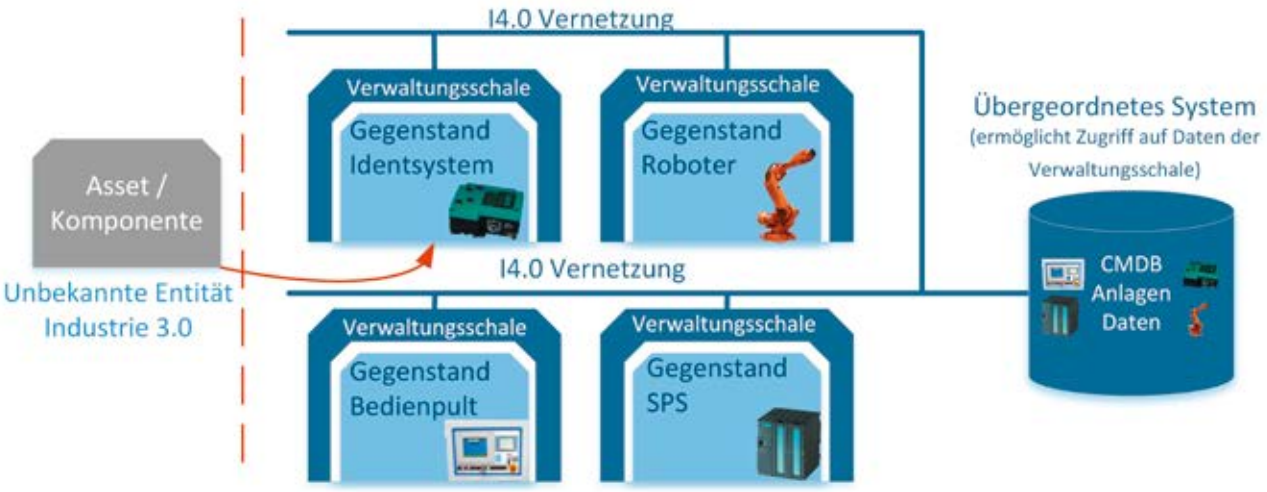
Es ist zu erwarten, dass die Produktionsmaschinen und Anlagen eigenständig die erforderlichen Ressourcen planen und entsprechende Bestellprozesse an zuliefernden Anlagen in die Wege leiten. Produktions- und Materialflüsse der Industrie 4.0 werden dann dezentral von den an der Wertschöpfung beteiligten Produktionsmaschinen gesteuert. Der Planungsprozess des Materialflusses verlagert sich und wird horizontal über mehrere Anlagen und Anlagenverbünde organisiert.

Gerade der hohe Grad an Vernetzung eröffnet viele potenzielle Einstiegspunkte für Angreifer, eine übergreifende Absicherung aller am Wertschöpfungsnetzwerk beteiligten Komponenten ist daher unabdingbar.

2.3 Produkt-Maschine-Kommunikation

Kommunikation und Datenaustausch findet nicht nur zwischen Maschinen statt, sondern auch zwischen Produkt und Maschine oder den Komponenten der Industrie 4.0. Beispielsweise ist für jedes Produkt ein virtuelles Gegenstück denkbar, das sämtliche Anforderungen und Parameter der relevanten Produktionsschritte an die das Produkt verarbeitende Maschine weiterleitet. Im Zusammenhang mit Industrie 4.0 wird hier von der Verwaltungsschale[1] gesprochen: Sie speichert das virtuelle Abbild des Produkts, das sämtliche zur Fertigung und Betrieb notwendigen Daten enthält. Zusätzlich zu den Komponentendaten bietet die Verwaltungsschale auch Funktionen und Dienste an,

Abbildung 3: Verwaltungsschale als Träger der Asset-Information



Quelle: Plattform Industrie 4.0

1 Vgl. ZVEI (Hrsg.) (2015)

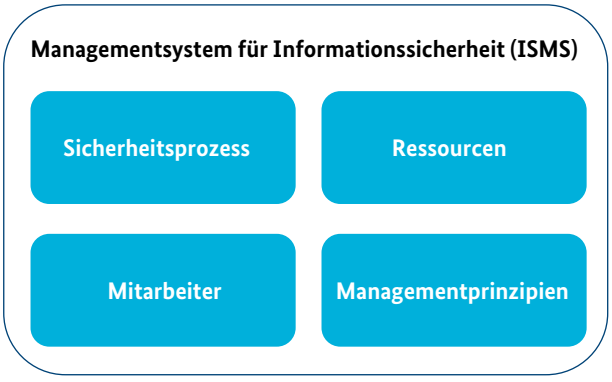
die speziell an das Produkt angepasst sind. Die Maschine kann sich so beispielsweise individuell auf die produktspezifischen Fertigungsprozesse einstellen. Der Fertigungsprozess des Produkts kann sich so über viele verteilte Maschinen und Anlagen erstrecken, ohne dass eine zentrale Kontrolle der beteiligten Maschinen notwendig ist. Nach Fertigstellung ist auch die Übermittlung weiterer Daten denkbar. Beispielsweise könnte die Maschine dem Produkt eine Frühwarnung schicken, falls in einer bestimmten Serie ein Defekt bekannt wurde und sämtliche Produkte der Serie ersetzt werden müssen. Auch ist die Übermittlung von Daten seitens des Produkts denkbar. Erhält die Maschine beispielsweise die Information, dass ein großer Teil der produzierten Produkte im Nachgang mit einer Komponente eines bestimmten Typs bestückt werden, so könnte die Maschine eine entsprechende Optimierung in Logistik und Preisermittlung (bei automatischem Handel auf digitalen Marktplätzen) einleiten.

3 Organisation, Prozesse und Zuständigkeiten

Eine der größten aktuellen und zukünftigen Herausforderungen stellt die Schaffung und Aufrechterhaltung eines geeigneten IT-Sicherheitsniveaus dar. Insbesondere für kleine und mittelständische Unternehmen (KMUs) der Industrie ist dies aus eigener Kraft kaum zu bewältigen. Die IT-Sicherheit ist ein Projekt, bei dem alle mitmachen müssen und Anpassungen der Organisation notwendig sind. Weiterhin müssen neue Prozesse definiert und neue Ressourcen sowie Zuständigkeiten geschaffen werden. Dies gilt für die klassische Office-IT ebenso wie für die Produktions-IT. Viele der notwendigen Managementprinzipien sind für die Office-IT bereits umgesetzt, während die IT-Sicherheit in der Produktion typischerweise gar nicht oder nur unzureichend verwaltet wird. Im Folgenden werden daher grundlegende Prinzipien zur Schaffung von IT-Sicherheit mit Fokus auf die Produktion aufgezeigt. Hierbei wird sich hauptsächlich an den Empfehlungen aus dem BSI IT-Grundschutz orientiert.

Die im Folgenden vorgestellten Konzepte sind die gleichen, wie für alle Managementsysteme (z. B. Qualitätsmanagement, Umwelt, Safety). Die hier vorgestellten Strukturen und Prozesse sollten daher schon an vielen weiteren Stellen des Unternehmens vorhanden und vertraut sein. Diese Prinzipien und Prozesse gilt es jetzt auch für die Security einzuführen und anzuwenden.

Abbildung 4: Managementsystem für Informationssicherheit (ISMS)



Quelle: nach BSI (Hrsg.) (2008a), S. 14

3.1 Managementsystem für Informationssicherheit (ISMS)

„Das ISMS legt fest, mit welchen Instrumenten und Methoden das Management die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert)." Es ist damit eine Unterstützung für das Management, um die Ziele der Informationssicherheit erreichen zu können, das Unternehmensrisiko zu minimieren und regulatorische Anforderungen zu erfüllen. Es wird im Rahmen des BSI-Standards 100-1[2] beschrieben und setzt sich aus den vier Komponenten Sicherheitsprozess, Ressourcen, Mitarbeiter und Managementprinzipien zusammen (siehe Abbildung 4).

2 Vgl. BSI (Hrsg.) (2008a)

Mit der Einführung von einem **Sicherheitsprozess** werden unter anderem die notwendigen organisatorischen Veränderungen eingeleitet und Hilfsmittel zur Erreichung der Ziele aus der Sicherheitsstrategie erarbeitet. Aufgrund der übergeordneten Bedeutung des Sicherheitsprozesses wird dieser im nachfolgenden Abschnitt detaillierter betrachtet.

Für die Komponente des ISMS **Ressourcen** wird insbesondere auf die Verantwortlichkeiten des Managements hingewiesen. Es wird betont, dass in der Praxis den für die Sicherheit Verantwortlichen häufig die Zeit oder auch die Grundlagen fehlen, um sich ausreichend mit sicherheitsrelevanten Themen (z. B. gesetzliche Anforderungen oder technische Fragen) auseinanderzusetzen. In solchen Fällen wird empfohlen, auf externe Experten zurückzugreifen.[3]

Mit der ISMS-Komponente **Mitarbeiter** wird deutlich gemacht, dass Informationssicherheit ohne Ausnahme alle Mitarbeiter betrifft und das Handeln eines jeden Einzelnen erfolgsentscheidend sein kann. Daher sind alle Mitarbeiter in den Sicherheitsprozess einzubeziehen. Jeder Einzelne kann durch verantwortungs- und qualitätsbewusstes Handeln Schäden vermeiden und zum Erfolg beitragen.[4]

Für die Erreichung der unternehmensinternen und der gesetzlichen Anforderungen an die Informationssicherheit sind **Managementprinzipien** eine unverzichtbare Grundlage. Da hier in der Praxis starker Nachholbedarf besteht, fasst das BSI sechs Aufgaben und Pflichten der Leitungsebene zusammen.[5]

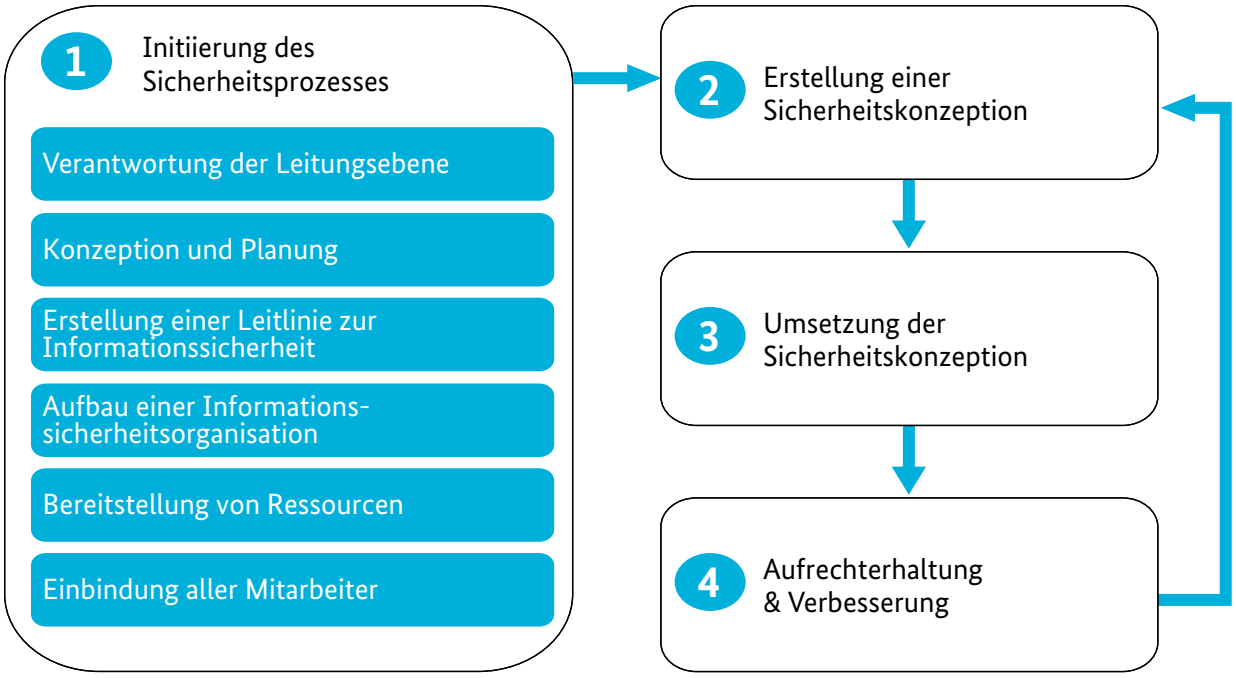
Auch wenn ein solches ISMS bereits im Unternehmen umgesetzt ist, beschränkt es sich zumeist auf die Office-IT und bedarf der Erweiterung auf die Produktions-IT. In den seltensten Fällen sind separate Ressourcen, Mitarbeiter, Prozesse und Managementprinzipien auch für die Produktion vorhanden bzw. definiert. Hier müssen Unternehmen, insbesondere die Betreiber von Maschinen und Anlagen, dringend nachsteuern.

KMUs, bei denen noch keinerlei Management der Informationssicherheit (IS-Management) eingeführt wurde, sind hier noch dringender zum Handeln aufgerufen. In diesem Fall sollten die besonderen Anforderungen der Produktion von Beginn an berücksichtigt und entsprechend angepasste Konzepte erarbeitet werden.

3.2 Sicherheitsprozess

Der Sicherheitsprozess stellt ein zentrales Element des Managementsystems für die Informationssicherheit dar

Abbildung 5: Phasen des Sicherheitsprozesses



Quelle: nach BSI (Hrsg.) (2008b), S. 13

3 Vgl. BSI (Hrsg.) (2008a), S. 22
4 Vgl. BSI (Hrsg.) (2008a), S. 23
5 Vgl. BSI (Hrsg.) (2008a), S. 17 f

und hilft bei der Einführung und Aufrechterhaltung eines geeigneten IT-Sicherheitsniveaus. Die vier Phasen des Prozesses sind in Abbildung 5 dargestellt. Aufgrund von gesetzlichen Anforderungen und Regelungen hat die Unternehmensleitung die volle Verantwortung, den Sicherheitsprozess aufzusetzen und und dessen Einhaltung zu gewährleisten.

Das IT-Sicherheitsmanagement ist als zyklischer Prozess zu verstehen, welcher Phasen-Planung, Umsetzung der Planung, Erfolgskontrolle und Beseitigung von erkannten Mängeln und Schwächen umfasst. Dieses PDCA[6]-Modell ist weit verbreitet und findet beispielsweise auch in ISO 27001 und weiteren Standards zur Gestaltung von Managementsystemen Anwendung. Das Modell kann auch auf einzelne Komponenten des Sicherheitsprozesses wie beispielsweise das Sicherheitskonzept angewendet werden.

Wesentliches Element des Sicherheitsprozesses ist die Sicherheitsleitlinie, mit der die Zielsetzungen und Erwartungshaltung im Unternehmen festgelegt werden. Die Sicherheitsleitlinie muss alle Mitarbeiter erreichen, damit sie die notwendige Aufmerksamkeit für Risiken in ihrem Tätigkeitsfeld entwickeln können. Zu diesem Zweck sollte die Sicherheitsleitlinie schriftlich fixiert und möglichst einfach formuliert und zugänglich sein. Die Sicherheitsleitlinie wird dann entsprechend dem Kreislaufcharakter des Sicherheitsprozesses kontinuierlich verbessert.

Der Sicherheitsprozess muss unternehmensweit umgesetzt werden, damit das angestrebte Sicherheitsniveau erreicht werden kann. Aufgrund dieses übergreifenden Charakters sind verantwortliche Rollen einzuführen.

3.3 Rollen und Zuständigkeiten

Bevor auf die einzelnen Rollen und Zuständigkeiten eingegangen wird, sollen hier drei Grundregeln für die Definition von Rollen im Kontext des Unternehmens und seines ISMS aufgezeigt werden:

1. Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit für die Informationssicherheit) verbleibt bei der Leitungsebene.

2. Mindestens eine Person (typischerweise der **IT-Sicherheitsbeauftragte**) fördert und koordiniert den Informationssicherheitsprozess.

3. Jeder Mitarbeiter ist im Kontext seiner Aufgabe und seines Arbeitsplatzes verantwortlich für die Aufrechterhaltung der IT-Sicherheit.

Die genannten Grundregeln beziehen sich auf die Umsetzung des ISMS in allen Teilen des Unternehmens, also Produktion und Verwaltung gleichermaßen. Eine besondere Rolle kommt dabei dem IT-Sicherheitsbeauftragten zu, auf welchen im Folgenden eingegangen wird. Erst im zweiten Schritt erfolgen konkrete Forderungen für die Abbildung der Sicherheit in der Produktion im ISMS und den notwendigen Rollen.

3.3.1 IT-Sicherheitsbeauftragter und Informationssicherheitsteam

Der IT-Grundschutz empfiehlt, für die Einführung und Umsetzung eines Sicherheitsprozesses sowohl IT-Sicherheitsbeauftragte als auch ein Informationssicherheitsteam einzusetzen und mit notwendigen Ressourcen auszustatten. Der IT-Sicherheitsbeauftragte ist in der Organisation zuständig für alle Fragen rund um die Informationssicherheit; dies schließt die Produktion, deren IT-Komponenten und Prozesse mit ein. Idealerweise ist er organisatorisch unabhängig, d. h. als Stabsstelle implementiert. Er hat wichtige Aufgaben inne, zu welchen u. a. nachfolgend genannte zählen:

- Steuern und Koordinieren des Sicherheitsprozesses
- Unterstützung der Unternehmensleitung bei der Erstellung der Sicherheitsleitlinie
- Koordination sicherheitsrelevanter Projekte
- Untersuchung sicherheitsrelevanter Vorfälle
- Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit

Unterstützt wird der IT-Sicherheitsbeauftragte vom Informationssicherheitsteam, welches aus Zuständigen für Informationssicherheit gebildet wird.

In kleineren Organisationen können diese Aufgaben auch von wenigen bzw. einer Person – in diesem Falle dem IT-Sicherheitsbeauftragten – wahrgenommen werden. Wichtig ist, dass die Governance, also die Organisation und Verwaltung der Informationssicherheit für Produktion und Verwaltung, einheitlich und von einer Organisationseinheit in ihrer Gesamtheit ausgeübt wird, um ein gleichmäßiges Sicherheitsniveau zu erreichen.

6 PDCA ist die Abkürzung für Plan, Do, Check, Act (Planen, Handeln, Prüfen, Nachsteuern).

3.3.2 Industrial Security Officer

Die bisherige Trennung von Office-IT und Produktions-IT führt zu Maßnahmen, die die Auswirkungen in den jeweiligen anderen Bereichen nicht berücksichtigen. Daher ist die Überwindung dieses Silodenkens zwingend notwendig. Es wird eine Überblickskompetenz erforderlich, deren Dringlichkeit mit zunehmendem Vernetzungsgrad steigt.

Es wird also ein „Kümmerer" benötigt, der die Security bereichsübergreifend gestaltet und standortweit steuert. Diese Funktion muss entsprechend organisatorisch eingebunden und mit den notwendigen Kompetenzen ausgestattet werden.

Kriterien, wie die Unternehmensgröße, Know-how und Wissensanforderungen in der jeweiligen Verantwortungsrolle, werden die Organisation der Securityverantwortung zukünftig bestimmen.

Es kann sich beispielsweise anbieten, eine eigene Stelle für dieses Aufgabenfeld im Sinne eines Chief (Information) Security Officer (C(I)SO) zu schaffen, der gleichermaßen für die Konzeption und Umsetzung der Sicherheitsmaßnahmen sowohl in Office-, Produktions-IT und der Produktentwicklung verantwortlich ist. Solche Stellen (oder Positionen) sind in der Regel bei größeren Unternehmen bereits eingeführt, jedoch liegt deren Fokus bisher auf der Office-IT. Die Bereiche Industrial Security und/oder die Security der Produktentwicklung werden in dieser Verantwortungsrolle nur selten berücksichtigt (vgl. Abbildung 6).

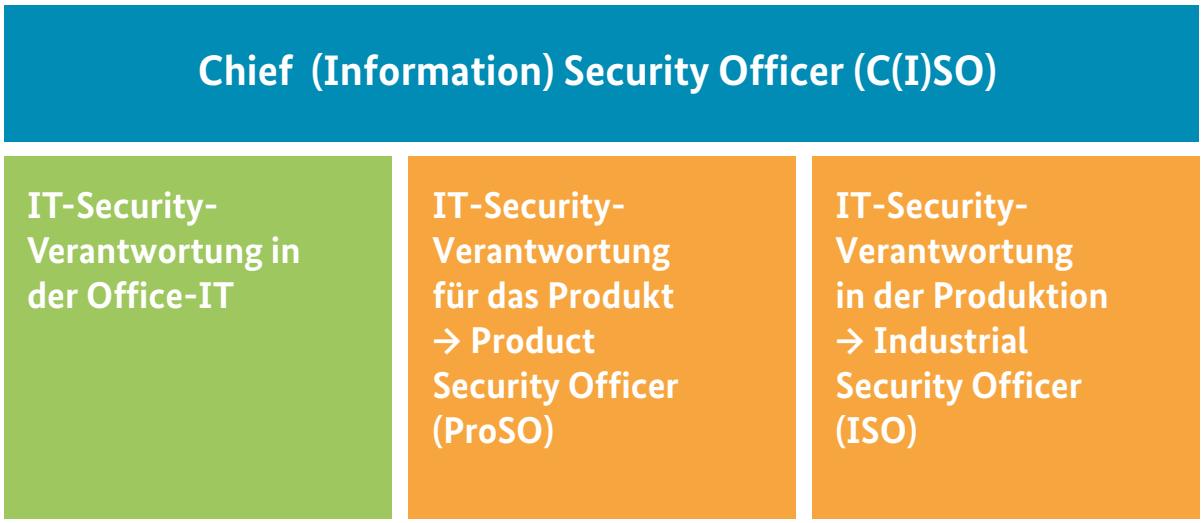
Rollenkonzepte, in denen sich ein C(I)SO und eine korrespondierende Rolle für die Produktion, etwa ein Industrial C(I)SO, miteinander die Verantwortungsaspekte teilen, sind ebenfalls denkbar.

Der verantwortliche C(I)SO kann durch bereichsspezifische Rollen aus der Office-IT, der Produktions-IT (Industrial Security Officer (ISO)) sowie der Produktentwicklung (Product Security Officer (ProSO)) operativ unterstützt werden. Die Einbeziehung aller spezifischen Governance- und Maßnahmenaspekte muss dabei passfähig gewährleistet sein. Es ist jedoch davon auszugehen, dass gerade bei kleinen und mittleren Unternehmen mehrere Rollenfunktionen häufig in Personalunion geführt werden müssen.

Der Industrial Security Officer übernimmt die Verantwortung für die Gewährung der Schutzziele in der Produktion und muss über IT, IT-Sicherheits-, Ingenieurs- und Managementkenntnisse sowie spezifische Soft Skills verfügen, um die produktionsspezifischen Sicherheitsmaßnahmen zu konzeptionieren und deren Umsetzung vor dem Hintergrund der gültigen Governance zu managen. Zur organisatorischen Einbindung und zum Kompetenzprofil eines Industrial Security Officer können weitere Details der Publikation „Securityanforderungen an die Aus- und Weiterbildung von Mitarbeitern im Kontext Industrie 4.0" der Plattform Industrie 4.0 entnommen werden.

Ebenso übernimmt der Product Security Officer (ProSO) die Verantwortung für den Schutz der erzeugten Produkte und über deren Lebenszyklus hinweg, angefangen bei der Produktkonzeption und Entwicklung über technische Dienstleitung während des Einsatzes beim Kunden,

Abbildung 6: Aufgabenfelder eines Chief (Information) Security Officer



Quelle: Plattform Industrie 4.0

beispielsweise mit Updates der Software mit neuen Securityfunktionen, bis hin zur Auflösung oder Rücknahme.

3.4 Kompetenzen

Die Verfügbarkeit des notwendigen (Security-)Wissens und der Kompetenzen ist essentiell für die Einführung und Durchsetzung des IT-Sicherheitskonzepts. Jeder Mitarbeiter des Unternehmens muss in der Lage sein, die in seinem Arbeitsbereich und in der jeweiligen Lebenszyklusphase relevanten Securityanforderungen zu berücksichtigen. Ihm muss die Gelegenheit gegeben werden, die notwendigen Kenntnisse und Fertigkeiten zu erwerben und anzuwenden. Gleichzeitig muss ein grundlegendes Bewusstsein hinsichtlich Sicherheit und möglicher Sicherheitsrisiken der IT in der Produktion vorhanden sein (vgl. nächster Abschnitt).

Bereits im Bereich der Standard-IT ist es kleinen und mittleren Unternehmen häufig kaum möglich, mit den wachsenden Anforderungen an Spezialisierung und Qualifikation Schritt zu halten, daher wird auf die Unterstützung durch externe Spezialisten und Dienstleister zurückgegriffen. Neben einem Ausbau der internen Kompetenzen können also auch Dienstleister beispielsweise durch Rahmenverträge oder Abrufleistungen eingebunden werden.

3.4.1 Sachkenntnisse der Mitarbeiter

Bei der ganzheitlichen Durchsetzung von IT-Sicherheit ist der „Faktor Mensch“ elementar, was dazu führt, dass Sachkenntnisse bezüglich des richtigen Verhaltens und des Umgangs mit IT-Sicherheit entsprechend geschult werden müssen. Damit alle Mitarbeiter eines Unternehmens entsprechend ihrem Aufgabengebiet handlungsfähig sind, müssen Grundlagen von Informationstechnologie und Informationssicherheit unternehmensweit geschult werden. Darüber hinaus müssen Mitarbeiter in entsprechenden Rollen oder Funktionen erweiterte Kenntnisse und gegebenenfalls auch Expertenkenntnisse zu IT-Sicherheit, Netzwerksicherheit und den Besonderheiten von IT und IT-Sicherheit im Bereich der Produktion nachweisen können.

Damit einher geht auch die Forderung, etablierte Berufsfelder entsprechend zu erweitern und an den Erfordernissen der Industrie 4.0 auszurichten.[7] Ebenfalls in der Entwicklung sind entsprechende Weiterbildungsmaßnahmen, um die Mitarbeiter zeitgemäß zu qualifizieren.

3.4.2 Trainingsmethoden

Im Kontext zu planender Schulungen muss auf eine zielgruppengerechte Aufbereitung der Inhalte und die Wahl geeigneter Trainingsmethoden geachtet werden. Bei dieser Wahl sind besonders die unterschiedlich ausgeprägten Kenntnisse der Mitarbeiter und deren Tätigkeitsfeld im Unternehmen zu berücksichtigen.

Die Schulungsaktivitäten sollten darüber hinaus so gestaltet sein, dass sie verpflichtend, nachweisbar und dokumentiert sind. Auch die Inhalte der Schulungen müssen Teil des ganzheitlichen Sicherheitsprozesses sein und sind regelmäßig zu verbessern.

Die Schulungsinhalte sollten hierbei in enger Zusammenarbeit zwischen Personalabteilung, den Verantwortlichen für IT-Sicherheit und dem Management des Unternehmens erarbeitet und abgestimmt werden. Die Personalabteilung ist primär durch ihren Auftrag für Betreuung des Personals sowie dessen Weiterbildung und Schulung mit einzubeziehen, sollte aber auch im größeren Kontext der Industrie 4.0 entsprechende Maßnahmen zur Qualifikation begleiten.

Die Schulungen können dann – je nach Qualifikation und Freiraum für die Erstellung der Materialien – von internen Mitarbeitern, in Zusammenarbeit mit Externen oder gänzlich von Externen durchgeführt werden. Die Umsetzung folgt im Wesentlichen den Anforderungen und Möglichkeiten des Unternehmens.

7 So wird z. B. mit den IHKs diskutiert, ob das Berufsfeld eines Cyber-Mechatronikers als Ausbildungsberuf definiert werden soll.

4 Risiko-Management

Um sinnvoll und nachhaltig Risiko-Management betreiben zu können, ist zunächst die Kenntnis der zu schützenden Unternehmenswerte notwendig. Im Sicherheitskontext werden die zu schützenden Unternehmenswerte Assets genannt. Ohne eine solche Liste der der zu schützenden Assets (etwa Prozess-Know-how im Sinne von Fertigungsparametern oder Rezepturen) ist es nicht möglich, die Maßnahmen für mehr IT-Sicherheit richtig zu priorisieren. Es ist also notwendig, die kritischen wertschöpfenden Prozesse zu erkennen, die beteiligten Komponenten und Informationen zu dokumentieren und dann den Schutzbedarf Assets-spezifisch, also für die zu schützenden Unternehmenswerte abzuleiten. Darauf folgt eine Bedrohungsanalyse, die die nicht relevanten Bedrohungen von denen abgrenzt, die auf die kritischen Assets einwirken können. Letztlich betrachtet man die möglichen Schwachstellen, die die Assets gefährden und denen relevante Bedrohungen gegenüberstehen. Diese müssen mit einer Eintrittswahrscheinlichkeit belegt werden, um Risikowerte ableiten zu können.

4.1 Zu schützende Unternehmenswerte (Assets) als Basis für die Risikobetrachtung

Die Kenntnis der zu schützenden Informationen, der (Informations-)Assets, ist die Basis für alle Bewertungen. Die nachfolgenden Abschnitte grenzen die Aufgaben des Asset-Managements als Basis für das Risiko-Management ab.

4.1.1 Abgrenzung der schützenswerten Assets

Die Bezeichnung Assets bezieht sich auf alle zu schützenden Unternehmenswerte, sie umfasst also sowohl physische Gegenstände als auch geistiges Eigentum wie geheime Rezepturen oder Kenntnisse über bestimmte Produktionsverfahren und deren Parameter. Geheime Rezepturen und Verfahren werden von jeher streng geschützt, etwa durch Aufbewahrung in Tresoren (Papier) oder durch verschlüsselte Speicherung. Für Hardware Assets ist es in der Office-IT bereits Standard, alle vorhandenen Geräte vor der ersten Verwendung in einer Asset-Datenbank zu erfassen (Configuration Management Database, CMDB, genannt). Den Geräten wird typischerweise eine Asset-ID zugeordnet und es findet eine erste Klassifizierung statt. Auch technische Detailinformationen können und sollen hier hinterlegt werden. Durch diese Form des Asset-Managements erhalten Unternehmen einen Überblick zu den vorhandenen Geräten und der vorhandenen IT-Infrastruktur. Auf Basis dieses Überblicks kann jederzeit eine Risikobewertung der vorhandenen Assets vorgenommen werden. Auf Basis der vorhandenen Assets und deren Risiko-Einstufungen müssen Entscheidungen bezüglich des vorzusehenden Schutzniveaus getroffen und entsprechende Maßnahmen abgeleitet werden. Der Fokus muss hierbei auf dem Schutz der Kernkompetenzen und der kritischen Daten liegen. Dies können z. B. Verfahrensanweisungen, Produktdaten oder Fertigungstechnologien sein.

4.1.2 Asset-Management-Herausforderungen in der Produktion

In der Produktion ist ein vollständiger Überblick zu den vorhandenen Assets nur selten vorhanden. Es ist daher unbedingt notwendig, die in der Produktion vorhandenen Komponenten im Detail zu erfassen, um ein angepasstes Schutzkonzept überhaupt erarbeiten zu können. Im Detail bedeutet dabei, dass eine Produktionsanlage beispielsweise

Abbildung 7: Grundlegende Informationen zur Verwaltung von Assets

Quelle: Plattform Industrie 4.0

nicht mehr als nur eine Anlage erfasst werden kann, sondern eine Aufgliederung in die verbauten Komponenten notwendig ist. Es ist beispielsweise zu dokumentieren, welche Anlagenkomponente über welche Kommunikationsmöglichkeiten aus dem System heraus verfügt. Mit den zunehmend vernetzten und in der Anlage enthaltenen IT-Komponenten gehen viele Schwachstellen und damit Bedrohungen für die IT-Sicherheit einher, da die (teilweise bereits bei Lieferung veralteten) IT-Komponenten bereits unsicher sind, oder es durch fehlende Updates schnell werden können. Es ist daher erforderlich, die einzelnen (IT-) Komponenten der Anlage genau zu erfassen und im Detail zu dokumentieren, um bei Bekanntwerden von Sicherheitslücken gezielt entsprechende Maßnahmen einleiten zu können. Einen ersten Ansatz hierzu findet man in Information Technology Infrastructure Library (ITIL) als auch in der Beschreibung der IEC 62443 zu Systemen und Komponenten.

Da eine Aufstellung der enthaltenen IT-Komponenten häufig nicht in dem üblichen Lieferumfang oder der Dokumentation enthalten ist, müssen die IT-Assets meist mühsam manuell erfasst werden. Die Tätigkeiten rund um das Asset-Management sind dringend in Prozessen zu beschreiben und müssen aktiv durch neu geschaffene Verantwortlichkeiten in der Produktion vorangetrieben werden.

4.1.3 Vorgehen zur Verwaltung von Assets

Um eine geeignete Verwaltung der Assets zu ermöglichen, sind diesen entsprechende Informationen, wie z. B. die Verantwortlichkeiten, zuzuordnen, d. h. es ist zunächst eine entsprechende Bestandsaufnahme durchzuführen. Alle Informationen sind entsprechend zu dokumentieren und müssen in regelmäßigen Abständen aktualisiert werden. Mit der Einführung eines Asset-Managements sind die folgenden Schritte durchzuführen und die zugehörigen Fragestellungen zu beantworten (siehe Abbildung 7):

4.1.4 Bestandsaufnahme der vorhandenen Assets

Die Bestandsaufnahme der Assets ist der erste Schritt in dem Prozess des Assets-Managements bzw. zur Verwaltung und Administration der vorhandenen IT-Komponenten. Prinzipiell stehen in der IT diverse Tools zur automatisierten Erfassung und Speicherung dieser Komponenten zur Verfügung. Hiervon sind allerdings nur wenige auch für die Erfassung von Produktions-Assets geeignet, da diesen bislang häufig die erforderlichen Schnittstellen fehlen. Der Einsatz von Agenten zur Asset-Erfassung wird in der Regel durch die Integratoren der Anlagen aus Gründen der Stabilität abgelehnt. Es bietet sich deshalb an, schon bei der Lieferung einer Anlage ein umfassendes Verzeichnis der verwendeten Komponenten vom Lieferanten einzufordern beziehungsweise als Abnahmebedingung zu definieren. Für Bestandssysteme bleibt die manuelle Erfassung und Dokumentation in eigenen Datenbanken – oder zunächst zumindest in Excel-Tabellen – die einzige Alternative. Um Änderungen zumindest in IP-basierten Netzen leicht erkennen zu können, bieten sich zudem passive Überwachungswerkzeuge an, die sowohl neue IP- als auch MAC-Adressen erkennen und entsprechende Benachrichtigungen versenden.

4.1.5 Konfigurationsverwaltung

Eine Art, Assets zu dokumentieren, stellt die Nomenklatur in sogenannten „Configuration Items“ (CI) dar, wie sie im Rahmen der Prozesse der IT Infrastructure Library (ITIL) genutzt wird. Unter der Bezeichnung Configuration Items werden in ITIL alle Betriebsmittel der IT verstanden. Die Verwaltung von Zugriffen auf Configuration Items und deren Konfiguration lässt sich mittels Datenbanken abbilden, die man als Configuration Management Database (CMDB) bezeichnet. Eine CMDB dient der Zusammenführung aller Informationen, die zu einem Configuration Item vorliegen. Nicht selten sind verfügbare Informationen – insbesondere zu Produktions-Assets – im Unternehmen auf verschiedene Datenbanken verteilt. Die CMDB bietet die Möglichkeit, Informationen zusammenzuführen, ohne dass diese zwangsläufig zentralisiert abgelegt werden müssen (föderiertes Datenbankmanagement).

4.2 Daten(-fluss)-Analyse und Datenklassifikation

Für eine Risikoanalyse ist es notwendig, neben den kritischen Assets auch die relevanten Kommunikationsbeziehungen und die daran beteiligten Komponenten zu kennen und die verschiedenen Datenströme zu erfassen, auf Basis derer die Produktionsprozesse ablaufen. Hierfür ist es notwendig, die Verbindungen zwischen den Komponenten, die ausgetauschten Daten und genutzten Protokolle zu kennen und zu dokumentieren. Um diese Übersicht im Bestand zu erhalten, bietet sich die Nutzung von Netzwerkanalysetools an.

Sobald die Datenströme übersichtlich erfasst wurden, sollten diese einer Klassifizierung unterzogen werden, um Erkenntnisse über mögliche Zonen oder Schutzbedarfe ableiten zu können. Leider basieren viele etablierte Klassifikationssysteme und automatisierte Tools auf der Annahme, dass die Vertraulichkeit das primäre Schutzziel sei. Dies leitet sich aus der Herkunft der Klassifikationsstufen aus dem Datenschutz ab.

Für die Produktion ist es jedoch erforderlich, auch Anforderungen an Laufzeiten (Echtzeitanforderungen), Integrität und Authentizität zu erfassen und per Klassifikation abbilden zu können. Die Erfassung von Daten und deren Klassifizierung in der Produktion wird mit steigender Vernetzung und Komplexität von Maschinen und Anlagen immer relevanter für die IT-Sicherheit, da immer mehr Kommunikationspartner einbezogen werden, was zwangsläufig zu mehr Angriffsflächen führt.

Für die Umsetzung eines IT-Sicherheitskonzepts ist es sinnvoll, Daten insbesondere bezüglich ihres Wertes bzw. der Sensibilität und der daraus resultierenden Schutzwürdigkeit zu klassifizieren. Der individuelle Schutzbedarf wird in der Regel im Rahmen einer Risikoanalyse festgelegt. Im Kontext von Industrie 4.0 wird hier die Forderung nach einer unternehmensübergreifenden und standardisierten Klassifizierung von Daten gestellt, um bezüglich der Klassifizierung interoperabel zu sein und Missverständnissen vorzubeugen. Ein Vorschlag für ein einheitliches und einfaches Klassifikationsschema wird in dem Ergebnispapier „Sichere unternehmensübergreifende Kommunikation“ der Plattform Industrie 4.0 vorgeschlagen (vgl. Abbildung 8).

4.3 Risikoanalyse in der Produktion

Im Rahmen einer Risikoanalyse ist die Frage zu beantworten, wie groß der mögliche Schaden innerhalb eines Unternehmens wäre, wenn die Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität) kritischer Assets in der Produktion beeinträchtigt werden. Bei einem solchen

Abbildung 8: Klassifizierung von Daten anhand der Sensibilität

1 Öffentlich

- Keine Geheimhaltung erforderlich, keine Schutzmaßnahmen
- Informationen und Dienste sind nicht schützenswert beziehungsweise gewollt öffentlich verfügbar
- Z. B. Maschinen-Bewegungsdaten oder Sensordaten, wenn diese unkritisch bei einer Veröffentlichung sind

2 Vertraulich Geschäftspartner (neuartig bei Industrie 4.0-Szenarien)

- Mittlere Schutzwürdigkeit
- Unternehmensübergreifender Informationsaustausch für Industrie 4.0 zwingend erforderlich
- Sachgemäßer Umgang mit Geschäftsinformationen und Dokumentation der korrekten Behandlung ist grundlegend
- Gilt z. B. für den automatischen Austausch von Produktionsinformationen

3 Vertraulich intern

- Höchste Schutzwürdigkeit
- Daten oder Dienste dürfen Unternehmensgrenzen nicht überschreiten
- Z. B. vertrauliche Produktdaten, Technologiedaten oder noch nicht veröffentlichte Patente

Quelle: nach BMWi (Hrsg.) (2016a), S. 15 f

Sicherheitsvorfall könnten zum Beispiel bestimmte Typen von Daten gestohlen, manipuliert oder Produktionsprozesse verändert werden.

Für ein nachhaltiges Risiko-Management und ein darauf aufbauendes Schutzkonzept gelten die drei folgenden Grundsätze, die die Bedeutung und Aufgaben des Asset-Managements nochmals verdeutlichen:

- Es können nur Dinge geschützt werden, deren Existenz bekannt ist!
- Nur, wenn die Schwachstellen und relevante Bedrohungen bekannt sind, können nachhaltige Schutzmaßnahmen ergriffen werden!
- Nur wenn Assets, Schwachstellen und Lokation/Besitzer bekannt sind, kann eine richtige Reaktion auf Angriffe und Ausfälle erfolgen!

Auf Basis der erfassten und klassifizierten IT-Komponenten und Datenflüsse ist eine individuelle Risikoanalyse zwingend notwendig. Durch die Ergebnisse der Risikoanalyse können sinnvolle Maßnahmen abgeleitet werden, um die identifizierten Gefährdungen angemessen zu entschärfen.

Der Prozess der Risikoanalyse ist regelmäßig zu durchlaufen, damit sich verändernde Bedrohungslagen erfasst und entsprechende Maßnahmen eingeleitet werden. Die Studie des BMWi zur IT-Sicherheit in der Industrie 4.0 schreibt hierzu: „Die besonderen Eigenschaften industrieller Anlagen erfordern [...] ein Vorgehen, das über eine reine Bedrohungs- und Risikoanalyse hinausgeht und eher als stetig aktualisierte IT-Sicherheitsdokumentation bezeichnet werden kann. Der Hauptgrund hierfür ist der Lebenszyklus industrieller Anlagen, der sich über mehrere Jahrzehnte erstrecken kann." Ein geeignetes Vorgehen zur Risikoanalyse beschreibt u. a. der BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz. Vor einer Risikobewertung sollten interne Verantwortlichkeiten und Kompetenzen bereits geschaffen worden sein.

Ein einheitliches Bild zur Analyse von Risiken und Sicherheitsanforderungen verschiedener Industrie 4.0-Anwendungsfälle soll u. a. im Rahmen des nationalen Referenzprojektes „IUNO – IT-Sicherheit in der Industrie 4.0"[8] erarbeitet werden.

4.3.1 Schwachstellenanalyse

Sobald die wichtigen Assets identifiziert wurden, müssen die jeweils vorhandenen Schwachstellen dieser Assets bestimmt werden. Bei dieser grundlegenden Identifikation und Bewertung der Schwachstellen kann und soll der Lieferant mit einbezogen werden. So sind ein Kontextdiagramm über die Netzwerkkommunikation und die verwendeten Protokolle sowie eine Darstellung der genutzten Softwarekomponenten die Basis für die Schwachstellenanalyse. Aus der IT steht eine Reihe von Hilfsmitteln bereit, mit denen die Bewertung etwaiger Schwachstellen vereinfacht wird. [9]

Neben diesen Bewertungssystemen muss jeder Betreiber für sich bewerten, wie kritisch eine Schwachstelle in eben seinem eigenen Umfeld wirkt.[10]

Letztlich muss der Betreiber auch solche Schwachstellen betrachten, die eventuell nur ihm bekannt sind – etwa zusätzliche Remote-Zugänge oder versteckte Berechtigungen in Systemen, die nur unter bestimmten Voraussetzungen aktiv werden. Auch müssen die Besonderheiten der Betriebssituation berücksichtigt werden. Werden vermehrt Fremdarbeiter und Leihkräfte eingesetzt, sind die üblichen Sicherungsmaßnahmen nicht immer wirksam und auch ablesbare Betriebsparameter an kritischen Anlagen werden zur Schwachstelle.

4.3.2 Bedrohungsanalyse

Je nach Art des Assets muss bewertet werden, welche Angriffsvektoren auf welche Schutzziele einwirken können, die die Funktion oder den Wert des Assets beeinträchtigen können. Das kann zum einen der Verlust der Vertraulichkeit eines geheimen Produktionsverfahrens sein oder die Veränderungen der Integrität der Steuerungs- oder Prüfwerte in einem kontinuierlichen Prozess. Wichtig ist, das Asset möglichst dicht in seinem Kontext zu betrachten. Eine vollkommen autark arbeitende Fertigungsinsel (etwa eine einzelne Presse) ohne Vernetzung kann natürlich nicht über das Netzwerk angegriffen werden – die entsprechenden Bedrohungen sind nicht relevant!

8 Vgl. http://www.iuno-projekt.de/

9 Das Common Vulnerability Scoring System (CVSS) und das Common Configuration Scoring System (CCSS) ermöglichen die Vergleichbarkeit von Schwachstellen aus dem Bereich der Softwareentwicklung (Buffer Overflows oder Privilege Escalation) während der Konfiguration (etwa Nutzung veralteter Algorithmen bei SSL/TLS).

10 Hierfür wird der sogenannte Environmental Factor (EF) als Multiplikator für Schwachstellen herangezogen. Dieser leitet sich aus der Exposition des Systems gegenüber möglichen Angriffsvektoren ab.

4.3.3 Risikobewertung

In der Praxis erfolgt eine Risikobewertung häufig durch die Abschätzung von internen und externen Experten. Auf Basis der identifizierten schützenswerten Güter, der Datenanalyse und der Schwachstellen und Bedrohungen werden Risiken gemeinsam abgeleitet. Die abgeleiteten Risiken werden dann hinsichtlich ihrer Eintrittswahrscheinlichkeit und des Schadensausmaßes bewertet. Bewertungsskalen können individuell festgelegt werden, wobei häufig fünfstufige oder dreistufige Skalen zur Anwendung kommen. Eine mögliche dreistufige Kategorisierung des Schadensausmaßes kann zum Beispiel wie folgt aussehen:

- Hoch: große, nur schwer zu kompensierende Auswirkungen auf die Organisation bis hin zum Existenzverlust
- Mittel: spürbare Auswirkungen auf die Organisation
- Gering: geringe Auswirkungen auf die Organisation, die problemlos absorbiert werden können

Aus der Kombination von Eintrittswahrscheinlichkeit und Schadensausmaß ergibt sich ein Risikolevel für jedes einzelne Risiko. Dies kann man dann gemeinsam mit den möglichen Schutzmaßnahmen tabellarisch aufarbeiten, wie in Abbildung 9 als Beispiel gezeigt. Solche Tabellen eignen sich auch als einfaches Werkzeug zur Nachverfolgung von Risiken über die Zeit, wenn diese Risiken als nummerierte Elemente mit einem Zuständigen (Risiko-Eigner) und einem Datum für die Umsetzung der Maßnahme versehen werden.

Dieses erlaubt es nun, solche Risiken zu ermitteln, die jenseits des vom Management zu definierenden Risikoappetits liegen und mittels Einsatz von Gegenmaßnahmen auf ein akzeptables Niveau zu reduzieren sind. Hierbei sollte man sich auf solche Maßnahmen konzentrieren, die insbesondere den Schutz der kritischen Assets stärken. Es darf jedoch nicht außer Acht gelassen werden, dass eine starke Verteidigung in eine Richtung nichts nützt, wenn an anderer Stelle Angriffe mühelos Erfolg haben können.

4.3.4 Schutzmaßnahmen definieren

Eine Ausgewogenheit der Maßnahmen kann nur aus der Sicht auf das Gesamtrisiko und die Einzelrisiken erreicht werden. Die Priorisierung der Maßnahmen muss sowohl das einzelne Schutzziel als auch die Gesamtheit der Schutzziele eines Assets berücksichtigen, da teilweise Maßnahmen für das eine Schutzziel negative Auswirkungen für andere Schutzziele haben können. So wird beispielsweise durch die Erstellung und externe Speicherung eines Backups der kritischen Produktionsparameter gleichzeitig deren Bekanntwerden riskiert, da sich die Parameter nicht mehr in der relativen Sicherheit der abgeschotteten Anlage befinden. Wird die Anlage jedoch durch einen Unfall zerstört, werden diese Parameter dringend für eine schnelle Wiederherstellung der Produktionsfähigkeit benötigt. Vor dem Hintergrund solcher Abhängigkeiten sollten Maßnahmen immer erst nach einer ganzheitlichen Risikoanalyse geplant und abgewogen werden.

4.4 Notfallmanagement und Wiederherstellung

Im Sinne einer Forderung nach größerer Resilienz der Produktion – also einer Widerstandsfähigkeit gegen Angriffe und einem eher elastischen Verhalten im Schadenfall – kommt der Betrachtung von Notfallmanagement, Wiederherstellungsprozessen und sinnvoller Nutzung von Backup-Technologien eine größere Bedeutung im Risiko-Management zu.

Der materielle Totalverlust einer Anlage kann durchaus durch entsprechende Versicherungen kompensiert werden – leider ist der Verlust des in der Anlage „konfigurierten Know-hows“ weitaus schwieriger zu kompensieren. Hier muss im Sinne eines Notfallmanagements dafür gesorgt werden, dass beispielsweise Konfigurationsdaten, Betriebsparameter und Einstellungen der Werkzeuge ordentlich dokumentiert sind und diese Dokumentation auch zur Wiederherstellung der Produktionsfähigkeit an einem anderen Standort genutzt werden kann. Da im Normalfall kein Unternehmen ein „Ausfallproduktions-Zentrum“ betreibt, ist stets die Frage

Abbildung 9: Beispiel einer einfachen Asset/Risiko-Tabelle

Asset	Mögliche Bedrohung	Eintritts-wahrscheinlichkeit	Erwartetes Schadensausmaß	Risikolevel	Mögliche Schutzmaßnahme
Leitrechner (HMI)	Infektion mit Malware	Mittel (tritt mehrmals im Jahr auf)	Mittel (Produktion bis zu 4 Stunden beeinträchtigt)	Mittel	USB deaktivieren AV[11] installieren System einfrieren

Quelle: Plattform Industrie 4.0

11 Anti-Viren-Software

nach einer Rückführbarkeit der gesicherten Daten in eine neue Anlage offen. Hier kann nur unter erheblichem Aufwand eine simulierte Umgebung beziehungsweise eine gestaffelte Rückspiegelung der gesicherten Konfiguration in einzelnen Segmenten der Anlage getestet werden (etwa in Wartungsfenstern).

Solange keine ausreichenden technischen und finanziellen Spielräume für Simulation, Test und Wiederherstellung in solchen Ausfallszenarien vorhanden sind, sollte dennoch nicht auf ein Backup bzw. eine Aufzeichnung der Daten verzichtet werden. Da diese Daten gleichsam das Know-how der Firma spiegeln, sollten entsprechende Datenträger nur unter höchsten physischen Sicherheitsvorkehrungen erstellt und transportiert werden. Die Verschlüsselung solcher Aufzeichnungen ist zwar aus Sicht der Vertraulichkeit sinnvoll, die Praxis zeigt jedoch, dass der Wiederherstellungsprozess ohnehin komplex genug ist und eine Verschlüsselung diesen weiter kompliziert. Maßnahmen wie der Transport in speziell gesicherten Boxen und Aufbewahrung in Schließfächern können hier kompensierend wirken.

5 Segmentierung von Geräten, Anlagen und Netzen

Um trotz der ansteigenden Vernetzung der Produktion ein angemessenes Sicherheitsniveau zu erreichen, müssen Zonen ähnlichen Schutzbedarfes identifiziert und mit technischen Mitteln voneinander separiert werden. Dies muss so geschehen, dass die Trennung der einzelnen Systembereiche keine wesentliche Einschränkung der Produktionsprozesse bewirkt. Kommunikation zwischen den Zonen kann weiterhin stattfinden, sofern die Übergänge klar definiert und entsprechend abgesichert sind. Eine sorgfältige Zonierung mit zugehöriger Identifikation und Absicherung der Informationsflüsse kann so ein hohes Sicherheitsniveau auch in der hochvernetzten Systemlandschaft der Industrie 4.0 gewährleisten.

5.1 Trennung von Office und Produktion

Insbesondere der fließende Übergang zwischen Office-IT und den unteren Ebenen der Produktion (wie Betriebsleitebene, Prozessleitebene, Steuerungsebene, Feldebene und Prozessebene) stellt oftmals einen direkten Einstiegspunkt für Angreifer dar. So kann ein kompromittiertes System auf Betriebsebene ohne ausreichende Segmentierung großen Schaden in den vernetzten Produktionssystemen anrichten. Umgekehrt sind Angriffe von einer kompromittierten Komponente der Produktion auf sensible Daten und Prozesse im ERP-System einer ungeschützten Anlage realistisch. Es müssen also zumindest Office-IT und die nachgelagerten Produktionssysteme in ausreichendem Maße voneinander getrennt werden. In einem ersten Schritt muss hierzu zunächst geklärt werden, was der eigentlichen Office-IT zuzurechnen ist. Einer solchen Zonendefinition sollte idealerweise die Identifikation des risikobasierten Schutzbedarfs zugrunde liegen: Den in der Risikoanalyse identifizierten schutzbedürftigen Werten und zugeordneten Schutzzielen wird über eine Bedrohungsanalyse der entsprechende Schutzbedarf zugeordnet. Komponenten mit ähnlichem Schutzbedarf werden dann in einer Zone zusammengefasst. Da eine vom Aufwand her angemessene Risikoanalyse jedoch oftmals von kleinen und mittleren Unternehmen nicht geleistet werden kann, ist auch eine direkte Zonierung, aufgrund einer groben Bedrohungsabschätzung möglich. Beispielsweise können alle Rechner der Office-IT, die Zugriff auf das interne E-Mail-System haben und somit einer besonderen Gefährdung ausgesetzt sind, in einer Zone zusammengefasst werden. Es ergeben sich so Netzsegmente mit Komponenten vergleichbaren Schutzbedarfs, sowohl in der Office-IT als auch in den Produktionssystemen. In einem zweiten Schritt können dann die Zonen der Betriebsebene mit technischen Mitteln von den Zonen der Produktionsebene getrennt werden.

5.2 Trennung von Anlagen-Subnetzen

Während die Segmentierung in Office-IT und Produktion eine vertikale Trennung beschreibt, so lassen sich in gleichem Sinne auch Anlagen-Subnetze horizontal trennen. Dies ist notwendig, um nach einem erfolgreichen Angriff auf Teilsysteme der Produktion einer weiteren Kompromittierung vor- oder nachgelagerter Anlagen und Systeme entgegenzuwirken. Die Notwendigkeit der horizontalen Trennung wird unmittelbar ersichtlich, wenn man die Produktionsanlage im Kontext der Industrie 4.0 betrachtet. So erstreckt sich die eigentliche Produktion über eine Vielzahl von Anlagen und Anlagenverbünden, deren Komponenten

nicht nur Daten, sondern ggf. ganze Funktionen transferieren. Eine einzelne kompromittierte Komponente in einem solchen Verbund kann signifikante Auswirkungen auf die gesamte Produktion haben, insbesondere wenn der Angreifer ungehindert Zugriff auf benachbarte Systeme erlangt und sich so sukzessiv im Anlagenverbund ausbreiten kann. Um solchen Szenarien entgegenzuwirken, müssen die Anlagen-Subnetze in Zonen eingeteilt und mit geeigneten technischen Isolationsmaßnahmen voneinander getrennt werden. Diese Trennung soll Kaskadeneffekten entgegenwirken und darf gleichzeitig die horizontale sowie vertikale Kommunikation mit benachbarten Anlagenkomponenten nicht funktionsbeeinträchtigend einschränken. Um dies zu gewährleisten, werden im nächsten Abschnitt spezielle Zonenübergänge beschrieben.

5.3 Zonenübergänge

Um die Segmentierung der identifizierten Zonen zu realisieren, sollten spezielle Übergänge zwischen diesen etabliert werden. Die gesamte Kommunikation zwischen zwei Zonen wird dann durch einen solchen Zonenübergang geleitet. Durch diese Bündelung der Kommunikationskanäle werden Filterung, Überwachung und insgesamt Absicherung der Kommunikation zwischen Zonen wesentlich erleichtert: Die konsequente Umsetzung von Zonenübergängen hat eine erhebliche Reduzierung der zu betrachtenden Komplexität zum Vorteil, da nun anstelle der Kommunikationskanäle zwischen einzelnen Komponenten lediglich die Zonenübergänge zwischen Zonen von Komponentenverbünden betrachtet werden müssen. Technisch lassen sich solche Zonenübergänge mittels entsprechend konfigurierter Router und Switches realisieren. Die Zonenübergänge selbst können flexibel mit geeigneten Isolationsmaßnahmen versehen werden. Hierzu kommen praktisch Firewalls und Datendioden zur Filterung der Kommunikation zum Einsatz. Bei Bedarf können Zonenübergänge auch mit speziellen Modulen zur Angriffserkennung ausgestattet werden (siehe hierzu Abschnitt 5.9). Für die genannten Filterfunktionen gibt es sowohl Hardware- als auch Softwarelösungen auf dem Markt, wobei Ersteren bei besonders kritischen Zonenübergängen der Vorzug zu geben ist, Letztere aber oft eine kostengünstigere Alternative darstellen. Die Vorgehensweise der Unterteilung in Zonen und Etablierung der Zonenübergänge ist ausführlich im Standard ISA/IEC 62443 beschrieben.

5.4 Funktechnologien

Das beschriebene Konzept der Zonen und Zonenübergänge sollte konsequent auch auf Funktechnologien übertragen werden. Dies bedeutet insbesondere, dass sämtliche Sender zumindest einer Zone zugeordnet werden sollen und die definierten Zonenübergänge auch über entsprechende Wireless-Gateways zu realisieren sind. Hierbei spielt besonders die sichere Konfiguration der eingesetzten Funktechnologien eine zentrale Rolle. So sollen durch Abschirmung und Anpassung der Signalstärke möglichst geringe Reichweiten erzielt werden. Auch soll die gewählte Funktechnologie eine möglichst geringe Störanfälligkeit (z. B. mittels Frequenzsprungverfahren) gewährleisten. Aufgrund der Exponiertheit des Funknetzes soll auf sämtlichen Zugangsknoten eine starke Authentisierung der Teilnehmer erfolgen, selbst eine einfache Zugangsbeschränkung wie MAC-Filterung kann hier sinnvoll sein – insbesondere, wenn noch schwache Endgeräte älterer Bauart genutzt werden, die keine stärkeren Verfahren unterstützen. Neuere Systeme unterstützen auch moderne Verfahren wie Network Admission Control (NAC)[12], was jedoch auch Investitionen in aktuelle Netzwerktechnologie und Access Points notwendig machen kann. Werden in Zonenübergängen Relay-Stationen eingesetzt, um geographisch weit entfernte Anlagen zu verbinden, müssen ungesicherte Kommunikationskanäle (ohne kryptographische Absicherung) durch sichere Protokolle getunnelt werden.

5.5 Fernzugriffe

Auch Fernzugriffsverbindungen, beispielsweise für Fernwartungen durch den Integrator, können auf die definierten Zonen und deren Übergänge abgebildet werden. So sollen Fernzugriffe immer durch mindestens einen dafür vorgesehenen Zonenübergang geschehen, wobei dieser durch Einsatz redundanter Gateways vor Ausfällen abgesichert sein sollte. Bei größeren Anlagen sind auch mehrere Zonenübergänge mit eigenständiger Hardware denkbar. Beispielsweise könnten sämtliche M2M-Verbindungen aus entfernten Anlagen über einen separaten Übergang geroutet werden.

Zu Beginn jeder Sitzung muss eine starke Authentisierung der Kommunikationspartner stattfinden. Unabhängig von einer weiteren möglichen Authentisierung auf der Zielmaschine sollte dies bereits im Gateway des Zonenübergangs geschehen. Sämtliche externe Kommunikation über unsi-

12 Hierbei wird das Protokoll 802.1x genutzt, das eine Authentisierung der Clients auf Ebene der Schicht 2 – also vor der Nutzung von IP – ermöglicht.

chere Netze muss kryptographisch abgesichert werden. Dabei sollen zumindest Integrität und Authentizität der übermittelten Daten gesichert sein, zusätzlich sollten Daten ohne spezielle Echtzeit-Anforderungen nach Möglichkeit verschlüsselt werden. Hierfür empfiehlt sich unter anderem der Einsatz von kryptographisch abgesicherten hochwertigen VPN-Lösungen. Dies hat den praktischen Vorteil, dass kommerziell verfügbare VPN-Gateways oftmals bereits mit einer Firewall ausgestattet sind. Zur Filterung der eingehenden Anfragen ist eine Firewall unabdingbar. Als weitere Option bietet sich die Kapselung in OPC UA an, wie sie in Abschnitt 5.6 beschrieben wird. Selbst die schon weitgehend mögliche Umstellung der Konfigurations- und Virtualisierungs-Zugänge auf https bietet eine grundlegende Sicherheit, auf die nicht verzichtet werden sollte. Im Sinne der Verbreitung von M2M-Kommunikation sollten auch abgesicherte REST-APIs als Alternative betrachtet werden.

Für jeden Zonenübergang (für Fernzugriffe) sollten spezielle Regelungen zum Aufbau, Ablauf und Beenden einer Sitzung definiert sein. Zu den Sitzungsregeln zählen beispielsweise Anforderungen an Dauer und Funktionsumfang der Sitzung, erlaubte Wartungsintervalle und IP-Adressbereiche sowie Umfang der aufgezeichneten Sitzungsdaten. Bei Verstoß gegen diese vordefinierten Sitzungsregeln muss die Verbindung automatisch abgebrochen werden. Die Regelungen für Fernzugriffe können dabei flexibel an die definierten Rollen angepasst werden. Zum Beispiel sind für Wartung, Nutzung, Update, Backup, M2M-Kommunikation maßgeschneiderte Sitzungsregeln sinnvoll.

Oft sind Maschinen und Dienste nicht direkt erreichbar, sondern können nur über mehrere Zonenübergänge erreicht werden. In diesem Fall ist es notwendig, die Sitzungsregeln für jeden genutzten Übergang zu erfüllen. Verbindet sich beispielsweise eine Maschine über drei Zonenübergänge zu einer Maschine einer entfernten Anlage, so kann es durchaus sein, dass sich die Maschine dreimal authentisieren muss. Auch gelten dann für diese Verbindung sämtliche Sitzungsregeln der drei genutzten Zonenübergänge.

5.6 Interne und externe Vernetzung der Produktionsanlagen

Wie eingangs erwähnt zeichnen sich Industrie 4.0-Anlagen durch einen hohen Grad an Vernetzung aus. Dabei ist nicht nur ein hohes Maß an anlangeninterner Vernetzung zwischen den einzelnen Maschinen sowie zwischen den Automatisierungsebenen zu beobachten. Auch die Maschinen und Planungssysteme weit entfernter Anlagen sind zu Anlagenverbünden zusammengefasst. Auch hier sollte das oberste Ziel die Trennung der Kommunikation und Netze sein, wozu sich wieder der Zonenbegriff eignet. So empfiehlt es sich beispielsweise, die Kommunikation auf Betriebsebene und die M2M-Kommunikation der Feldgeräte über verschiedene Zonenübergänge zu leiten. Wie in Abschnitt 5 erwähnt, sind hier für jeden vorgesehenen Zonenübergang durchaus verschiedene Gateways denkbar. Dies erleichtert die Auswahl der Schutzmechanismen und bildet die logische Trennung der miteinander kommunizierenden Zonen auch hardwareseitig ab. Sind zwei Zonen (auch entfernter Anlagen) langfristig miteinander verbunden, empfiehlt sich die Einrichtung eines Site-to-Site-VPN-Tunnels. Sämtliche Kommunikation der beiden Zonen wird hierbei direkt durch die zugeordneten VPN-Gateways geleitet. Dies lässt sich leicht mittels IPsec oder SSL VPN realisieren. Für kurzzeitige Verbindungen ist die Einrichtung eines VPN nicht sinnvoll. Hier sollten die Kommunikationspartner den beschriebenen Weg über die vordefinierten Zonenübergänge gehen. Beispielsweise würde man für eine Maschine, die monatlich eine einzelne Anfrage an eine externe Datenbank stellt, keinen Site-to-Site-Tunnel errichten. Die Grenzen hier sind jedoch fließend und es sind Zonen denkbar, die sich über mehrere verteilte Anlagen erstrecken. Um hier den Überblick zu bewahren, benötigt der Anlagenbetreiber ein klares Bild der Zonenarchitektur.

Maschinen innerhalb einer Zone kommunizieren meist über geeignete Feldbusse. Diese verfügen oft über keinerlei Absicherung und können weder Authentizität, Integrität oder gar Vertraulichkeit der Kommunikation gewährleisten. Aufgrund der teils hohen Echtzeitanforderungen ist zumindest eine Verschlüsselung auf Feldbusebene nicht immer sinnvoll. Im Industrie 4.0-Kontext sollten jedoch immer zumindest Authentizität und Integrität gewährleistet sein. Für M2M-Kommunikation zwischen entfernten Anlagen lassen sich Feldbusse durch sichere Kanäle tunneln. Als Beispiel sei hier die Kapselung von Modbus in OPC UA genannt, um entfernte Zonen auf Feldebene miteinander zu verbinden. Über solche Tunnel wird auch die direkte vertikale Integration der Fertigung in die Produktionsplanung und Bestellabwicklung moderner ERP-Systeme realisiert.

5.7 Kryptographie

Viele der bereits genannten Schutzmechanismen beruhen auf Kryptographie. Um die sichere Kommunikation, starke Authentisierung oder Datenvertraulichkeit sowie Datenintegrität zu gewährleisten, werden mathematische Verfahren genutzt, die nach gegenwärtigem Stand der Technik einen ausreichenden Schutz bieten. Dabei sollten ausschließlich bereits erforschte und standardisierte Verfahren zum Einsatz kommen. Auch wenn Eigenentwicklungen in Einzelfällen der direktere und einfachere Weg zu sein scheinen, so ist doch dringend von solchen abzuraten: Meistens werden diese innerhalb kurzer Zeit gebrochen. Daher sprechen öffentliche Stellen Empfehlungen zu sicheren Verfahren und zugehörigen Parametern aus, die nicht nur öffentlich

zugänglich, sondern auch stets der aktuellen Bedrohungslage angepasst sind. Besonders die Empfehlungen des BSI[13, 14], des NIST[15] sowie der Bundesnetzagentur[16] bieten einen guten und aktuellen Überblick über sichere Kryptographie.

In der Praxis ist eine Diskrepanz zwischen den öffentlichen Empfehlungen und den auf dem Markt verfügbaren Komponenten zu erkennen. Im Idealfall können sämtliche kryptographischen Parameter vom Betreiber nach Kauf eingestellt und die Komponenten sicher konfiguriert werden. Beim Einkauf von Anlagenkomponenten sollte der Betreiber darauf achten, dass die Komponente den Austausch und somit die Aktualisierung der verwendeten kryptographischen Verfahren unterstützt. Nur so kann die Anlage auch bei langer Einsatzdauer der hochdynamischen Bedrohungslage entsprechen.

5.8 Public-Key-Infrastrukturen (PKI) beim Betreiber

Idealerweise verfügt der Anlagenbetreiber bereits über eine Public-Key-Infrastruktur (PKI) für die Office-IT, mit der er auch Zertifikate für seine Anlagen und Module sowie für die Netzwerkgeräte erstellen kann. In diesem Falle ist es wichtig, dass sich neue Anlagenkomponenten in die bereits bestehende PKI integrieren lassen. Besitzt der Betreiber noch keine eigene PKI, so sollte diese in enger Zusammenarbeit mit der Office-IT geplant, erstellt und betrieben werden, da diese Aufgaben zur klassischen IT-Sicherheit gehören. Hier ist ein Betreibermodell anzustreben, in dem die Office-IT der Produktion lediglich eine eigene Issuing CA bereitstellt, diese aber zusammen mit der restlichen Vertrauenshierarchie und den begleitenden Technologien betreibt.

Der Betreiber sollte insbesondere darauf achten, ob die Zertifikate (z. B. X.509) von den Komponenten verarbeitet werden können und ob ausreichend Speicher für die Hinterlegung von Wurzelzertifikaten vorhanden ist. Viele Geräte aus dem Embedded-Umfeld sind zudem zu schwach ausgelegt, um die üblichen Anforderungen an Algorithmen und Schlüssellängen zu erfüllen. Hier ist in Zusammenarbeit mit der Office-IT eine angepasste Policy zu entwerfen. Auch sollte der Betreiber zur Verwaltung der Zertifikate ein Certificate Lifecycle Management (CLM) Tool verwenden – idealerweise lassen sich die Zertifikate sämtlicher Anlagenkomponenten hiermit verwalten und auch im laufenden Betrieb aktualisieren. Häufig unterliegt die Anlage einer hohen Komponentenfluktuation: Nicht nur werden die Komponenten innerhalb der Anlage häufig ausgetauscht, auch können temporäre Komponentenverbünde mit anderen Anlagen entstehen. Werden dann massenhaft Zertifikate ungültig erklärt, müssen diese auch entsprechend kenntlich gemacht werden. Das Standardverfahren hierfür bilden die eher statischen Certificate Revocation Lists (CRLs) für die Bekanntmachung der ungültigen Zertifikate. Vorfälle der jüngsten Vergangenheit zeigen jedoch, dass diese Technik an ihre Grenzen stößt.[17] Um der höheren Dynamik Rechnung zu tragen, empfiehlt sich der Einsatz des Online Certificate Status Protocol (OCSP): Hier wird die Validierung von Zertifikaten von den Komponenten auf einen Validierungsdienst ausgelagert, statt im Problemfall sehr lange CRLs zu erzeugen, die eventuell schon überholt sind. Auch bei OCSP ist es in jüngster Zeit zu Sicherheitsproblemen gekommen, die derzeit noch nicht abschließend gelöst sind. In Ermangelung von Alternativen bleibt dem Anwender derzeit jedoch keine andere Wahl als OCSP.

5.9 Kontrolle der Netzkommunikation

Standen im bisherigen Kapitel Methoden und Herangehensweisen zur Trennung der Kommunikationsnetze im Vordergrund, so werden in diesem Abschnitt Aspekte der Steuerung und Pflege von Netzkommunikation erläutert.

5.9.1 Monitoring

Wie bereits in Abschnitt 5.2 angedeutet, sind Zonenübergänge geeignete Stellen in der Netzinfrastruktur, um die Anlagenkommunikation aufzuzeichnen und auf Auffälligkeiten zu untersuchen. Kommerziell verfügbare Monitoring-Systeme bieten bislang nur Erkennung möglicher Schadsoftware auf Basis von Signaturen oder verhaltensbasierter Erkennung von Protokollanomalien. Derzeit sind diese Verfahren jedoch nur unter gewissem Aufwand für die Produktion umsetzbar, da entsprechende Konfigurationen und Lernphasen hohes Know-how erfordern und oft Kenntnisse der lokalen Umgebung voraussetzen.

Dabei wird unter Anomalie ein vom Normalbetrieb abweichendes Verhalten verstanden, welches insbesondere auf der Feldebene mit relativ gleichförmigen Kommunikationsmustern gut erkannt werden kann. Solche Lösungen bieten zwar keinen vollständigen Schutz gegen Angriffe über das Netzwerk, decken diese aber oft in hinreichendem Maße

13 Vgl. BSI (Hrsg.) (2012)

14 Vgl. BSI (Hrsg.) (2015)

15 Vgl. NIST (Hrsg.) (2014)

16 Vgl. Bundesnetzagentur (2015)

17 Siehe hierzu die stark gestiegene Netzwerklast nach Bekanntwerden der Heartbleed-Schwachstelle in der OpenSSL Library und der massenhaften Revokation von Zertifikaten.

auf. Aufgrund der hohen Dynamik der Angriffsmuster müssen die eingesetzten Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) immer auf aktuellem Stand gehalten werden: Nur mit neuesten Signaturen können schadhafte Anomalien zuverlässig erkannt werden. Die aufgezeichneten Daten sollten hierbei zentral gespeichert und zum Zwecke einer möglichen forensischen Untersuchung zumindest temporär aufbewahrt werden. Der Umfang der erfassten Daten sollte hier den Sicherheitsanforderungen des Zonenübergangs angepasst werden: Von der Aufzeichnung und Analyse einzelner Messdaten auf Feldebene bis hin zu vollständiger Erfassung der Identitäten aller Kommunikationspartner, Zeitpunkt und Dauer der Kommunikation sowie gesprochenen Protokollen aller Sitzungen lassen sich geeignete Monitoring-Systeme flexibel anpassen. Sensible Daten sollten jedoch von der Aufzeichnung ausgenommen werden.

Zusätzlich zur Datenerfassung auf den Zonenübergängen können Monitoring-Systeme auch direkt im Leitstand integriert werden. Dies kann je nach Netzinfrastruktur den Vorteil haben, dass auf sicherheitsrelevante Ereignisse direkter und von zentraler Stelle aus reagiert werden kann. Dabei sollten Betreiber und Integrator sorgfältig abwägen, ob die Netzinfrastruktur der Kommunikationslast bei möglicherweise sehr hohem Datendurchsatz zum zentralen Leitstand gewachsen ist. Ein Kommunikationslagebild mit Anomalie-Erkennung als zusätzlicher Informationsquelle ist hier in Zukunft unbedingt erforderlich. Zur zentralen Erfassung und sicheren Speicherung von Log-Daten sollte zunächst ein zentralisiertes Log-Management etabliert werden. Dies verhindert die nachträgliche Manipulation von Logs durch privilegierte User und ermöglicht Analysen nach Sicherheitsvorfällen von zentraler Stelle aus. Ein bisher nur im Konzern-Umfeld zur Anwendung kommendes Werkzeug für die weitergehende Harmonisierung der Logs, deren Analyse und für die Korrelation von Daten aus verschiedenen Sicherheitskomponenten stellen die Security Information and Event Management (SIEM)-Lösungen dar. Mit diesen hat der Betreiber den Zustand sämtlicher sicherheitsrelevanter Komponenten im Blick und kann auf erkannte Störfälle in Echtzeit und zentral gesteuert reagieren. Die Kompatibilität der verwendeten Sicherheitskomponenten ist Voraussetzung für eine gut funktionierende Integration in das SIEM-System. Doch auch unter strenger Beachtung von Standards und der Auswahl geeigneter Quellsysteme stellen SIEM-Lösungen die Krönung der IT-Sicherheitsmaßnahmen dar, da ihre Implementierung oft einige Mannjahre Aufwand verzehrt und sie im Betrieb stets an die Änderungen der Quellsysteme angepasst werden müssen. Daraus resultiert, dass die Nutzung von SIEM primär im Sinne eines „Managed Service“ erfolgen sollte, da der Mittelstand weder die notwendigen Ressourcen noch das erforderliche Betriebspersonal oder geschulte Incident Manager vorhalten kann.

5.9.2 Isolation von Störfällen

Erkennt der Betreiber einen erfolgten Angriff oder Befall mit Schadsoftware frühzeitig, müssen die betroffenen Netzsegmente von der Netzinfrastruktur isoliert werden, um so eine weitere Ausbreitung zu verhindern. Auch hier kommt dem Betreiber die beschriebene Zonierung der Netzinfrastruktur sehr zugute: Ist ein Subnetz von einer Störung befallen, die auf angegliederte Netzbereiche überzugreifen droht, genügt es, die entsprechenden Zonenübergänge zu kappen und so den Störfall vom Gesamtsystem zu isolieren. Dies lässt sich durch kurzfristiges Einbringen von wenigen Filterregeln in die jeweiligen Firewalls schnell und einfach realisieren. Ist der Störfall isoliert, lässt sich der betroffene Netzbereich wieder in einen vertrauenswürdigen Zustand bringen. Der bei Betreibern von Rechenzentren und Cloud-Servern bereits etablierte Einsatz von Software-defined Networking (SDN)-Technologien kann zukünftig auch für die Produktionsnetze in Betracht gezogen werden. SDN erlaubt die zentrale Steuerung und automatisierte Konfiguration der Netztopologie.

6 Sicheres Identitäts-Management

Bereits im Ergebnispapier „Sichere Identitäten“ hat die Plattform Industrie 4.0 herausgearbeitet:

> ***„Sichere Identitäten sind der Ausgangspunkt für die Sicherheitskette, welche die Datenerhebung, den -transport und die -verarbeitung auf Hardware-, Software- und Prozessebene absichert. Sie fungieren als Voraussetzung für viele weitere Schutzmaßnahmen. Wenn es einem Angreifer gelingt, unberechtigt eine Identität anzunehmen, laufen alle darauf aufbauenden Maßnahmen wie z. B. der Zugriffsschutz ins Leere. Hauptziel von sicheren Identitäten ist der Start der Vertrauenskette in der automatisierten Kommunikation.“***

Sowohl für die Sicherstellung der Authentizität, die Wahrung der Integrität und vor allem für die Nachvollziehbarkeit ist die Nutzung eindeutiger sicherer Identitäten unabdingbar.[18] Das Arbeiten auf Basis sicherer Identitäten ist in den Systemen der Office-IT bereits zum Standard geworden. Für Industrie 4.0 spielt die Beziehung zwischen Mensch und Maschine (beziehungsweise deren Identitäten) eine wichtige Rolle. Dies wird durch die Identitäten für Anlagen, Maschinen und Werkstücke in der Maschine-zu-Maschine-Kommunikation (M2M) in Zukunft an Bedeutung übertroffen. Die nachfolgenden Abschnitte geben einen Einblick, welche Funktionen des etablierten Identitäts- und Berechtigungs-Managements auch für die Produktion nutzbar sind, und wo neue Prozesse und Funktionen geschaffen werden müssen.

Eine der vornehmsten Aufgaben bei der sicheren Ausgestaltung von Produktionssystemen ist die Sicherstellung der Authentizität des jeweiligen Bedieners. Seit jeher wird hierauf im Bereich der Pharmazie, der Lebensmittel und der Chemischen Industrie genauestens geachtet – denn Organisationen wie die Food and Drug Administration (FDA) in den USA und die europäischen Verordnung REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals) aus dem Jahre 2007 haben in diesen Branchen zu einer erheblichen Regulierung geführt, die wiederum eine Nachvollziehbarkeit der Frage „Wer hat wann wie mit welcher Charge der Substanz an welchem Produktionsschritt mitgearbeitet?“ impliziert. Folglich ist die persönliche Anmeldung eines Werkers an einer Anlage der chemischen Industrie durchaus üblich, während ähnliche Ansätze bisher in der Stückgutindustrie – vornehmlich durch Intervention des Betriebsrates aufgrund der vermuteten Arbeitnehmerüberwachung oder durch technische Probleme – nicht umgesetzt wurden.

Fakt ist, dass eine Nachvollziehbarkeit von Handlungen und eine persönliche Zuordenbarkeit nur durch die Nutzung persönlicher Nutzerkonten an den Anlagen und Maschinen sowie den Bedien-Rechnern erreicht werden kann. Dies erfordert wiederum die Verwaltung einer weitaus größeren Zahl an Konten (die bisher eher nur zwischen „Einrichter/Instandhalter“ und „Bediener“ unterschieden haben). Diese Personalisierung der Benutzerkonten führt wiederrum zum Bedarf, diese auch auf einer Vielzahl von Anlagen und Maschinen parallel und effizient zu verwalten – oder zumindest eine persönliche Zuordenbarkeit auf Ebene der Fachanwendung zu ermöglichen, wenn der Zugang zu den Betriebssystemen aus technischen Gründen nicht personalisiert werden kann oder soll.

18 Vgl. BMWi (Hrsg.) (2016b), S. 11

6.1 Benutzerkonten in Betriebssystem und Applikation

Zunächst muss unterschieden werden zwischen einer Anmeldung (Identifikation) des Benutzers am Betriebssystem und der Anwendung. Bislang war es üblich, dass Anlagen und Maschinen nur im Kontext eines lokal im Betriebssystem angelegten Benutzers ausführbar waren. Der folgende Abschnitt beschreibt, dass in Zukunft nur noch zentral in einem Verzeichnis verwaltete Benutzerkonten (gemeinhin als „AD[19]-Konten“ bezeichnet) für die Anmeldung am Betriebssystem zum Einsatz kommen sollten. Es muss angemerkt werden, dass viele derzeit eingesetzte Softwareprogramme die Nutzung solcher Konten nicht erlauben, da ein lokales Systemkonto zur Ausführung erwartet wird. Eine weitere Problemstellung bei der Benutzung solcher Konten ist, dass zur Sicherstellung der Benutzbarkeit auch eine Betreuung des Verzeichnisdienstes in einem 24/7-Betrieb notwendig sein kann. Dies ist erforderlich, um eventuell „ausgesperrte“ Benutzer wieder auf ihre Konten zugreifen lassen zu können, was zumeist die Interaktion mit dem Servicedesk erfordert. Eine Alternative hierzu ist die Nutzung sich automatisch anmeldender Systemkonten für den Start des Betriebssystems und eine komplette Fokussierung auf die Verwaltung der Benutzerkonten in den Applikationen der Produktion. Dies wiederum setzt zumeist den Einsatz von zentral gesteuerten Provisionierungs-Lösungen voraus, die eine Erstellung und Löschung von Benutzerkonten auf Basis von Regeln und Schwellwerten bzw. Grenzwerten ermöglichen.

Neben den zentral verwalten „AD-Konten“ sollten auch die Benutzerkonten für die Applikationen der Produktion[20] individuell den Mitarbeitern zuordenbar und zentral verwaltet werden. Hierfür ist eine Schnittstelle zu den zentralen Identitäts- und Berechtigungs-Management (IAM)-Systemen erforderlich.[21] Ebenfalls ist ein schreibender Zugriff auf die Benutzerkontendatenbank denkbar – dies setzt jedoch einen Einblick in die Struktur der Tabellen voraus.

6.2 Lebenszyklus von Benutzerkonten

Wie im vorigen Abschnitt beschrieben, müssen für die Benutzung einer Applikation entsprechende Benutzerkonten vorhanden sein. Diese müssen jedoch zunächst beantragt und genehmigt werden. Diese Prozesse bilden die Kern-Abläufe eines Identitäts- und Berechtigungs-Managements – und hier kann weitgehend auf die bekannten Oberflächen und etablierten Workflows des IT-Identitäts-Managements zurückgegriffen werden. Allein die Beantragung und Genehmigung sowie die anschließende Erzeugung des Benutzerkontos (grob-granular) sind jedoch nicht vollständig. Zum einen muss die technische Umsetzung der Provisionierung korrekt erfolgen – was zumeist nicht ohne die Mitwirkung des Lieferanten oder Herstellers der Software funktioniert –, zum anderen müssen dem Benutzerkonto im nächsten Schritt die notwendigen Berechtigungen und Funktionen in der Anwendung zugeordnet werden (Entitlement Management). Diese fein-granulare Abstimmung und Festlegung, „was der Benutzer in der Applikation darf“, ist oftmals eine eher komplexe Kette von Funktionen innerhalb der Anwendung und nur selten direkt über das IAM-System abbildbar. Hier muss gegebenenfalls auch weiterhin ein Sachkundiger die Berechtigungen manuell zuordnen, sobald das Konto automatisch erstellt wurde.

Die Funktion der automatisierten Erstellung allein ist nun nicht ausreichend. Insbesondere der schnellen Deaktivierung oder nachhaltigen Löschung von Konten kommt in der Zukunft eine große Bedeutung zu, denn sogenannte „Waisenkonten“ (EN: orphaned accounts) ohne eine zugeordnete Person (etwa nach Entlassung oder in Elternzeit bzw. Todesfall) stellen ein hohes Missbrauchspotenzial dar (siehe hierzu 6.7 Privilegierte Zugriffe verwalten). Folglich muss das IAM-System zentral, aber auch die Anwendung selbst die Funktion bieten, über Schnittstellen oder das User-Interface schnell und unkompliziert Benutzerkonten zu deaktivieren oder diese zu löschen.

6.3 Logs: Auditierbarkeit von Benutzerkonten und Zugriffen

Letztlich ist nicht auszuschließen, dass es zu einem gegebenen Zeitpunkt zu Unregelmäßigkeiten oder offensichtlich missbräuchlicher Nutzung von Anlagen und Applikationen kommt. Hier muss ermöglicht werden, detailliert nachverfolgen zu können, wer wann wo zugegriffen hat, und wer wann wo welche Änderungen vorgenommen hat. Dies setzt voraus, dass die Anwendung entsprechend detaillierte Logmeldungen speichert und diese auch über längere Zeiträume möglichst unveränderbar vorhält. Im Sinne einer in der IT üblichen Log-Zentralisierung wären Funktionen zur direkten, zugriffgeschützten Speicherung der Logs auf einem abgesetzten (Syslog)Server wünschenswert. Ideal wäre dabei die Beachtung bzw. die Einhaltung oder Orientierung an Standardformaten, wie sie etwa durch Syslog, LEAF oder CEF vorgegeben werden. Dies erleichtert die zentrale Auswertung und Korrelation von Meldungen und ermöglicht die Definition zentraler Schwellwerte (thresholds), wie etwa der Alarmierung der Security, falls mit einem

19 Active Directory

20 Etwa in einem Fertigungs-Informationssystem (FIS) oder Manufacturing Execution System (MES) bzw. Produktionsplanungs- und Steuerungssystem (PPS)

21 Etwa per Simple Provisioning Markup Language (SPML) oder Simple Cloud Identity Management (SCIM)

Benutzerkonto mehrfach innerhalb kurzer Zeit an diversen Geräten ein erfolgloser Zugriffsversuch unternommen wird (vornehmlich über die Nutzung von sogenannten Security Information & Event Management SIEM-Lösungen).

6.4 Identifikation, (starke) Authentisierung und Autorisierung

In der Regel wird auch in der Industrial IT weitgehend mit der Verwendung des klassischen „Benutzername/Passwort"-Schemas gearbeitet. Hierbei stellt der Anwender dem Betriebssystem oder der Anwendung zunächst seinen Benutzernamen als Mittel der Identifikation bereit. Dem System gegenüber identifiziert er sich, bzw. stellt er die Behauptung auf, der Anwender „Johann_Schmitt" zu sein (durch Bereitstellung seines Benutzernamens). Um diese Behauptung zu beweisen, sich also als „Johann_Schmitt" zu authentisieren, stellt er zusätzlich das zum Konto gehörende Passwort bereit. Ist diese Authentifizierung erfolgreich, erhält der Benutzer Zugriff auf die ihm zugeordneten bzw. die für ihn freigeschalteten Funktionen (Autorisierung). Diese rein auf Wissen basierenden Verfahren haben sich in der Vergangenheit mehrfach als unzureichend erwiesen, da Anwender etwa dazu neigen, Passworte aufzuschreiben bzw. diese sogar aktiv weiterzugeben. Um einem Missbrauch entgegenzuwirken, werden seit geraumer Zeit Mehrfaktorverfahren eingesetzt. Diese kombinieren das Wissen bzw. die Kenntnis eines Benutzernamens mit dem Besitz eines Tokens oder einer Smartcard bzw. dem Abgleich biometrischer Eigenschaften wie Fingerabdruck oder Netzhautmuster bzw. Gesichtsform und anderen Eigenschaften. In der Produktion haben diese Verfahren oft Schwierigkeiten bei der Umsetzung, da durch Schutzkleidung bzw. Verschmutzung die Leistungsfähigkeit dieser Authentifizierungstechnologien eingeschränkt sein kann. Lediglich der Einsatz von stabilen Token auf Basis aktiver oder passiver RFID/NFC-Technik hat sich weitgehend bewährt. Insbesondere für den „administrativen Zugriff" von Instandhaltern oder Einrichtern auf Maschinensteuerungen kommen solche Token (etwa „electronic key-system" eks von Euchner) zum Einsatz. Dies erstreckt sich explizit auch auf die Steuerungsgeräte, wie an spezifischen Software-Modulen der Hersteller zur Integration der Hardware erkennbar wird (etwa Siemens Device Manager).[22]

Neben diesen Verfahren steigt die Bedeutung von Zertifikaten auf Basis von x.509v3, sowohl für Benutzer als auch Maschinen bzw. Server, stetig an. Diese aus dem Bereich der Webserver im eCommerce allseits bekannte Technologie hat auch bei der Absicherung der Web-Interfaces für Anlagen und SPS Einzug gehalten. Es sei an dieser Stelle jedoch auf den ebenfalls erheblich steigenden Bedarf für ein unternehmensweites Schlüssel- und Zertifikatsmanagement (Enterprise Key and Certificate Management) hingewiesen, da es unmöglich scheint, die erhebliche Menge kryptographischen Materials in einer Industrie 4.0-Produktion manuell zu verwalten.

6.5 Maschine-zu-Maschine-Kommunikation

Insbesondere bei der Kommunikation zwischen Anlagen und Maschinen wird auf die bereits beschriebene Verwendung von Zertifikaten zurückgegriffen. Diese werden zudem oft zur Ausführung einer beidseitigen Authentifizierung eingesetzt, um das jeweilige Gegenüber eindeutig identifizieren zu können und bei Bedarf auch eine verschlüsselte Kommunikation etablieren zu können (hierbei wird über die Nutzung der vorhandenen asymmetrischen Schlüssel der Zertifikate ein symmetrischer Schlüssel für die eigentliche Datenübertragung ausgetauscht). Neben den Zertifikaten haben sich – speziell aus dem Umfeld der sicheren Kommunikation über Unternehmensgrenzen hinweg und der Nutzung von Apps – neue Protokolle etabliert[23]. Insbesondere OAuth 2.0 wird bei kleinen mobilen Anwendungen (sogenannten Apps) dazu verwendet, den Zugriff auf Ressourcen zu erlauben, ohne der bereitstellenden Ressource direkt Credentials (wie Nutzername oder Passwort) bereitstellen zu müssen. Über die Nutzung bzw. den Einsatz dieser Protokolle können auch komplexe Zugriffe auf Ressourcen Dritter abgebildet werden, wie sie im Umfeld der Industrie 4.0 üblich sein werden.

6.6 Berechtigungsmanagement

Die Verwaltung der Berechtigungen innerhalb einer Applikation bzw. die Zuordnung der Berechtigungen zu Benutzerkonten wird gemeinhin als Berechtigungsmanagement bezeichnet. Im Idealfall kombiniert man Berechtigungen zu logisch passenden Rechtebündeln, deren Nutzung üblicherweise über die Zuordnung einer Rolle oder Gruppe erfolgt – dies wird gemeinhin unter Rollenbasierter Rechteverwaltung subsumiert.[24] Die Art Zuweisung kann jedoch auch auf diskreter Basis erfolgen, indem für jede Ressource explizit festgelegt wird, welches Subjekt zugreifen darf,[25] und welche Möglichkeiten des Zugriffs erlaubt sind.[26]

22 Vgl. Siemens AG (Hrsg.) (2010)

23 Etwa die Security Assertion Markup Language (SAML 2.0) für Föderation, OAuth 2.0 für API Autorisierung und OpenIDConnect (OIDC) als Identitätsschicht

24 RBAC – Role-based Access Control

25 DAC – Discretionary Access Control

26 Zumeist wird dabei von CRUD – Create|Read|Update|Delete gesprochen, also erstellen, lesen, aktualisieren/ändern und löschen.

Hierdurch ergeben sich im schlimmsten Fall unzählige direkte Beziehungen zwischen Objekten und Subjekten, so dass eine größere Anzahl Ressourcen oder Anwender schnell zu unübersichtlichen Lösungen führen.

Aus dem militärischen Bereich stammen Verfahren, die Ressourcen in Klassen einteilen[27] (etwa Public|Internal|Confidential|Secret oder wie in Abbildung 8 „öffentlich | vertraulich Partner | vertraulich intern“) und den Personen entsprechende Freigaben[28] erteilen.[29]

Folglich hat sich ein modifizierter rollenbasierter Ansatz weitgehend etabliert: Eine Reihe der wichtigsten und üblichen Rechte wird per Rollen geordnet und zugewiesen, während eine kleinere Anzahl an Einzelrechten diskret vergeben wird.

Um ein höheres Maß an Sicherheit zu erreichen und gleichzeitig mehr Flexibilität zu gewähren, werden Verfahren verwendet, die Personen nicht zu Gruppen oder Rollen zuordnen, sondern im Rahmen der Autorisierungsprüfung eine Reihe von Attributen prüfen, die das Subjekt erfüllen muss.[30] Es kann auch der Kontext des Zugriffs mit einbezogen werden, etwa wenn ein Subjekt laut seiner Rollen oder Gruppenzugehörigkeit Zugriff erhalten sollte, dieser aber untersagt wird, falls der Zugriff zu ungewohnter Zeit von einem unbekannten Gerät erfolgt.[31] Diese kontextbasierte Authentisierung kann somit als Ergänzung zu Rollen und diskreten Rechten gesehen werden, da es den Zugriff zur Laufzeit weiteren Restriktionen oder Prüfungen unterzieht.

6.7 Privilegierte Zugriffe verwalten

Eine besondere Herausforderung für die Sicherheit stellen jeweils die hoch- und höchst-privilegierten Konten dar. Diese „administrativen Konten“ oder „superuser“ sind in der Lage, substantielle Änderungen an den Systemen durchzuführen, und sind dabei oft gleichzeitig in der Lage, ihre Tätigkeiten durch Manipulation des Systems zu verschleiern. In der Produktion sind die Konten der Einrichter, Instandhalter (Maintenance) und oft die der Dienstleister bzw. Lieferanten besonders privilegiert, da diese Personen oder Rollen jeweils Anpassungen an der Anlage ausführen müssen. Vergleich mit den „root“ accounts auf Linux oder dem Domänen-Administrator im Microsoft Active Directory sind solche erheblichen Berechtigungen potenziell gefährlich. Hinzu kommt, dass aus Gründen der Effizienz bzw. der Wartbarkeit die Kontoname-Passwort-Kombination (gemeinhin „Credentials“ genannt) an vielen Systemen der Produktion identisch gehalten wird und einer Reihe Personen bekannt ist (üblicherweise allen Einrichtern oder Instandhaltern). Dies führt zwangsläufig zu einer unsicheren Gesamtlage, da weder Nachvollziehbarkeit noch Vertraulichkeit ausreichend geschützt werden. Für Systeme mit Netzwerkanbindung und rudimentärer Protokollunterstützung (SSH – Secure Shell oder https) bietet es sich nun an, den Zugriff derartig privilegierter Konten über ein zentrales System zu führen. Diese Werkzeuge werden als Privileged Access|Identity|User Management[32] bezeichnet und bringen zum einen Funktionen für die sichere Speicherung einer Vielzahl von Credentials mit, ermöglichen zum anderen aber auch die schnelle und intensive Rotation der Passwörter. Letzteres wird durch einen Automatismus ermöglicht, der nach Beendigung einer User-Session das Passwort im System ändert, den neuen Wert in der internen Datenbank speichert und diese dem nächsten Benutzer für die Dauer seines Zugriffs freischaltet. Im Idealfall startet das System direkt diese Sessions und injiziert das Passwort, so dass die Benutzer niemals Kenntnis der Credentials erhalten.

6.8 Verzeichnisdienste für die Verwaltung von Identitäten

Bereits heute stellen die vernetzten Komponenten der Produktion eine größere Anzahl als die betrieblich genutzten IT-Komponenten in der Office-IT. Auch wenn im Unternehmen hunderte oder gar tausende Mitarbeiter über eine digitale Identität verfügen, um auf ihre IT-Systeme zugreifen zu können, so wird die Anzahl der individuell zu identifizierenden Anlagenbestandteile, Steuerungen, Sensoren und Aktoren sehr bald eine nahezu unüberschaubare Anzahl an zu verwaltenden sicheren Identitäten erfordern. Im ersten Ansatz wäre denkbar, dass diese Identitäten als Teil der Asset-Datenbank vorgehalten werden. Sinnvollerweise helfen die Identitäten auch dabei, Assets eindeutig und sicher identifizieren zu können. Ein Großteil der Kommunikation in der Industrie 4.0 soll jedoch sicher, das heißt primär „authentisiert“, erfolgen – was wiederum den Bedarf für eine häufige und schnelle Abfrage der ID-Informationen generiert. Für viele Millionen solcher Abfragen pro Sekunde auf eine schier unermessliche Anzahl an Einträgen

27 EN auch „Classification“. Die Datenklassifikation im Bestand zählt zu den schwierigsten und aufwändigsten Aufgaben in der IT-Sicherheit.

28 Clearance

29 MAC Mandatory Access Control ist ein sehr striktes Prinzip, das sich nicht für den Einsatz in der Industrie bewährt hat.

30 Attribute Based Access Control (ABAC)

31 Context Based Access Control (CBAC)

32 PAM/PIM/PUM – je nach Hersteller und Schwerpunkt werden die Lösungen jeweils als Privileged User Management, Privileged Access Management oder Privileged Identity Management bezeichnet. Deren Funktionalitäten konvergieren jedoch seit geraumer Zeit.

eignen sich Datenbanken nur bedingt – hier spielen Verzeichnisdienste eine entscheidende Rolle. Im Gegensatz zu den auf effiziente Speicherung ohne Dubletten ausgelegten Datenbanken bieten Verzeichnisse eine mehrfache Speicherung ähnlicher Datensätze an verschiedenen Stellen im hierarchischen Baum an. Somit können Anfragen zur selben Identität in unterschiedlichen Kontexten erheblich schneller beantwortet werden. Als Vergleich für die Industrie 4.0 sollen hier die Daten der Telefon- und Kabelgesellschaften dienen. Seit jeher werden die Kundendaten für die Bereitstellung der Dienste in Verzeichnissen gespeichert, um schnelle, wiederkehrende Abfragen zu beschleunigen und höchste Anforderungen an Verfügbarkeit gewährleisten zu können.

7 Sicherheit von Software in der Produktion

Industrie 4.0 und die starke Vernetzung von Produktionsanlagen erfordern robuste, verlässliche und vertrauenswürdige Software. Von den ERP- und MES-Systemen über die Prozessleit- und SCADA-Systeme bis zu den Speicherprogrammierbaren Steuerungen (SPS) bildet Software sicherheitskritische Prozesse ab. Dabei sieht sich der Anlagenbetreiber mit einer hochgradig heterogenen Softwarelandschaft konfrontiert: Er hat die Wahl zwischen einer Vielfalt an Technologien, Anbietern und Implementierungen. Der Anlagenbetreiber sollte die wesentlichen Eckpunkte sicherer Softwareentwicklung kennen, um von Zulieferern einen sicheren Entwicklungsprozess einfordern zu können. Nur mit diesem Wissen kann der Betreiber sicherstellen, dass seine Anlage der Bedrohungslage gewachsen ist. Zusätzlich gibt es Betreiber, die mit Software-Eigenentwicklungen die auf dem Markt verfügbaren Komponenten an die eigenen Bedürfnisse und Gegebenheiten anpassen. Auch hier spielen die Kriterien und Methoden sicherer Softwareentwicklung eine entscheidende Rolle. Dieses Kapitel führt die wesentlichen Schritte und Kriterien auf, die es bei Entwicklung, Wartung und Zusammenstellung der eingesetzten Software zu beachten gilt.

7.1 Softwaresicherheit

Maßgeblich dafür, ob ein Softwaremodul als sicher bewertet werden kann, ist ein sicherer Entwicklungsprozess der Software. Auch wenn es dem Betreiber beim Zukauf oftmals nicht möglich ist, im Detail nachzuvollziehen, welche Kriterien dem Entwicklungsprozess einer Software von Zulieferern zugrunde lagen, so lassen sich doch grobe Eckpunkte in Erfahrung bringen. Wie bereits erwähnt sollten diese Punkte insbesondere bei Eigenentwicklungen berücksichtigt werden.

Bereits bei Entwurf und Planung der Software spielt die spätere Einsatzumgebung eine wesentliche Rolle. Software, die einer großen Angriffsoberfläche (z. B. auf Verfügbarkeit, wie bei Distributed Denial of Service (DDoS)-Angriffen über externe Schnittstellen) ausgesetzt ist, muss der zu erwartenden Bedrohungslage speziell angepasst werden. Hierzu sollte zunächst eine grobe Risikoabschätzung stattfinden (siehe Abschnitt 2.4): Aus den schutzbedürftigen Werten (Assets) und einer Angriffsanalyse ergeben sich Sicherheitsanforderungen an die Software. Verarbeitet die Software beispielsweise sensible oder sicherheitskritische Daten, muss dies im Softwaredesign berücksichtigt werden (beispielsweise in Form von entsprechenden kryptographischen Modulen zur Verschlüsselung dieser Daten). Ein Anlagenbetreiber kann dann abgleichen, ob die angesetzten Sicherheitsanforderungen der Drittsoftware dem Schutzbedarf der Anlage entsprechen.

Die identifizierten Sicherheitsanforderungen fließen anschließend in den Entwurf der Software ein. Ziel ist es hier, die Angriffsoberfläche auf besonders kritische Bereiche der Software zu minimieren. Wird beispielsweise eine komplexe Datenstruktur eingelesen, so ist dieser Prozess oftmals sehr fehleranfällig: Angreifer nutzen oft Schwachstellen beim Parsen von solchen Datenstrukturen aus, um Schadcode auf das angegriffene System zu schleusen. In diesem Falle würde sich anbieten, zunächst die Herkunft der Datei zu überprüfen, gegebenenfalls auch durch die Überprüfung einer digitalen Signatur. Es werden dann zumindest nur Dateien aus vertrauenswürdigem Ursprung an den eigentlichen Einlese- und Verarbeitungsprozess

weitergeleitet. Grundsätzlich sollte man das Prinzip der geringstmöglichen Privilegien systematisch und konsequent durchsetzen: Jedes Modul, ob Prozess, Nutzer oder weiteres Programm, darf nur auf diejenigen Funktionen und Daten zugreifen, für die es die notwendigen Rechte besitzt. Die Rechteverteilung ist dabei so konservativ wie möglich anzusetzen. Im obigen Beispiel ist eine dreifache, aufeinanderfolgende Sicherheitsprozedur zu erkennen: Zunächst prüft die Software die Herkunft der Daten anhand eines digitalen Zertifikats, dann überprüft sie anhand der Zugriffsrechte, ob die Daten weiterverarbeitet werden dürfen, und dann erst wird die eigentliche Verarbeitung gestartet. Im Entwurfsprozess der Software sollte dieses Prinzip der mehrschichtigen Sicherheitsmaßnahmen („defense in depth“) systematisch angewendet werden, um die Angriffsoberfläche kritischer Softwaremodule auf ein Minimum zu reduzieren. Zusätzlich sollte der Funktionsumfang der Software weitestgehend eingeschränkt werden. Der Betreiber sollte zugekaufte Komponenten durch Deaktivieren nicht benötigter Softwaremodule und Funktionen selbst anpassen, vorausgesetzt die Komponente bietet eine solche Konfigurationsmöglichkeit an.

Für die Implementierung sollte auf geeignete Entwicklungsumgebungen zurückgegriffen werden. Schon über die Wahl der Programmiersprache lassen sich viele bekannte Einfallstore von vornherein ausschließen. Ferner lassen sich über Einstellungen des Compilers einige Sicherheitsaspekte ohne großen Aufwand realisieren. Auch sollte bei der Entwicklung auf möglichst sichere und aktuelle Software-Bibliotheken zurückgegriffen werden. Wird beispielsweise ein Modul zur Verschlüsselung von Daten implementiert, sollte der Entwickler auf gängige kryptographische Bibliotheken zurückgreifen, die insbesondere noch aktiv gepflegt werden.

Der Implementierung folgen Sicherheitstests, zunächst in Form von statischer und dynamischer Codeanalyse. Hier sind insbesondere Fuzzing (das Testen von Software mit randomisierten Eingabedaten) und das Testen auf Schwachstellen in der Speicherverwaltung (z. B. mittels Address-Sanitizer und ähnlichen Werkzeugen) zu nennen. Häufig werden so bereits viele Programmierfehler erkannt. Idealerweise findet zusätzlich ein manuelles Codereview anhand des Quellcodes statt.

Vor dem eigentlichen Release muss sichergestellt sein, dass sämtliche der im ersten Schritt identifizierten Sicherheitsanforderungen erfüllt wurden. Ausführbare Programme und sämtliche nachfolgenden Updates sollten vom Integrator digital signiert sein.

Für tiefergehende Informationen zur Entwicklung und Bewertung von Softwarekomponenten sei an dieser Stelle schließlich auf die Norm ISO/IEC 25000 („Software Engineering – Software Product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE”) als auch die zugehörige Normenreihe ISO/IEC 250xx hingewiesen. Ferner bietet der von Microsoft definierte Security Development Lifecycle (SDL)[33] detailliertere Beschreibungen zu den genannten Punkten.

7.2 Software-Pflege und -Wartung

Mindestens ebenso wichtig wie die sichere Entwicklung der Software ist deren Pflege und Wartung nach Auslieferung, soweit dies der Betrieb und die Wartungsfenster zulassen. Um der hochdynamischen Bedrohungslage gerecht zu werden, sollte idealerweise eine regelmäßige Neubewertung der Risiken stattfinden: Aus dieser ergeben sich dann neue Sicherheitsanforderungen, die entsprechend als Change Request in den Entwicklungsprozess einfließen. Diese Anpassung (Change) sollte beim Entwickler der Software stattfinden, der auf neue Angriffstrends mit entsprechenden Schutzmaßnahmen reagiert. Bei der Auswahl der Komponenten sollte der Betreiber also unbedingt abklären, inwiefern diese Form der Wartung und Anpassung (also die Möglichkeit, Changes zu beantragen und einzuspielen) an aktuelle Bedrohungen vom Zulieferer unterstützt wird. Insbesondere sollte der Softwareentwickler schnell auf bekannt gewordene Sicherheitslücken reagieren und entsprechende Updates ausliefern können, die dann ebenso rasch im Rahmen von Instandhaltungsarbeiten einfließen können. Die Auslieferung der Updates sollte dabei in einen fest definierten Release-Management-Prozess eingegliedert sein, der auch umfassende Tests der Softwareupdates einschließt – der Betreiber kann es sich nicht leisten, die Verfügbarkeit oder Integrität seiner Anlage durch ein Softwareupdate zu gefährden, das eine nur unwahrscheinlich angreifbare Schwachstelle absichert. Zudem ist auch der Updateprozess vor Angriffen abzusichern: Remoteupdates müssen über gesicherte Kanäle erfolgen, sämtliche neu eingespielte Software muss vom Entwickler digital signiert und diese Signatur von der gewarteten Komponente verifiziert werden können. Besonders im Feldbereich muss zusätzlich die Kompatibilität des Updates zu weiteren abhängigen Komponenten sichergestellt sein.

33 Vgl. Microsoft (Hrsg.) (2016)

7.3 Software-Governance

Zusätzlich zur Entwicklung und Wartung spielt Software-Governance, also die Organisation und Verwaltung der gesamten Software-Infrastruktur, eine wesentliche Rolle. Die Komplexität moderner Anlagen erfordert eine Vielzahl aufeinander abgestimmten Softwarelösungen. Für die Verwaltung dieser teils sehr heterogenen Softwarelandschaft innerhalb einer Anlage müssen Regelungen zur Einbringung und Verwaltung von Programmen aufgestellt werden. Als Erstes muss hierfür eine Inventarisierung und Dokumentation aller Softwarekomponenten der Anlage stattfinden. Diese Gesamtübersicht muss stets aktuell gehalten werden, unabhängig von den definierten Regeln zur Einbringung neuer Komponenten.

Die Umsetzung einer sicheren Softwareverwaltung setzt zunächst eine Regelung voraus, unter welchen Bedingungen neue Softwarekomponenten und Programme in die Anlage integriert werden dürfen. Zumindest sollen hier die definierten Kriterien für sichere Software berücksichtigt werden. Dabei sollten die Regelungen zur Einbringung der Software für jede Zone einzeln definiert werden. Beispielsweise kann für jede Zone festgelegt werden, welche Softwareklassen oder gar speziellen Programme installiert werden dürfen. Hier ist der Einsatz von Application-Whitelisting (siehe nächsten Abschnitt) und Blacklisting zu empfehlen, auch in Kombination mit spezifischen Regeln für die relevanten Akteure und Rollen. Benötigt ein Akteur dann ein Programm oder eine spezielle Programmversion, für das er keine Installationsberechtigung besitzt, kann die Anlage durch die Etablierung eines Software-Anforderungsprozesses dennoch weiterhin flexibel und sicher angepasst werden. Ein solcher Prozess wird dann die Überprüfung der oben genannten erforderlichen Mindeststandards beinhalten, wodurch die Softwaresicherheit der Gesamtanlage auf einem angemessenen Niveau gehalten werden kann. Ferner ist der Einsatz von Software-Managementsystemen sinnvoll, über die der Betreiber verteilte Programme gleichzeitig zentral einbringen, verwalten, updaten oder entfernen kann.

Die eingangs erwähnte Inventarisierung und Dokumentation aller Softwarekomponenten der Anlage ist ferner Grundlage für die Beobachtung der aktuellen Bedrohungslage: Werden Schwachstellen oder Sicherheitslücken bekannt, so kann der Betreiber abgleichen, ob seine Anlage direkt von diesen betroffen ist. Zum gegenwärtigen Zeitpunkt stellt die Inventarisierung aller Softwarekomponenten Anlagenbetreiber vor große Herausforderungen, für Anlagen der Industrie 4.0 wird eine solche aber unabdingbar sein und sollte zumindest angestrebt werden.

7.4 Whitelisting und Systemhärtung

In der Office-IT ist es seit wenigen Jahren üblich, Serversysteme nur mit den unbedingt notwendigen Funktionen auszuliefern bzw. zu betreiben. Noch in den späten 90er Jahren und Anfang des Jahrtausends war es üblich, sämtliche im Betriebssystem verfügbaren Dienste im Auslieferungszustand aktiv zu haben, auch wenn diese nicht genutzt wurden. Später wurden dann nachträglich sogenannte „Systemhärtungen“ vorgenommen, bei denen die nicht genutzten Dienste und Funktionen deaktiviert wurden. Dies ist bis heute in den IT-Komponenten der Produktion eher unüblich und führt durch die nicht aktualisierten Systeme zu sehr großen Angriffsflächen. Diese Angriffsflächen sind im Kontext der Industrie 4.0 nicht mehr annehmbar, so dass für veraltete und nicht mehr in Wartung befindliche Systeme dringend Schutzmaßnahmen benötigt werden. Neben den zum Zeitpunkt der Erstellung dieses Leitfadens aufkommenden mathematisch-prädiktiven Systemen[34] haben sich Whitelisting-Lösungen als wirksam und anwendbar erwiesen. Im einfachsten Falle bedeutet Whitelisting die Erstellung einer Liste von erlaubten Programmen: Ausschließlich Programme dieser Liste können gestartet werden. Wesentlich fortgeschrittener sind Listen, die anhand des normalen Systemverhaltens automatisiert erlernt wurden. Diese aus heutiger Sicht wichtigste Methode zum Schutz von Bestandssystemen wird als kleine Softwarekomponente auf einem als „sauber“ eingestuften Alt-System installiert und beobachtet über einen Zeitraum das Verhalten der Systemprozesse, Dienste, die Netzwerkkommunikation und die Interaktionen der Programme. Nach dieser Lernphase wird das System in den Überwachungsmodus geschaltet, und meldet vormals nicht protokolliertes Verhalten als außergewöhnlich. Nach einer manuellen Entscheidung, welche der neu gefundenen Muster normal oder anormal waren, wird das System aktiviert. Jegliche außergewöhnliche Aktivität (wie sie durch einen Virusbefall oder den Start von Programmen von einem USB-Stick ausgelöst werden) wird nun aktiv unterbunden.

34 Etwa die vom US-Unternehmen Cylance vorgestellten Mechanismen

8 IT-Sicherheit beim Einkauf von Maschinen und Anlagen berücksichtigen

Mit der steigenden Vernetzung von Maschinen und Anlagen im Rahmen von Industrie 4.0 gehen neue Gefahren einher, die bislang im Einkaufsprozess kaum eine Betrachtung finden. Der Fokus bei der Auswahl von Maschinen und Anlagen liegt bislang z. B. auf Funktionsumfang, Verfügbarkeit und Ausbringungsraten. Dies führt unter anderem dazu, dass neue Produktionsmaschinen noch heute mit Systemsoftware ausgeliefert werden, deren Wartungszusage durch den Integrator bereits abgelaufen ist.

Dass Securityanforderungen keine Berücksichtigung finden, ist insbesondere in Verbindung mit der langen Lebensdauer (häufig länger als 20 Jahre) von Maschinen und Anlagen kritisch. Eine nachträgliche Anpassung an die neue Bedrohungslage ist häufig nicht möglich, da solche Veränderungen an Maschinen und Anlagen in der Regel weitreichende Konsequenzen wie den Verlust der Unterstützung durch den Anbieter oder die vollständige erneute Prüfung der Anlage nach der Betriebssicherheitsverordnung (BetrSichV) nach sich ziehen würden. Der laufende Betrieb der vorgenannten abgekündigten Betriebs- und Steuerungssysteme stellt eine der größten Herausforderungen der heutigen Produktions-IT dar. Hier muss abgewogen werden, ob ein „Einfrieren“ der Systeme durch spezielle Software sinnvoll und mit dem Integrator vereinbar ist.

Erschwerend kommt die fatale und immer bestehende Denkweise hinzu, dass Maschinen die praktisch nicht am Internet hängen, unangreifbar sind. Angriffe wie Stuxnet haben hier das Gegenteil bewiesen und zeigen den nachträglichen Anpassungsbedarf an eine veränderte Bedrohungslage ebenfalls auf.

Die veränderte Sicherheitslage mit einer Vielzahl neuer Malware und gezielten Angriffen auf Industrieanlagen macht deutlich, dass bei der Auswahl von Maschinen und Anlagen auch ein Mindestmaß an nachhaltiger IT-Sicherheit gefordert werden muss, sodass eine sichere Anbindung und ein sicherer Betrieb ermöglicht werden. Hierbei ist nicht nur der Anschaffungszeitpunkt, sondern auch der komplette Lebenszyklus der Maschinen und Anlagen zu beachten. Im Rahmen der Einführung eines Sicherheitskonzepts für die IT in der Produktion muss zunächst der Einkaufsprozess betrachtet und überarbeitet werden, um die Weichen für die Zukunft richtig zu stellen. Durch die Erstellung oder Erweiterung von Einkaufsrichtlinien können Vorgaben an die IT-Sicherheit von Maschinen und Anlagen eingeführt und gegenüber dem Lieferanten eingefordert werden.

Bei der Anschaffung von neuen Maschinen oder Anlagen ist schon im Vorfeld darauf zu achten, dass gemeinsam mit dem Lieferanten eine abgestimmte und langfristige Lösung für den sicheren Betrieb der Anlage über den kompletten Lebenszyklus ausgearbeitet und vereinbart wird. Industrieverbände wie ZVEI und VDMA weisen ihre Mitglieder in eigenen Publikationen auf diesen Bedarf hin und erstellen ihrerseits Forderungen zu mehr IT-Sicherheitskriterien bei der Beschaffung von Modulen oder Bauteilen.

8.1 Gesamtheitliche Betrachtung des Einkaufsprozesses

Mit dem Vorhaben, IT-Sicherheit von Maschinen und Anlagen bereits im Einkaufsprozess zu berücksichtigen, zeigt sich einmal mehr, dass IT-Sicherheit ein komplexes Projekt ist, welches sich auf alle Unternehmensbereiche auswirkt. Die durchgehende Anpassung des Einkaufsprozesses auf die neuen Anforderungen von IT-Sicherheit und Industrie 4.0 ist mit recht hohem Aufwand verbunden. Die langfristig sinnvolle Digitalisierung und Automatisierung der Prozesse ist aus Sicht von KMU mit hohem Aufwand und großen Investitionen verbunden. Aber natürlich müssen nicht alle Maßnahmen gleichzeitig gestartet werden und häufig helfen schon einfache Veränderungen oder die Einführung neuer Werkzeuge, um das Level der IT-Sicherheit bereits im Einkaufsprozess zu verbessern.

IT-Sicherheit muss ein wesentlicher Bestandteil des Beschaffungsprozesses von Maschinen und Anlagen sein. Hierfür muss zunächst ein einheitlicher Beschaffungsprozess mit ausreichendem Gültigkeitsbereich definiert sein und dieser muss auch entsprechend gelebt werden. Wenn bereits gute Prozesse, Richtlinien und Werkzeuge etabliert sind, müssen diese hinsichtlich der Berücksichtigung von IT-Sicherheit erweitert werden. An einigen Stellen wird es sinnvoller sein, zusätzliche Prozesse zu definieren, als bewährte Prozesse anzupassen. Solche Entscheidungen müssen für jedes Unternehmen bzw. jeden Beschaffungsprozess individuell getroffen werden und müssen eine ausreichende Analyse zur Grundlage haben.

Daher ist der erste Schritt zur IT-Sicherheit im Beschaffungsprozess eine entsprechende **Prozessanalyse** mit Fokus auf die Berücksichtigung von IT-Sicherheit. Hierbei zeigt sich in der Praxis häufig, dass der Beschaffungsprozess selbst und seine zugehörigen Prozesse (z. B. Prozesse des Lieferantenmanagements) nicht ausreichend definiert sind und IT-Sicherheit keinerlei Betrachtung findet. Auch angrenzende Prozesse, die als wichtiger Input für die IT-Sicherheit dienen würden (z. B. Asset-Management), fehlen in der Regel. Die für IT-Sicherheit bei Industrie 4.0 notwendigen Kompetenzen sind ebenfalls häufig noch nicht vorhanden und in der Unternehmensstrategie oft auch nicht vorgesehen. Adressiert werden in der Analysephase unter anderem folgende Fragestellungen:

- Ist eine Einkaufsrichtlinie für Maschinen und Anlagen vorhanden und findet IT-Sicherheit hier Beachtung?
- Werden Lieferanten bzgl. der IT-Sicherheit ihrer Prozesse, Produkte und Serviceangebote bewertet?
- Wie werden die IT-Komponenten neuer Maschinen und Anlagen in bestehende Systeme eingepflegt (Asset-Management)?
- Sind ausreichend Kompetenzen hinsichtlich IT-Sicherheit in der Produktion vorhanden und in den Einkaufsprozess eingebunden?
- Gibt es eine Übersicht über „Kommunikationspartner“ in der Produktion und die ausgetauschten Daten?
- Wird diese Übersicht bereits im Rahmen des „Einbindungskonzepts“ auf IT-Sicherheitsrisiken geprüft?

Die Analyse zeigt im Idealfall möglichst viele der relevanten Schwachstellen im Unternehmen auf und muss Beachtung auf höchster Managementebene finden, damit die **Planung** neuer Prozesse durch die notwendigen Ressourcen ermöglicht wird. Im Folgenden sind wesentliche Aktivitäten der Prozessplanungsphase aufgeführt:

Schritte der Prozessplanung

- Erarbeitung neuer Konzepte
- Erstellung neuer Richtlinien
- Überarbeitung bestehender Prozesse
- Neudesign fehlender Prozesse
- Aufbau von notwendigen Kompetenzen
- Entwurf neuer Richtlinien

Die **Umsetzung** der definierten Maßnahmen muss aktiv durch das Management gefordert und gefördert werden. Wurden Analyse, Planung und Umsetzung durchlaufen, muss im letzten Schritt eine kontinuierliche **Evaluierung** der umgesetzten Maßnahmen in der Betriebsphase erfolgen. Aufgrund der Ergebnisse der Evaluation werden die durchgesetzten Maßnahmen und Prozesse kontinuierlich verbessert und überarbeitet.

8.2 Ziele einer Einkaufsrichtlinie

Mit dem Einkauf von Produktionseinrichtungen in Form von Maschinen und Anlagen kauft der Betreiber die zugehörigen IT-Komponenten in der Regel mit ein. Er muss sich daher auch mit der IT des Produkts und mit der IT-Sicherheit auseinandersetzen. Ein gutes und wenig komplexes Werkzeug für IT-Sicherheit im Einkaufsprozess stellt eine aktuell gehaltene Einkaufsrichtlinie dar. Auch wenn sie im ersten Schritt nicht alle Anforderungen vollumfänglich beinhaltet, ist es zunächst wichtig, die IT-Sicherheit von Maschinen und Anlagen hier überhaupt zu verankern. Die Anweisungen in einer solchen Einkaufsrichtlinie macht das Auseinandersetzen mit dem Thema IT-Sicherheit notwendig und hilft dabei, grundlegende Anforderungen gegen-

über dem Lieferanten durchzusetzen und aktiv Fragen zur IT-Sicherheit zu stellen. Hierfür ist es notwendig, die Inhalte der Einkaufsrichtlinie in enger Zusammenarbeit mit den Verantwortlichen der IT-Sicherheit zu erarbeiten.

Alle bisher in diesem Leitfaden betrachteten Grundlagen der IT-Sicherheit können und müssen auch und insbesondere für Produktionsmaschinen und die darin verbauten Komponenten sowie die verwendete Software gelten. Die Erkenntnisse aus den vorgelagerten Abschnitten führen damit direkt zu Anforderungen, die mittels einer Einkaufsrichtlinie aktiv beim Anlagenlieferanten einzufordern sind. Um beispielsweise ein vollständiges Asset-Management zu ermöglichen, muss dem Betreiber ersichtlich sein, welche IT-Komponenten in einer Anlage verbaut wurden (Vgl. Kapitel). Die Sicherheitsanforderungen, die sich direkt oder indirekt aus den vorherigen Abschnitten ableiten lassen, sind nachfolgend übertragen auf die Inhalte einer Einkaufsrichtlinie in Form eines Anforderungs- und Feature-Kataloges dargestellt. Dieser hat dabei keinen Anspruch auf Vollständigkeit und soll als eine erste Inspiration dienen. Es muss weiterhin darauf hingewiesen werden, dass für einige Anforderungen und Features im Kontext von Industrie 4.0 zunächst neue Gesetze und Standards geschaffen werden, so dass derzeit noch nicht alle Anforderungen durchgesetzt werden können.

8.3 Exemplarischer Katalog für die Einkaufsrichtlinie

In dem nachfolgenden Anforderungs- und Feature-Katalog ist aufgeführt, welche Anforderungen an den Integrator von Maschinen und Anlagen zu stellen sind beziehungsweise hinsichtlich welcher sicherheitsrelevanter Features die Produkte zu bewerten sind. Ob es sich jeweils um harte (unmittelbare Beeinflussung der Kaufentscheidung) oder um wünschenswerte Aspekte (z. B. Anforderungen, die mit Industrie 4.0 einhergehen werden, aber heute noch nicht nötig sind) handelt, muss dabei jedes Unternehmen individuell evaluieren. Dabei muss der Markt eingehend hinsichtlich der maximal möglichen Anforderungserfüllung geprüft werden.

A. Zugriffsschutz durch User-Management (siehe Abschnitt 6)

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Strikte Funktionstrennung von administrativen und produktiven Berechtigungen durch internes User-Management an der Anlage und ihren IT-Komponenten.	6.7
Benutzerkonten des Systems können über ein zentrales Berechtigungsmanagement (Identitäts- & Berechtigungs-Management) provisioniert werden.	6.1
Vereinfachte Anmeldung an IT-Komponenten und Web-Applikationen durch Schnittstellen zu zentralen Anmeldeverfahren.[35]	6.1
Methoden der starken Authentisierung können genutzt werden.[36]	6.1

B. Zugangsschutz

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Es wird verhindert, dass unberechtigte Personen Modifikationen an Anlagenteilen und Steuerungskomponenten vornehmen können, z. B. durch physische Separation von Bediener- und Administrator-Funktionen, durch abschließbare Bedienungspanel oder durch Funktionsfreischaltung unter der Verwendung von Funk-Chips (RFID).	6.4
Möglichkeiten zur Überwachung der Leitungen des Kontrollsystems. Erkennungsfunktionen bringen bereits einige neue Intrusion Detection Systeme (IDS) mit.	5.9

35 Einbindung in ein Enterprise Single Sign-On (SSO) oder Web-SSO, das die einmalige Anmeldung und einfache Nutzung mehrerer Applikationen und Systeme ermöglicht

36 Etwa die Verwendung von Ausweiskarten/Chipkarten (sogenannten Smartcards) oder die Nutzung von elektronischen Schlüsselkarten bzw. Anhängern mit Funktechnik (RFID)

C. Kryptographische Fähigkeiten der Anlage und der Komponenten

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Verwendete Algorithmen und Schlüssellängen sowie die vom Software-Hersteller verwendeten Crypto-Bibliotheken werden offengelegt.	5.7
Risikoanalyse der eingesetzten Software wurde durchgeführt. Die Ergebnisse werden dem Betreiber transparent dargelegt.	7
Schwache Protokolle oder gefährdete Datentransfers sind durch Kryptographie angemessen abgesichert.	Siehe auch 5.7 und 5.9
Änderungen an Verschlüsselungs-Algorithmen, Schlüssellängen oder verwendeten Bibliotheken müssen dem Betreiber mitgeteilt bzw. offengelegt werden.	7.3
Offene und bekannte, erprobte kryptographische Standards wie TLS 1.2 oder höher werden eingesetzt und bei der Wahl der zugelassenen Algorithmen wird den Empfehlungen des BSI gefolgt.	5.5 und 6.5

D. Definition des sicheren Auslieferungszustands (Security by Default)

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Die Maschine oder Anlage ist durch den Integrator so auszuliefern, dass alle für den Minimal-Betrieb nicht unmittelbar benötigten Funktionen in der Basis-Installation standardmäßig deaktiviert sind.	7.1
Hinweise zur Aktivierung und Deaktivierung von Features müssen in der mitgelieferten Dokumentation vorhanden sein.	4.1
Die Sicherheitseinstellungen für die Features des Minimal-Betriebs sind zu validieren.	
Bei der Inbetriebnahme darf die Software keinerlei Standard-Passwörter oder -Benutzerkonten verwenden.	6.1 und 6.7
Bei der Vergabe neuer, individueller Passwörter für die administrativen Accounts Passwort-Regeln zur Vergabe sicherer Passwörter einsetzen.	6.7
Passwörter der administrativen Zugänge müssen aus der Software heraus geändert werden können (sofern kein Verzeichnisdienst zur Rechteverwaltung eingesetzt wird).	6.1

E. Nachweis der sicheren Software-Entwicklung

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Durchgängiges Qualitäts- und Test-Management bei der Entwicklung der Software und entsprechende Dokumentation.	7
Offenlegung von Testfällen, Testreports und Pflege der Release Notes zu jedem Update.	7.2 und 7.3
Nachweis über die Entwicklung der Software nach den Vorgaben des Security Development Lifecycle (SDL): Der Maschinen- oder Anlagenhersteller soll nachweisen, dass dies bei der Auswahl der Softwarezulieferer berücksichtigt wurde.	7.1
Versicherung, dass in den Produkten ausschließlich Software eingesetzt wird, die bereits in der Designphase auf Sicherheit ausgelegt wurde, und dass Software Dritter, insbesondere Open Source Software, ordnungsgemäß auf Schwachstellen untersucht wurde.	7.3
Die Software muss (falls erforderlich) ausfallsicher betrieben werden können. Der Integrator soll nachweisen können, wie diese Ausfallsicherheit erreicht werden kann.	

F. Funktionstrennung (Segregation of Duties – SoD)

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Betrieb der eingesetzten Software darf keinesfalls im Kontext eines höher privilegierten Benutzers (admin, system root etc.) erfolgen.[37]	6.7
Die Software muss auf die Nutzung minimaler Privilegien ausgelegt sein und muss auch im Kontext eines über das Active Directory (AD) verwalteten Benutzerkontos ohne besondere Privilegien ausführbar sein.	6.6

37 Insbesondere durch die Einführung des User Account Control (UAC) bei Windows Vista, 7 und 8 kann heute ein Großteil der für Windows XP entwickelten Anwendungen nicht mehr laufen, da diese „SYSTEM“- oder „ADMINISTRATOR“-Kontext erfordern.

G. Applikations-Integration über eine DMZ/Service Zone

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Für den Betreiber ist insbesondere die Einbindung des Anlagennetzes in die Produktion über die bekannten „Gateways“ interessant. Hier sollte der Anbieter spezifizieren, welche Protokolle und Ports er für einen sicheren Betrieb benötigt.	5.2 und 5.3

H. Integration der Software in das bestehende Security-Management

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Die Anbindung der Software an bestehende Security-Management-Systeme wird z. B. durch die eingesetzten Protokolle und Schnittstellen ermöglicht. Beispiele für unter Umständen anzubindende Systeme sind: • IAM Identitäts-Management/Berechtigungsmanagement • Log-Management und SIEM Security Information and Event Management • AD Active Directory	6 5.9.1 6.8

I. Internet-Zugriff

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
In der Maschine oder Anlage verwendete Software darf nicht von sich aus eine Verbindung nach außen (in das Internet) herstellen.	etwa 5 ff.
Ein „Stand-alone“-Betrieb der Software (ohne Verbindung zum Internet) muss möglich sein. Wenn der Internet-Zugriff elementar und notwendig ist, muss der Betrieb der Maschine oder Anlage aus einer DMZ heraus möglich sein.	5.1
Detaillierte Darstellung, welche Protokolle und Ports genutzt werden und welche Daten zu welchem Zweck ausgetauscht werden, wird durch den Lieferanten bereitgestellt.	5.2 und 5.3
Der Betreiber muss zu jeder Zeit in der Lage sein, Verbindungen von sich aus unilateral zu unterbinden, ohne die Produktion dauerhaft zu beeinträchtigen.	5.5

J. Offenheit der (Fern-)Wartungsfunktionen der Anlage

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Sofern eine Fernwartung als notwendig angesehen wird, muss dieser Zugang möglichst über ein etabliertes Standardverfahren erfolgen[38] und jeweils zeitlich begrenzt sein.	Abschnitt 5.5
Eine Initiierung der Verbindung kann nur von innen nach außen vorgenommen werden, um nicht-autorisierte Zugriffe Dritter zu erschweren.	5.5
Der Aufbau der Verbindung darf ausschließlich mit einer expliziten Zustimmung im Rahmen des Verbindungsaufbau-Prozesses durch einen Administrator seitens des Betreibers erfolgen (Vier-Augen-Prinzip).	5.5
Ein Monitoring der während der Fernwartung durchgeführten Aktivitäten muss ermöglicht werden.	5.9
Die eingehende Verbindung muss nach Möglichkeit auf den betroffenen Anlagenteil beschränkt werden können. (Hierzu empfiehlt es sich, bereits bei der Planung der Anlage seitens des Integrators eine Abgrenzung der logischen Teile bzw. Segmente der Anlage derart zu gestalten, dass der Betreiber die Eintrittspunkte entsprechend setzen kann.)	5.9 und insbesondere 5.9.2

K. Schwachstellen- und Update-Management

Anforderungen an den Integrator von Maschinen und Anlagen	Details u. a. in Abschnitten
Der Integrator der Maschine oder Anlage verpflichtet sich, Informationen zu neu gefundenen Schwachstellen in seinen Anlagen umgehend an die Anlagenbetreiber weiterzugeben.[38]	7.1 sowie 7.2 und 7.3
Der Maschinen- oder Anlagenhersteller sollte vertragliche Nachweise über das vereinbarte Schwachstellen-Management mit seinen Softwarezulieferern erbringen.	7 ff.
Der Maschinen- und Anlagenhersteller sollte selbständig die bekannten Kanäle für Veröffentlichung von Sicherheitsschwachstellen überwachen.	7.3
Der Integrator soll zeitnah nach Bekanntwerden von Sicherheitslücken geeignete Sicherheits-Updates und Patches liefern. Dafür ist es notwendig, dass die Software mit Hilfe von Updates, Upgrades, Patches, Fixes und Hotfixes aktualisiert werden kann.	7, insbesondere 7.2

38 Vgl. VDMA Verlag (o. J.)

L. Patch-Management durch den Betreiber

Anforderungen an den Integrator von Maschinen und Anlagen	Details u.a. in Abschnitten
Im Laufe des Produktlebenszyklus bekannt werdende Schwachstellen von Systemkomponenten und verwendeter Software müssen über Patches geschlossen werden können.	wie oben Abschnitt 7 ff.
Patches sollten nur in streng definierten und angemessenen Fällen (Safety-kritische Anwendungen und Systeme) dazu führen, dass der Anbieter aufgrund der Veränderung des Auslieferungszustands Nachteile im Support oder den Verlust des Supports fürchten muss.	7.2

M. Beschränkung der Unveränderbarkeit des Lieferzustands

Anforderungen an den Integrator von Maschinen und Anlagen	Details u.a. in Abschnitten
Es muss aufgezeigt werden, inwiefern der Maschinen- und Anlagenhersteller der Forderung nach Aktualisierbarkeit, Updatefähigkeit und ggf. sogar Austauschbarkeit IT-relevanter Anlagenkomponenten gerecht werden kann.	7.2
Es muss aufgezeigt werden, welche Veränderungen an dem Produkt vorgenommen werden können, ohne dass dies negative Konsequenzen (wie z. B. eine notwendige Neuprüfung nach Betriebssicherheitsverordnung (BetrSichV)) mit sich bringt.	7.2

N. Dokumentation

Anforderungen an den Integrator von Maschinen und Anlagen	Details u.a. in Abschnitten
Detaillierte Dokumentation zur Software wird bereitgestellt und beinhaltet u. a.: • Darstellung der internen Architektur der Software • Beschreibung der Kernfunktionen • Struktur der Schnittstellen • Hinweise auf die Rahmenbedingungen, unter denen die Software betrieben werden kann (System Requirements, Systemanforderungen). • bekannte Probleme und Einschränkungen bei der Interoperabilität[39]	insbesondere Abschnitt 7 ff.
Dokumentation der anlageninternen und übergreifenden Datenflüsse[40]	5 und 6.5
Die Dokumentation muss regelmäßig bei Änderungen der Software angepasst werden und dem Betreiber zur Verfügung gestellt werden.	

O. Anforderungen für die spätere Administration (Security in Deployment)

Anforderungen an den Integrator von Maschinen und Anlagen	Details u.a. in Abschnitten
Dokumentation und Tools des Software-Integrators sollen mitgeliefert werden, um die Administratoren in die Lage zu versetzen und dabei zu unterstützen, die Software bestmöglich einzurichten.	7.2, 7.3
Eine Auflistung sämtlicher Dateien und Konfigurationen der Basis-Installation und sämtlicher nachinstallierbaren Features, Upgrades, Updates, Patches, Fixes und Hotfixes wird geliefert.	besonders 4.1.4 und 4.1.5
Die Software soll über eine Rollback-Funktionalität verfügen, mit der zu gegebener Zeit vorgenommene Aktualisierungen wieder rückgängig gemacht (deinstalliert/entfernt) werden können.	4.4
Die Software sollte eine integrierte Versionskontrolle beinhalten, mit deren Hilfe z. B. der Administrator jederzeit die aktuelle Version bzw. den aktuellen Patchlevel der Software ermitteln kann.	

39 Sich evtl. ausschließende Kombinationen von anzubindender Software, Betriebssystem, Datenbanken etc.

40 Insbesondere dann unabdingbar, wenn eine gesicherte Überwachung dieser Kommunikation etwa mittels Intrusion Prevention Systemen (IPS) erfolgen soll.

8.4 Anforderungen an Lieferanten/Integratoren von Maschinen und Anlagen

Aus den vorgenannten Einkaufsbedingungen leitet sich eine Reihe von Anforderungen an IT-Sicherheit insbesondere für die Lieferanten ab. Diese können – auf Basis des derzeitigen Kenntnisstands der Lieferanten und deren begrenzten Ressourcen – nicht sofort bindenden Charakter haben oder als Ausschlusskriterien definiert werden, da dies die Lieferanten gleichermaßen überfordert. Dennoch ist der Bedarf der Betreiber nach mehr Sicherheit für die Anlagen und mehr Anpassbarkeit der IT-Komponenten ein Pflichtbaustein für die mittelfristige Migration auf Prozesse der Industrie 4.0. Nur durch eine klare Kommunikation des Bedarfs für solche Funktionen und Eigenschaften erfahren die Integratoren und Lieferanten den notwendigen „Sog" aus dem Markt, um entsprechende Funktionen entwickeln zu lassen. Einige der Anforderungen sind wie folgt:

- Gewährleistung der IT-Sicherheit der Anlagen und Subsysteme durch nachgewiesene Sicherheitsprozesse, Konzepte und Verantwortlichkeiten
- Sichere Entwicklung von Anlagen und Software unter Betrachtung der Sicherheitsanforderungen, die aus Bedrohungs- und Risikoanalysen abgeleitet werden
- Detaillierte Risikoanalyse für jeden Maschinentyp bzw. jede individuelle Anlage
- Präventives und aktives Schließen von gefundenen Sicherheitslücken
- Einsatz sicherer Software, auch Open-Source – Validierung und Code Reviews
- Schwachstellen-Management mit Zulieferern vertraglich absichern
- Dokumentation eingesetzter Hard- und Software zur Weitergabe an den Betreiber
- Anpassung der Geschäftsmodelle, um Support über Produktlebenszyklus gewährleisten zu können
- Anbindung von Security-Systemen ermöglichen

8.5 Anforderungen an Standardisierung

Damit der Integrator von Maschinen und Anlagen den Anforderungen aus der Einkaufsrichtlinie gerecht werden kann, sind zunächst klare Regelungen und verbindliche Standards zu definieren. An solchen Gesetzen, Standards und Werkzeugen zur praktischen Umsetzung wird in diversen Organisationen und Verbänden gearbeitet.

Solche Regelungen müssen vor allen Dingen bereichsübergreifend gültig sein, da nicht der Integrator von Maschinen und Anlagen alleine für die Sicherheit und den sicheren Betrieb der Maschine und Anlage verantwortlich sein kann. Die wesentlichen beteiligten Rollen (z. B. Hersteller, Integrator, Betreiber) und deren verschiedenen Aufgabenbereiche und Verantwortlichkeiten sind derzeit unter anderem durch IEC 62443 wie auch durch VDI/VDE 2182 definiert. In diesem Bereich bedarf es unter anderem weiterer Konkretisierung.

8.6 Relevante Rollen nach IEC 62443

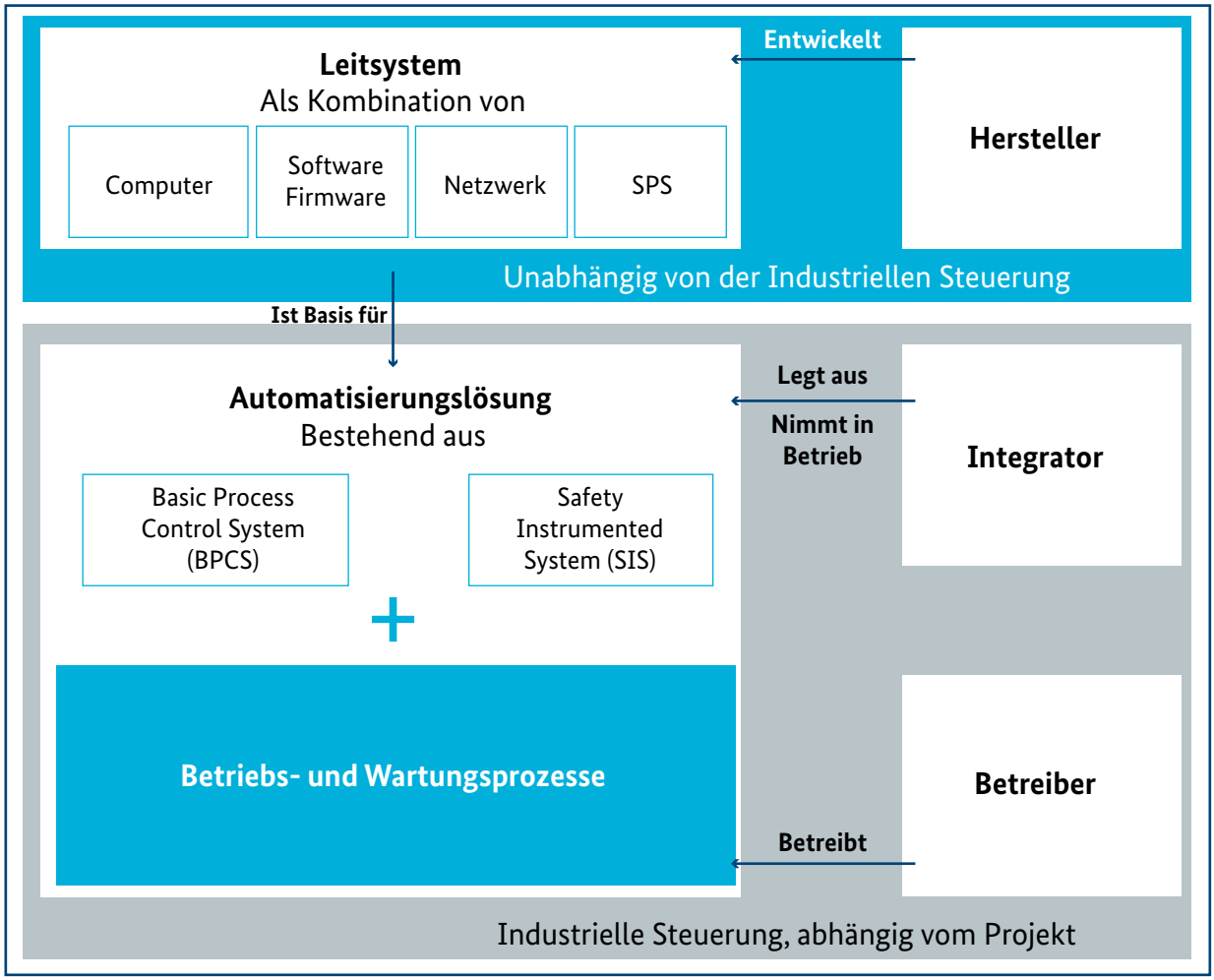
Insbesondere im Einkaufsprozess von Maschinen und Anlagen wird deutlich, dass die Sicherstellung von IT-Sicherheit nur durch das Zusammenwirken der kompletten Lieferkette erreicht werden kann und dass alle relevanten Rollen hier einen Beitrag leisten müssen. Als Rollen können in Anlehnung an IEC 62443 Hersteller, Integratoren und Betreiber von Maschinen und Anlagen benannt werden. Um eine erste Übersicht zu ermöglichen, kann die Abbildung 10 helfen.[41, 42]

Neben der Sicht der IEC 62443 werden diese Themen auch in VDI/VDE 2182 aus etwas anderer Perspektive betrachtet – hier wird neben den internen Zyklen für die Betrachtung der Sicherheit auch die Interdependenz zwischen Hersteller, Integrator und Betreiber dargestellt, wie in Abbildung 13 ersichtlich wird. Die Rollen selbst sind allerdings nicht immer scharf voneinander abtrennbar und die Zuweisung der entsprechenden Verantwortlichkeiten wird im Kontext von Industrie 4.0 auf verschiedenen Ebenen diskutiert. Unter Hersteller ist in diesem Zusammenhang der Hersteller und Zulieferer von (Steuerungs-)Komponenten zu verstehen. Die Rolle des Maschinen- und Anlagen-Herstellers wird an dieser Stelle durch den Integrator beschrieben, wobei es sich hier durchaus auch um zwei verschiedene Rollen handeln kann, da Auslegung und Inbetriebnahme auch getrennt voneinander betrachtet werden können. Die Rolle des Integrators im Sinne der Inbetriebnahme und die damit verbundenen Verantwortlichkeiten werden auch häufig zu externen Dienstleistern ausgelagert.

41 Vgl. Kobes, P. (2015)

42 Vgl. VDE Verlag (2016)

Abbildung 10: Rollen der IEC 62443



Quelle: nach Kobes, P. (2015)

9 Standards, Dokumente und Organisationen

Die sichere Umsetzung von Konzepten wie Industrie 4.0 und Internet der Dinge (Internet of Things – IoT) erfordern Regeln und Strukturen, welche die noch bestehenden Branchengrenzen zwischen Elektrotechnik, Maschinenbau und IT überwinden müssen. Einheitliche Standards und Richtlinien – im Idealfall auf globaler Ebene – ermöglichen erst die Interoperabilität von Unternehmen und schaffen, durch entsprechende Nachweise zur Einhaltung, eine Vertrauensbasis.

Bei der Umsetzung der empfohlenen und teilweise durch Gesetze geforderten Vorgehensweise zur Schaffung eines geeigneten IT-Sicherheitsniveaus stellen Standards, Richtlinien und Leitfäden ebenfalls ein unabdingbares Hilfsmittel dar. Für den Einstieg in die Thematik sollte zunächst ein Überblick über die Vielzahl von Standards und Richtlinien gewonnen werden, um anschließend die zielgruppengerechten und relevanten Dokumente auszuwählen.

Die notwendige vollumfassende Übersicht zu relevanten Dokumenten kann im Rahmen des Leitfadens nicht gegeben werden. Allerdings sollen einige der relevantesten Organisationen, Standards und Leitfäden und ähnlich weiterführende Dokumente übersichtlich vorgestellt werden.

9.1 Relevante Organisationen

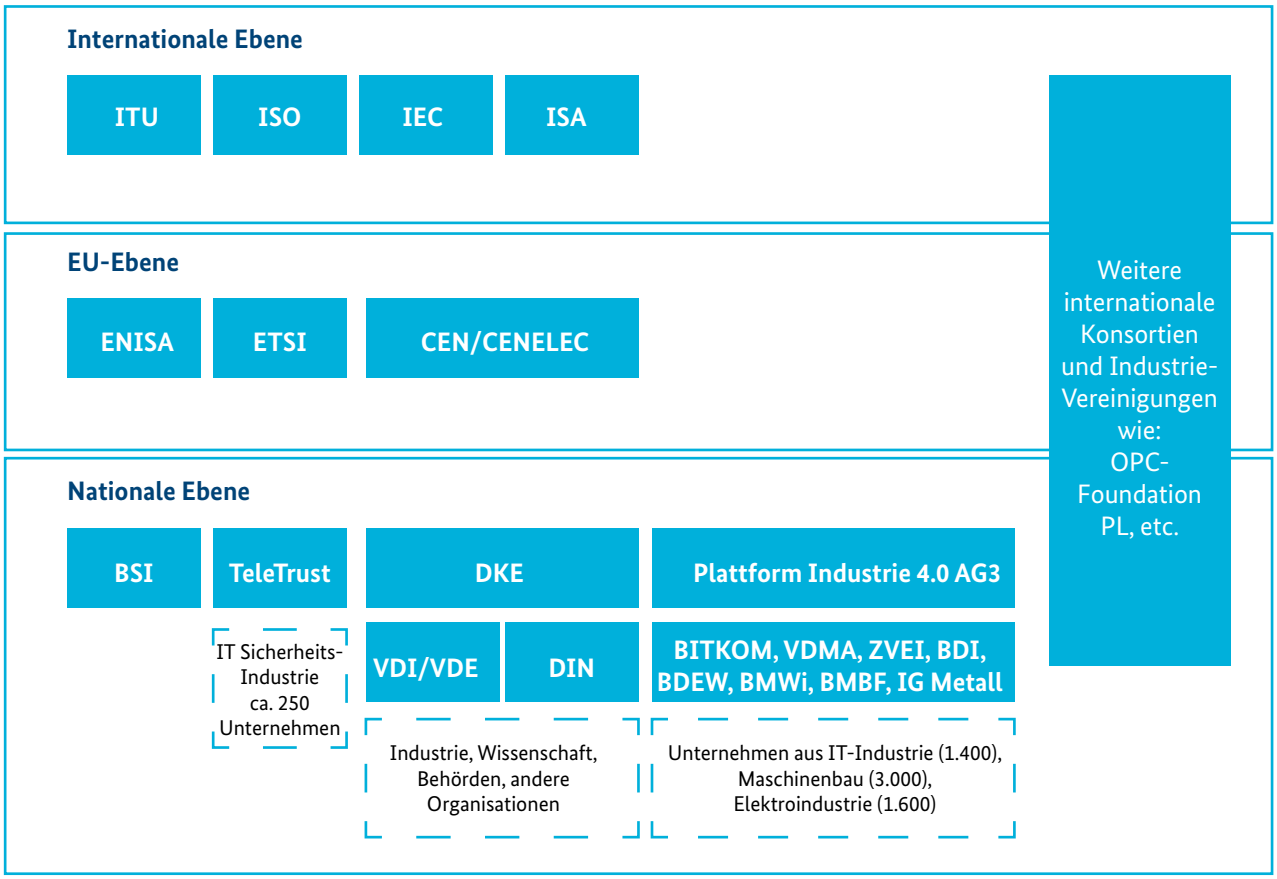
Die herausgebende Organisation stellt ein wesentliches Charakteristikum von Standards, Richtlinien und ähnlichen Dokumenten dar. Anhand der herausgebenden Organisation ist erkennbar, wie branchenübergreifend und geografisch verbreitet das Dokument von Relevanz ist. Das Wissen über die herausgebende Organisation ermöglicht damit eine erste Einordnung eines Dokuments. Für eine umfangreiche Übersicht existieren daher zahlreiche Dokumente, die an dieser Stelle deutlich als weiterführende Dokumente empfohlen werden sollen. Hierzu gehören unter anderem:

- Studie des BMWi „IT-Sicherheit für Industrie 4.0“[43]
- Grafische Übersicht des DKE zu „Arbeitsgruppen und Gremien im Bereich Industrie 4.0“[44]
- Kompass der IT-Sicherheitsstandards von Bitkom[45]
- „Handreichung zum Stand der Technik“ des TeleTrusT, im Kontext des IT-Sicherheitsgesetzes mit Empfehlungen hinsichtlich Stand der Technik[46]

In der Langfassung des Abschlussberichts zur oben benannten BMWi-Studie ist unter anderem eine durch das Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik (ESK) erstellte Übersicht zu den im Kontext von IT-Sicherheit und Industrie 4.0 relevanten Organisationen dargestellt (siehe Abbildung 11).

43 Vgl. BMWi (Hrsg.) (2016c)
44 Vgl. VDE (Hrsg.) (2016)
45 Vgl. bitkom (Hrsg.) (2014)
46 Vgl. TeleTrust (Hrsg.) (2014)

Abbildung 11: Übersicht der für IT-Sicherheit und I4.0 relevanten Organisationen



ITU – International Telecommunication Union
ISO – International Organization for Standardization
IEC – International Electrotechnical Commission
ISA – International Society of Automation
ENISA – European Union Agency for Network and Information Security
ETSI – European Telecommunications Standards Institute
CEN/CENELEC – European Committee for Standardization / European Committee for Electrotechnical Standardization
BSI – Bundesamt für Sicherheit in der Informationstechnik
TeleTrust – Bundesverband IT-Sicherheit e.V.
Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
DKE – Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
VDI – Verein Deutscher Ingenieure e.V.
VDE – Verband der Elektrotechnik und Elektronik
DIN – Deutsches Institut für Normung
VDMA – Verband Deutscher Maschinen- und Anlagenbau e.V.

Quelle: nach BMWi (Hrsg.) (2016 c), S. 30

9.2 Standards und Richtlinien

Generell kann unterschieden werden in ISO/IEC-, DIN EN- und andere Standards. Ein Standard ist nach der International Organization for Standardization (ISO) ein Dokument, das Anforderungen, Spezifikationen, Richtlinien oder Merkmale zur konsequenten Nutzung bereitstellt. Durch international agierende Organisationen wie die ISO werden international gültige Standards geschaffen, die Fortschritt ermöglichen und Lösungswege für globale Herausforderungen unterstützen.

Neben den Standards gibt es auch eine Reihe von Vorschriften und Gesetzen, die im Kontext von IT-Sicherheit Berücksichtigung finden, wie beispielsweise das Bundesdatenschutzgesetz (BDSG) oder das neue IT-Sicherheitsgesetz.

9.2.1 ISO/IEC 2700x

Die Norm ISO/IEC 27001 beschreibt die grundlegenden Anforderungen an das Managementsystem für Informationssicherheit (ISMS) einer Organisation. Weitere Standards aus der ISO/IEC 2700x-Reihe sind Ergänzungen der ISO/IEC 27001. In ISO/IEC 27006 werden beispielsweise Anforderungen an Stellen beschrieben, die ein ISMS auditieren bzw. zertifizieren. Eine solche Zertifizierung von Unternehmen oder Organisationen eignet sich auf globaler Ebene zum Nachweis über die Einhaltung von IT-Sicherheit. Die Zielgruppe der Normenfamilie ist die Unternehmens-IT. Die Reihe der Standards wird kontinuierlich gepflegt und erweitert.

9.2.2 IEC 62443/ISA 99

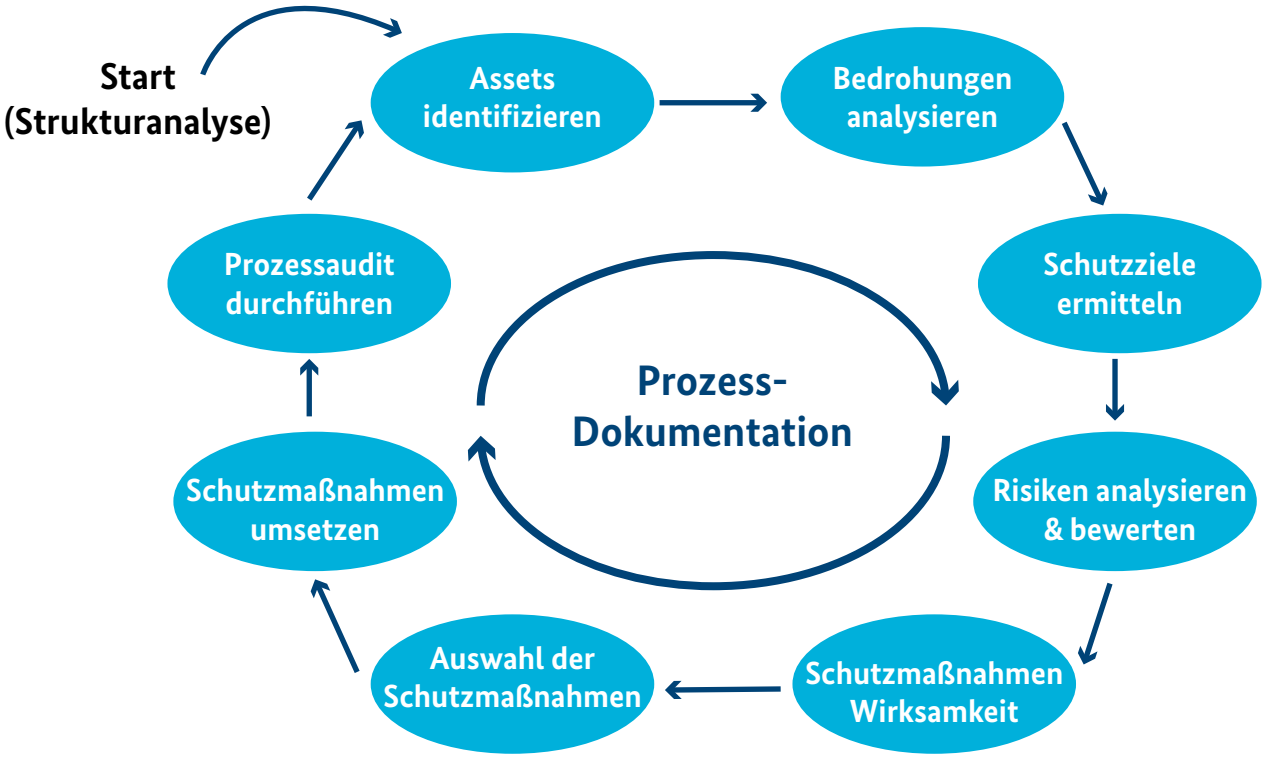
Die IEC 62443 „Industrial Communication Networks – Network and System Security“ ist die internationale Normreihe zur IT-Sicherheit in industriellen Automatisierungssystemen. Diese Normen werden sowohl für das Fachgebiet der Automatisierungstechnik als auch für das der Netzleittechnik und der Leittechnik für weitere kritische Infrastrukturen grundlegenden Charakter haben. Adressiert werden die Zielgruppen Hersteller, Integrator und Betreiber. Aus Sicht der Zielgruppe Betreiber werden die Anforderungen an einen Lieferanten beschrieben und die Anforderungen an ein Security Management System für Industrial Automation and Control Systeme (IACS) definiert, das als ein Profil aus der ISO/IEC 2700x zu sehen ist. Damit wird die enge Verbindung zu der ISO/IEC 2700x deutlich.

9.2.3 VDI/VDE Richtlinie 2182

Die Richtlinie beschreibt Abhängigkeiten zwischen Herstellern von Automatisierungslösungen, Maschinenbauern und System-Integratoren sowie den Betreibern von Fertigungs- und Prozessanlagen. Diese Akteure sind im Industrie 4.0-Kontext Teil eines Wertschöpfungsnetzwerkes, das es unter den Gesichtspunkten der IT-Sicherheit zu bewerten gilt. Die Richtlinie verfolgt einen risikobasierten Ansatz, der die Automatisierungslösung zunächst als Betrachtungsgegenstand bezeichnet. Dieser Betrachtungsgegenstand ist im Fokus bei der Anwendung des Vorgehensmodells der VDI/VDE 2182. Der Betrachtungsgegenstand durchläuft verschiedene Lebenszyklusphasen (Herstellung, Integration, Betrieb). Hier muss beachtet werden, dass eine Lebenszyklusphase nicht zwangsweise auf eine einzelne Organisation beschränkt ist. So ist allgemein bekannt, dass der Hersteller der Automatisierungslösung das Produkt nicht nur entwickelt, sondern auch fertigt. Somit schlüpft der Hersteller oft auch in die Rolle eines Betreibers. Im Rahmen von Industrie 4.0 können diese Lebenszyklusphasen durch eine Vielzahl von Organisationen abgebildet werden, die in Wertschöpfungsnetzwerken verbunden sind.

Die im Blatt 1 der Richtlinie definierte Methodik kann auf bereits existierende und auf in Entstehung befindliche Automatisierungslösungen angewendet werden. Das darin beschriebene Vorgehensmodell basiert auf einem prozessorientierten und zyklischen Ansatz. Das Modell besteht dabei aus mehreren Prozessschritten.

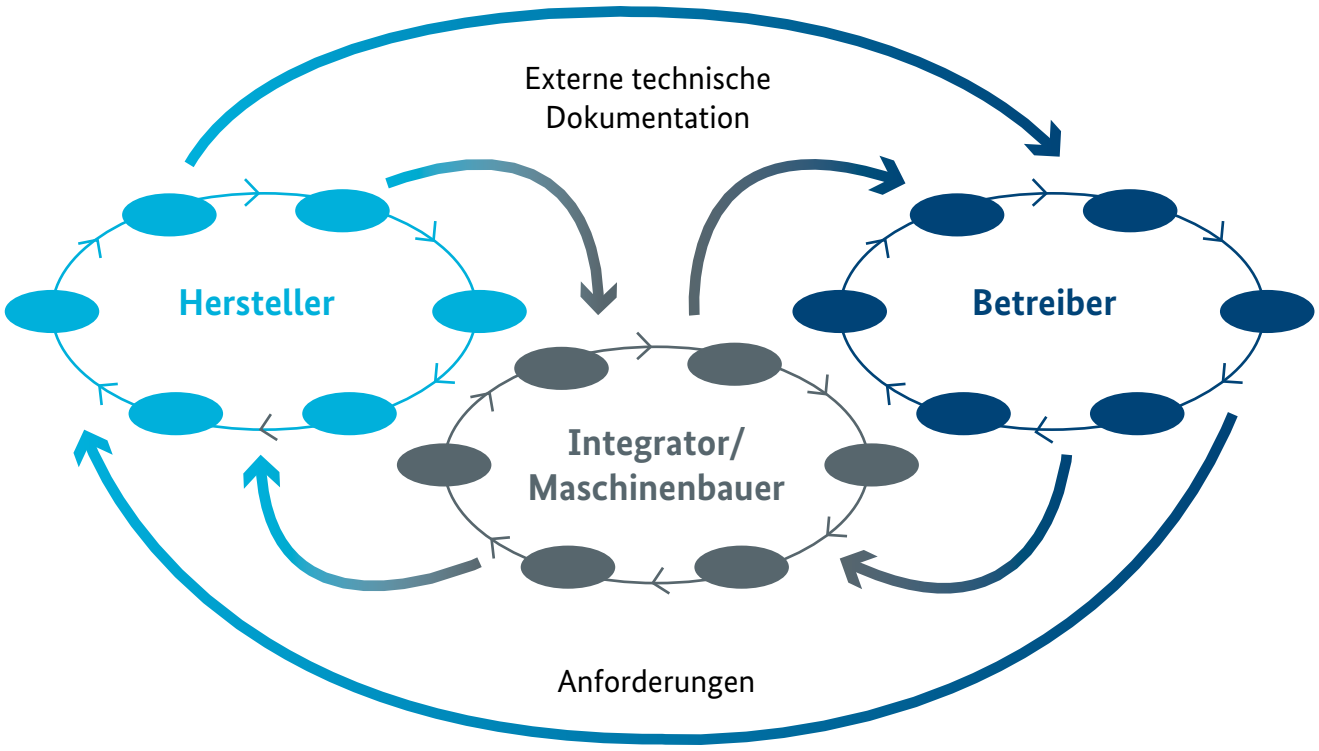
Abbildung 12: Abhängigkeiten im Sicherheitsprozess[47]



Quelle: nach VDI/VDE 2182

47 Vgl. VDI/VDE Richtlinie 2182-1

Abbildung 13: Vorgehensmodell für Interaktion Hersteller, Betreiber, Integrator[48]



Quelle: nach VDI/VDE 2182

Der gesamte Prozess selbst muss zu bestimmten Zeiten (zeitlich und/oder ereignisgesteuert) durchlaufen werden, um die Informationssicherheit des Betrachtungsgegenstandes über dessen gesamten Produkt- bzw. Anlagen-Lebenszyklus sicherzustellen.

Im Fokus im Rahmen der Risikoanalyse ist der Betrachtungsgegenstand, dessen spezifische beziehungsweise typische Einsatzumgebung im Rahmen einer Strukturanalyse zunächst definiert werden muss. Die Strukturanalyse bildet demnach die Grundlage für eine Abarbeitung der einzelnen Prozessschritte. Weitere Grundlage bildet die Definition der Anlässe, bei welchem Ereignis respektive nach welchen Zeitabschnitten der Prozess zu starten ist. Hiermit wird klar, dass der Prozess auf einem zyklischen, iterativen Modell beruht. Eine weitere essenzielle Grundlage bildet die Definition der Rollen, also derjenigen Personen, die in den jeweiligen Prozessschritten aktiv beteiligt sind und dabei eine bestimmte Aufgabe (unter anderem Verantwortlichkeit) übernehmen müssen.

Die Ergebnisse wie auch der Entscheidungsweg eines jeden Prozessschrittes müssen dokumentiert werden. Am Ende steht eine Prozessdokumentation zur Verfügung, die Nachvollziehbarkeit gewährleistet und letztlich Grundlage für eine Auditierung bildet.

Der beschriebene Prozess unterstützt den Anwender der Methodik bei der Bestimmung und Validierung einer angemessenen und wirtschaftlichen Sicherheitslösung für einen konkreten Betrachtungsgegenstand.

Die Richtlinie wird vom VDI/VDE-GMA Fachausschuss 5.22 betreut.

9.2.4 BSI IT-Grundschutz

Mit dem IT-Grundschutz stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine umfangreiche Bibliothek von Standards zur Informationssicherheit und ergänzender praxisnaher Dokumente zur Verfügung. Bis 2005 hieß die BSI-Publikation „IT-Grundschutzhandbuch“, die dann aktualisiert und umstrukturiert worden ist und in diesem Zuge „umbenannt“ wurde in BSI-Standards zur Informationssicherheit und IT-Grundschutz-Kataloge.

IT-Grundschutz-Kataloge untergliedern sich in Bausteine, Gefährdungskataloge und Maßnahmenkataloge. Die Bausteine umfassen u. a. Komponenten, Vorgehensweisen und IT-Systeme im Schichtenmodell und sind das Bindeglied zwischen Gefährdungs- und Maßnahmenkatalogen.

48 Vgl. VDI/VDE Richtlinie 2182-1

Der IT-Grundschutz interpretiert die sehr allgemein gehaltenen Anforderungen der ISO-Standards der 2700x-Reihe und hilft den Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrundinformationen und Beispielen. Zudem ist der IT-Grundschutz kompatibel mit der ISO 2700x-Reihe, sodass eine Zertifizierung nach ISO 2700x auf Basis des IT-Grundschutzeses möglich ist. Ein weiterer Vorteil des BSI IT-Grundschutzes ist die freie Verfügbarkeit der Informationen im Internet. Alle Dokumente sind in Deutsch verfügbar. Derzeit wird an einer Erweiterung für die Anforderungen in der Produktion gearbeitet, diese Entwürfe lagen den Verfassern jedoch zum Zeitpunkt der Erstellung des Leitfadens noch nicht vor.

Nachfolgend eine Übersicht der BSI-Standards zur Informationssicherheit:

100-1: Managementsysteme für Informationssicherheit (ISMS)

Dieser BSI-Standard beschreibt die grundlegenden Anforderungen an ein ISMS. Darüber hinaus wird dargestellt, welche Komponenten es enthält und welche Aufgaben bewältigt werden müssen. Die Darstellung berücksichtigt hierbei u. a. Vorgaben der Norm ISO 27001.

100-2: Vorgehensweise nach IT-Grundschutz

Im BSI-Standard 100-2 wird dargestellt, wie der BSI-Standard 100-1 praktisch umgesetzt werden kann (vgl. BSI (Hrsg.) (2008b)).

100-3: Risikoanalyse auf der Basis von IT-Grundschutz

Dieser BSI-Standard stellt ein vereinfachtes Verfahren zur Risikoanalyse bereit. Damit soll ein erhöhter Schutzbedarf geeignet berücksichtigt werden. Die Risikoanalyse ist gemäß Standard immer dann sinnvoll, wenn Komponenten alleine durch IT-Grundschutz-Maßnahmen nicht adäquat abgesichert werden können (vgl. BSI (Hrsg.) (2008c)).

100-4: Notfallmanagement

Der Standard zum Notfallmanagement zeigt einen systematischen Weg für den Aufbau, die Überprüfung und die Weiterentwicklung eines Notfallmanagements auf. Die zugrunde gelegten Konzepte sollen die Widerstandsfähigkeit der eigenen Institution erhöhen und die Kontinuität der Kerngeschäftsprozesse und Fachaufgaben bei Krisen und Notfällen sichern (vgl. BSI (Hrsg.) (2008d)).

9.3 Weitere Leitfäden und Veröffentlichungen der Plattform Industrie 4.0

Wie bereits im Rahmen des Rollenmodells nach IEC 62443/ISA 99 erwähnt wurde, verschwimmen die Rollen und Verantwortlichkeiten der relevanten Akteure. Ebenso wird auch die ursprüngliche Trennschärfe von Interessenverbänden und Standardisierungsorganisationen immer stärker aufgehoben. In den Veröffentlichungen von Organisationen sind typischerweise die relevanten Zielgruppen benannt, damit das Dokument entsprechend zielgerichtet adressiert werden kann. Dennoch ist es durchaus sinnvoll, sich mit Dokumenten auseinanderzusetzen, die über die eigene Zielgruppe hinausgehen. Zur vereinfachten Übersicht sind nachfolgend einige Leitfäden aufgeführt, denen ein ähnlicher Charakter wie dem vorliegenden Dokument zugrunde liegt und die sich an verschiedene Zielgruppen richten.

Leitfaden Industrie 4.0 Security – Handlungsempfehlungen für den Mittelstand

Zielgruppe: Hersteller von Maschinen und Anlagen
Autor: VDMA, accessec GmbH & Fraunhofer AISEC
Herausgeber: VDMA
Status: Veröffentlicht[49]

ZVEI Security-Orientierungsleitfaden für Hersteller (vorläufiger Arbeitstitel)

Zielgruppe: Hersteller aus der Elektroindustrie
Autor: ZVEI und Koramis GmbH
Herausgeber: ZVEI
Status: In Erarbeitung

Leitfaden Security für den Maschinen- und Anlagenbau. Der Weg durch die IEC 62443

Zielgruppe: Hersteller von Maschinen und Anlagen
Autor: Arbeitskreis Industrial Security beim VDMA und HiSolutions AG
Herausgeber: VDMA
Status: Veröffentlichung im November 2016 geplant

Weiterhin soll an dieser Stelle darauf verwiesen werden, dass die Plattform Industrie 4.0 neben diesem Leitfaden weitere Veröffentlichungen und Partnerveröffentlichungen zu den Themen Industrie 4.0 und IT-Sicherheit zur freien Verfügung stellt. Die Veröffentlichungen sind über die Online-Bibliothek zugänglich[50] und in deutscher sowie teilweise in englischer Sprache verfügbar.

49 Vgl. VDMA Verlag (o. J.)

50 http://www.plattform-i40.de/I40/Navigation/DE/In-der-Praxis/Online-Bibliothek/online-bibliothek.html

10 Abbildungsverzeichnis

11 Literatur- und Quellenverzeichnis

bitkom (Hrsg.) (2014): „Leitfaden: Kompass der IT-Sicherheitsstandards“
URL: https://www.bitkom.org/Bitkom/Publikationen/Kompass-der-IT-Sicherheitsstandards.html, letzter Zugriff: 19.10.2016

BMWi (Hrsg.) (2016a): „Technischer Überblick: Sichere unternehmensübergreifende Kommunikation“, Ergebnispapier der Plattform Industrie 4.0, URL: https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-unternehmensuebergreifende-kommunikation.pdf?__blob=publicationFile&v=8, letzter Zugriff: 19.10.2016

BMWi (Hrsg.) (2016b): „Technischer Überblick: Sichere Identitäten“, URL: https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-identitaeten.pdf?__blob=publicationFile&v=8, letzter Zugriff: 19.10.2016

BMWi (Hrsg.) (2016c): „Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie: IT-Sicherheit für die Industrie 4.0“, URL: http://www.bmwi.de/DE/Mediathek/publikationen,did=764200.html, letzter Zugriff: 19.10.2016

BMWi (Hrsg.) (2016d): „Plattform Industrie 4.0 – Online-Bibliothek“, URL: http://www.plattform-i40.de/I40/Navigation/DE/In-der-Praxis/Online-Bibliothek/online-bibliothek.html, letzter Zugriff: 19.10.2016

BSI (Hrsg.) (2008a): „BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)“,
URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1001.pdf?__blob=publicationFile, letzter Zugriff: 19.10.2016

BSI (Hrsg.) (2008b): „BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile, letzter Zugriff: 19.10.2016

BSI (Hrsg.) (2008c): „BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1003.pdf?__blob=publicationFile, letzter Zugriff: 19.10.2016

BSI (Hrsg.) (2008d): „BSI-Standard 100-4: Notfallmanagement“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile, letzter Zugriff: 19.10.2016

BSI (Hrsg.) (2012): „Technical Guideline TR-03111: Elliptic Curve Cryptography“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.pdf;jsessionid=3D1A9885F1F664C54D120C3633467099.2_cid368?__blob=publicationFile&v=1, letzter Zugriff: 19.10.2016

BSI (Hrsg.) (2015): „BSI – Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“,
URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=2, letzter Zugriff: 19.10.2016

Bundesnetzagentur (2015): „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)“, Entwurf, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf.pdf?__blob=publicationFile, letzter Zugriff: 19.10.2016

Kobes, P. (2015): „Defense-in-Depth: Grundlage für eine erfolgreiche Verteidigungsstrategie gegen Cyberangriffe“,
URL: http://www.elektrotechnik.vogel.de/defense-in-depth-grundlage-fuer-eine-erfolgreiche-verteidigungsstrategie-gegen-cyberangriffe-a-473371/, letzter Zugriff: 19.10.2016

Kobes, P. (2016): „Leitfaden Industrial Security, IEC 62443 einfach erklärt“, URL: https://www.vde-verlag.de/buecher/484165/leitfaden-industrial-security.html, letzter Zugriff: 21.09.2016

Microsoft (Hrsg.) (2016): „Security Development Lifecycle“, URL: https://www.microsoft.com/en-us/SDL, letzter Zugriff: 19.10.2016

NIST (Hrsg.) (2014): „Cryptographic Toolkit“, URL: http://csrc.nist.gov/groups/ST/toolkit/, letzter Zugriff: 19.10.2016

Siemens AG (Hrsg.) (2010): „Device Manager für SIMATIC LOGON“, URL: http://www.industry.siemens.com/datapool/industry/industrysolutions/services/de/Device-Manager-SIMATIC-LOGON-de.pdf, letzter Zugriff: 19.10.2016

TeleTrust (Hrsg.) (2014): „TeleTrusT-Handreichung: Stand der Technik“, URL: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/, letzter Zugriff: 19.10.2016

VDE (Hrsg.) (2016): „Arbeitsgruppen und Gremien im Bereich Industrie 4.0“, URL: https://www.dke.de/de/themen-projekte/excellencecluster-industrie-4-0/arbeitsgruppen-und-gremien-im-bereich-industrie-4-0, letzter Zugriff: 19.10.2016

VDI/VDE Richtlinie 2182-1: „Informationssicherheit in der industriellen Automatisierung – Allgemeines Vorgehensmodell“, Weißdruck 2011

VDMA Verlag (o. J.): „Leitfaden Industrie 4.0 Security“, URL: http://leitfaden-i40-security.vdma-verlag.de/, letzter Zugriff: 19.10.2016

ZVEI (Hrsg.) (2015): „Industrie 4.0: Die Industrie 4.0-Komponente“, URL: http://www.zvei.org/Downloads/Automation/Industrie%204.0_Komponente_Download.pdf, letzter Zugriff: 19.10.2016

12 Abkürzungsverzeichnis

ABAC – Attribute Based Access Control

API – Application Programming Interface

ASE – Automation Security Engineer

ASLR – Address Space Layout Randomization

ASO – Automation Security Officer

BYOD – Bring Your Own Device

CBAC – Context Based Access Control

CI – Configuration Item

CLM – Certificate Lifecycle Management

CMDB – Configuration Management Database

CSMS – Cyber Security Management System

DAC – Discretionary Access Control

DDoS – Distributed Denial of Service

DEP – Data Execution Prevention

ERP – Enterprise-Resource-Planning

I4.0 – Industrie 4.0

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

ISMS –Managementsystem für Informationssicherheit

ITIL – IT Infrastructure Library

MAC - Mandatory Access Control

M2M – Machine to Machine

MES – Manufacturing Execution System

OCSP – Online Certificate Status Protocol

PKI – Public Key Infrastructure

PSO – Production Security Officer

RBAC – Role-based Access Control

SDL – Security Development Lifecycle

SIEM – Security Information and Event Management

SPS – Speicherprogrammierbare Steuerung

SSO – Single Sign-On

UAC – User Account Control

VPN – Virtuelles Privates Netzwerk

AUTOREN:

Heiko Adamczyk, KORAMIS GmbH | Carsten Angeli, KUKA Roboter GmbH | Konstantin Böttinger, Fraunhofer AISEC | Bartol Filipovic, Fraunhofer AISEC | Wolfgang Fritsche, IABG | Dr. Detlef Houdeau, Infineon Technologies AG | Dr. Martin Hutle, Fraunhofer AISEC | Dr. Lutz Jänicke, Phoenix Contact GmbH & Co. KG | Michael Jochem, Robert Bosch GmbH | Marcel Kisch, IBM Deutschland GmbH | Dr. Wolfgang Klasen, Siemens AG | Dr. Bernd Kosch, Fujitsu Technology Solutions GmbH | Michael Krammel, KORAMIS GmbH | Lukas Linke, ZVEI e.V. | Torsten Nitschke, Phoenix Contact Software GmbH | Sebastian Rohr, accessec GmbH | Michael Sandner, Volkswagen AG | Dr. Michael Schmitt, SAP SE | Martin Schwibach, BASF SE | Nadine Sinner, accessec GmbH | Andreas Teuscher, Sick AG | Thomas Walloschke, Fujitsu Technology Solutions GmbH | Jürgen Zorenc, accessec GmbH

Diese Publikation ist ein Ergebnis der Arbeitsgruppe „Sicherheit vernetzter Systeme“ der Plattform Industrie 4.0.

www.plattform-i40.de