PLATTFORM INDUSTRIE 4.0

ERGEBNISPAPIER

Industrie 4.0-Security in der Aus- und Weiterbildung

Neue Aspekte für Unternehmensorganisation und Kompetenzen

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
danchooalex – iStock (Titel), Savas Keskiner – iStock (S. 3),
yoh4nn – iStock (S. 4), everythingpossible – Fotolia (S. 6)

Zertifikat seit 2002
audit berufundfamilie

Das Bundesministerium für Wirtschaft und Energie ist mit dem audit berufundfamilie® für seine familienfreundliche Personalpolitik ausgezeichnet worden. Das Zertifikat wird von der berufundfamilie gGmbH, einer Initiative der Gemeinnützigen Hertie-Stiftung, verliehen.

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C108626

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

Inhalt

Präambel

Durch die vernetzte Produktion in der Industrie 4.0 entsteht ein neuer Know-how-Bedarf in allen Unternehmensbereichen, der durch ein passfähiges Personalmanagement gedeckt werden muss. Eine besondere Rolle nehmen hier die Kompetenzen zur Erlangung des Vertrauens der Wertschöpfungspartner und die Sicherung des Regelbetriebs des eigenen Unternehmens durch den Einsatz von organisatorischen und technischen Securitymaßnahmen ein. Gefragt ist dabei übergreifendes Know-how, besonders in den Bereichen Industrial-IT und Security, Systemintegration, Automation und Produktionstechnik. Denken in Systemen und in interdisziplinären Zusammenhängen ist zudem die Voraussetzung, um verantwortliche Entscheidungen treffen zu können.

Mit dem vorliegenden Dokument möchte die AG 3 „Sicherheit vernetzter Systeme“ einen Überblick und Orientierung zu neuen Qualifizierungsanforderungen im Kontext von Industrie 4.0 geben.

Die Anforderungen an die Aus- und Weiterbildung von Beschäftigten im Kontext von Industrie 4.0-Security richten sich an Entscheidungsträger in Politik, Wirtschaft und Wissenschaft und sollen die Handlungsbedarfe und Ansatzpunkte zur Umsetzung aufzeigen. Ziel ist also in erster Linie, zu sensibilisieren und erste konkrete Qualifizierungsinhalte abzuleiten.

Der Fokus liegt auf der Beschreibung notwendiger Kompetenzen über alle Wertschöpfungspartner und Hierarchieebenen hinweg.

Es ist jedoch zu berücksichtigen, dass Security nicht statisch ist. Vielmehr ist es notwendig, Security über den gesamten Betrieb einschließlich der Ablösung der Systeme durch entsprechende technische und organisatorische Maßnahmen aufrechtzuhalten. Daher kann es kein vollständiges und aktuelles Merkblatt geben. Welche Kompetenzen aus heutiger Sicht als Startpunkt notwendig sind, ist Gegenstand dieses Dokuments.

Die umfassende und detaillierte Ableitung von Curricula für einzelne Rollen ist nicht Gegenstand des Dokuments. Hier sind in der Folge die Sozialpartner, die Politik und die Wissenschaft sowie Ausbildungsgremien weiter mit einzubinden.

1 Einleitung

Technologischer Wandel und die zunehmende Digitalisierung und Vernetzung im Produktionsumfeld zu Gunsten einer unternehmensübergreifenden, effizienteren und effektiveren Produktion (Industrie 4.0) stellen die Industrie vor neue sicherheitstechnische und -organisatorische Herausforderungen: Wenn es bisher ausreichte, den Schutz der Kommunikations- und Informationsinfrastruktur an der Unternehmensgrenze im Sinne eines Perimeterschutzes zu etablieren, wird diese Schutzmaßnahme in Zukunft alleine durch die zunehmende Vernetzung, und damit einhergehender Öffnung nach außen, nicht mehr ausreichen.

Um die sichere Zusammenarbeit in unternehmensübergreifenden Wertschöpfungsnetzwerken dennoch zu ermöglichen, wird das berechtigte Vertrauen der Partner ineinander benötigt. Berechtigtes Vertrauen kann bestehen, wenn der Schutz gegen Bedrohungen von außen (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 u. a. die Widerstandsfähigkeit gegen Angriffe zu erhöhen.

Digitale Transformation, neue Geschäftsmodelle und Industrie 4.0 erfordern neue Formen des Denkens, des Arbeitens, der Kooperation und letztendlich der Qualifikation des Personals.

Vor dem Hintergrund der unternehmensübergreifenden Zusammenarbeit wachsen unternehmensintern Produktion und IT zunehmend zusammen, eine Vielzahl an Zugangsmöglichkeiten erhöht die Komplexität und vergrößert die Angriffsfläche und somit auch das Gefährdungspotential. Die Konsequenzen:

Im Zuge der sich stark verändernden Rahmenbedingungen im Produktionsumfeld müssen sowohl die Unternehmensorganisationen als auch die Kommunikationsstrukturen angepasst werden. An der Schnittstelle zwischen Produktion, IT und Security entstehen neue Rollen und Tätigkeitsprofile. Dies schafft neue Anforderungen an Qualifikationen und Ausbildung, die aktuell erst noch aufgebaut werden müssen. Produktionsmitarbeiter/-innen müssen künftig über IT-Kenntnisse verfügen und IT-Mitarbeiter/-innen (zu einem gewissen Grad) über Produktionskenntnisse. Das Personalwesen muss sich dieser Kenntnisanforderungen bereits bei der Akquise zukünftiger

Beschäftigter bewusst sein. Ebenso sollte das Management in der Lage sein, den Stellenwert des Themas Security im Rahmen der Industrie 4.0 einschätzen zu können.

- Diverse Studien weisen auf den Mangel an qualifizierten Mitarbeitern/-innen in diesem Bereich als einem der größten Risikofaktoren bei der Umsetzung von Industrie 4.0-Strategien hin.

- Angriffe nehmen sowohl an Quantität als auch an Qualität zu. Das Thema Sicherheit gewinnt in diesem dynamischen Systemverbund immer mehr an Bedeutung. Die zunehmende Digitalisierung und fast lückenlose Vernetzung der Produktionsschritte führen zu einer Erhöhung des Gefährdungspotentials und der Schadenshöhe. Neben dem anfänglichen Fokus auf den direkten und sichtbaren Produktionsausfall verlagern sich die Gefährdungen durch Angriffe zunehmend auf die schleichende, nicht direkt ersichtliche Beeinträchtigung der Produktion bzw. der Qualität der Produkte, die erst zu einem späten Zeitpunkt ersichtlich werden. Dies kann aufgrund von möglichen Rückrufaktionen und Imageschäden zu einem wesentlich höheren Schaden führen als ein direkt ersichtlicher Stopp der Produktionslinie. Zusätzlich kann das Ausspionieren von Produktionsprozessen die Alleinstellungsmerkmale von Unternehmen gefährden. Die Sicherheitslösungen in der Office-IT sind jedoch nicht „1 zu 1“ auf die Produktions-IT übertragbar. Die produktionsnahe IT kann von den Erfahrungen der Office-IT partizipieren, die umzusetzenden Lösungen müssen jedoch auf Verträglichkeit mit den Rahmenbedingungen der Produktion geprüft und dementsprechend angepasst werden. Hierbei ist darauf hinzuweisen, dass unzureichende Sicherheitsmaßnahmen selbst ein Risiko für die Produktion darstellen können.

Aus- und Weiterbildungsmaßnahmen sind unbedingt erforderlich, um diesen Strukturwandel auf allen Ebenen zu unterstützen. Es muss der Brückenschlag und ein gemeinsames Verständnis für die Parallelwelten von Produktion und IT geschaffen werden, um qualifiziert Entscheidungen treffen zu können. Dieser Brückenschlag ist erforderlich, um die Akzeptanz für die neuen Arbeitswelten zu erhöhen, das Personal für zukünftige Aufgaben und Rollen zu qualifizieren und die Kommunikation im Unternehmen sowie die Zusammenarbeit von Unternehmensbereichen kulturell und organisatorisch zu verbessern.

Zusammenfassend ergeben sich folgende Kernthesen:

Security ist Grundlage für Vertrauen und betrifft den gesamten Lebenszyklus!

Auf einer hohen Abstraktionsebene umfasst der Lebenszyklus von Produkten, Prozessen und Projekten die Phasen Planung, Umsetzung und Betrieb. Wobei die Planung sowohl alle Prozesse von der Bedarfsentstehung bis hin zur Bestellung oder ggf. der Entwicklung eines Produktes als auch der Planung des Betriebes bspw. im Sinne der Ressourcen- und Kapazitätsplanung umfasst. Jede dieser Phasen muss sicher gestaltet werden, damit das notwendige Vertrauen zwischen den Wertschöpfungspartnern zunächst entstehen und später überprüft werden kann. Security ist integraler Bestandteil von Industrie 4.0 und hat die Funktion eines Enablers für das professionelle und sichere Arbeiten in der digitalen Welt.

Security geht alle an – Relevanz für Management und Beschäftigte!

Die Beherrschung des von Zielgruppenbedarf und Rollen abhängigen Security-Know-hows ist als wichtiger Bestandteil von Industrie 4.0 zu bewerten: Insbesondere muss sich das Management von Unternehmen – Geschäftsführung und Vorstände – der Tragweite und der unternehmerischen Relevanz der Einführung von Industrie 4.0-Prozessen bewusst werden. Sie haben die Aufgabe, Beschäftigte zu motivieren und die notwendige Akzeptanz zu schaffen. Dazu werden Mitarbeiter/-innen benötigt, die in der Lage sind, die in den Lebenszyklusphasen relevanten Security-Aspekte zu verstehen und anzuwenden. Die Awareness aller Beschäftigter für mögliche Bedrohungen ist zu schärfen, da das richtige Verhalten hier die Grundlage ist für weitergehende Aufgaben wie die Definition der Security in der Planungsphase, die Prüfung der Securityeigenschaften bei der Abnahme in der Umsetzungsphase oder die Aufrechterhaltung, die über die Betriebsphase hinweg zu entwickeln ist. Jeder Beschäftigte muss in seiner Funktion und seiner Rolle seinen Beitrag zur Security leisten und dazu notwendige Qualifikationen erwerben können.

Security ermöglicht Wettbewerbsvorteile!

Zur Erreichung eines optimierten & stabilen Betriebes im Sinne des Industrial Continuity Management bedarf es ausreichend abgesicherter Produktions-Rahmenbedingungen. Was passiert, wenn Angriffe auf die Produktion erfolgreich durchgeführt werden, zeigen eindrucksvoll Medienberichte der jüngeren Vergangenheit: Totalausfall von Produktionsstätten, Produktion mit falschen Fertigungsparametern, der Verlust von Prozesswissen oder die „Geiselnahme“ von Unternehmensdaten sind nur einige plakative Beispiele.

Security/Vertrauen ist eine der Voraussetzungen für die unternehmensübergreifende Zusammenarbeit in einer Industrie 4.0, in der bisher meist intern gehaltene Informationen zu Gunsten einer zukünftig flexibleren und effizienteren Produktion über Unternehmensgrenzen hinweg ausgetauscht werden. Zudem fordern zunehmend regulatorische und gesetzliche Vorgaben die Anwendung und Umsetzung von Sicherheitsmaßnahmen. Ein Beispiel ist das IT-Sicherheitsgesetz oder die derzeitige Fortschreibung der ISO/IEC 27000-Reihe, sowie die IEC 62443.

Das Angebot passfähiger Securityeigenschaften eines Produktes wird zukünftig Hersteller in die Lage versetzen, Mehrwerte für ihre Kunden zu generieren, Differenzierungspotential gegenüber dem Wettbewerb zu bieten sowie eine Sicherstellung der eigenen Anforderungslieferkette zum Kunden zu gewährleisten.

Die Investition in Aus- und Weiterbildung der Beschäftigten zum Know-how-Aufbau in Security wird sich somit schnell rechnen.

Security benötigt einen festen Platz in der Unternehmensorganisation!

Produktions-IT und Office-IT wachsen zunehmend zusammen. Vor diesem Hintergrund ist es notwendig, dass die Unternehmensorganisationen dieser Entwicklung Rechnung tragen und eine Rolle/Funktion mit entsprechendem Überblickswissen, -kompetenz und -verantwortung vorsieht. Nur wenn es eine verantwortliche Rolle im Sinne eines „Kümmerers“ gibt, der sowohl Produktions-, IT- als auch Securitykompetenzen einbringt und die Wechselwirkungen sowie Konsequenzen von Bedrohung, Risiko und Maßnahme bewerten kann, werden Unternehmen dazu befähigt, Security erfolgreich im Industrie 4.0-Prozess umzusetzen.

2 Zukunftsszenario – Rolle der IT-Sicherheit für die zukünftige Produktion

In den vorliegenden Beschreibungen der Securityanforderungen an Beschäftigte im Kontext Industrie 4.0 wird davon ausgegangen, dass in der fortgeschrittenen Industrie 4.0 der Kundenwunsch die gesamte Wertschöpfungskette bestimmt:

Der (End-)Kunde formuliert, eventuell mit Unterstützung durch einen Dienstleister, seinen Produkt- bzw. Dienstleistungswunsch, woraufhin, individuell und von wirtschaftlichen Restriktionen abhängig, ad hoc die notwendigen Kompetenzen und Kapazitäten in Wertschöpfungsnetzwerken unternehmensübergreifend zusammengeführt werden (Abbildung 1, rechter Teil „Auftragsgesteuerte Produktion“).

Diese vernetzte Produktion macht den Datenaustausch über Unternehmensgrenzen hinweg bspw. zu Produktionsfortschritten, Qualitätsdaten und Beständen notwendig, wie er heute nur unternehmensintern üblich ist. Dies erfordert von den Teilnehmern dieser Wertschöpfungsnetzwerke Vertrauen in die Wertschöpfungspartner hinsichtlich der Einhaltung der VIV- und Privacy-Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit und datenschutzkonformer Umgang mit den bereitgestellten Informationen), aber auch hinsichtlich der Leistungsfähigkeit, da die mit dem Kunden vereinbarte Leistung regelmäßig außerhalb der eigenen Einflussmöglichkeiten liegen wird: Liefert ein Partner nicht, scheitert das gesamte Netzwerk.

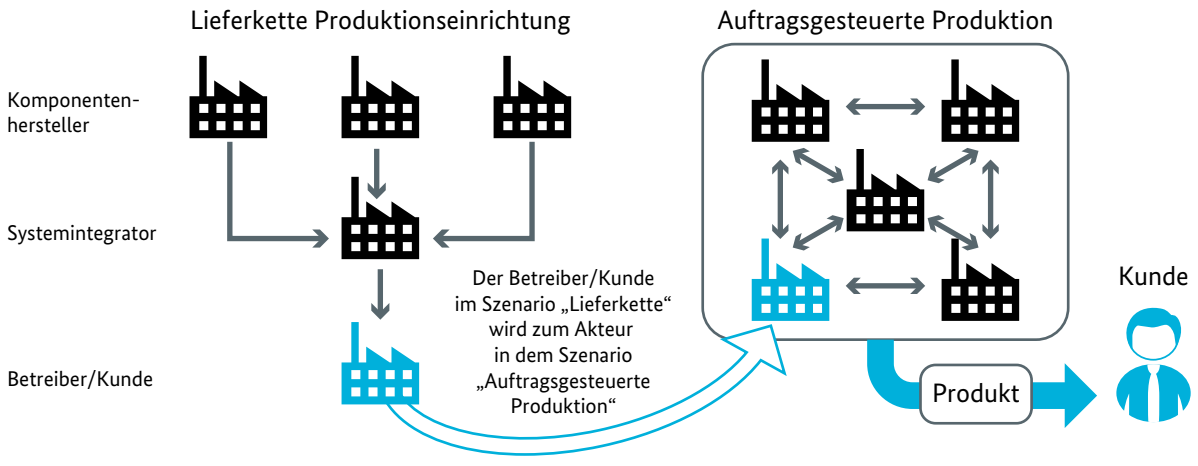
Um dieses Vertrauen zu schaffen, ist es notwendig, Maschinen und Anlagen einzusetzen, die den Securityanforderungen entsprechende Sicherheitstechniken und Konzepte bspw. zur sicheren Kommunikation und deren Überprüfbarkeit verwenden (vgl. Abbildung 1, linker Teil „Lieferkette neue Produktionseinrichtung“).

Bei der Beschreibung von Anforderungen an Maschinen, Anlagen oder Produkte werden grundsätzlich **funktionale und nicht-funktionale Anforderungen** unterschieden. Funktionale Anforderungen beschreiben, was das System oder das Produkt leisten soll (Drehen, Fräsen etc.), während nicht-funktionale Anforderungen die „Qualität“ der zu erbringenden Leistung beschreiben.

Aktuell werden jedoch die Securityeigenschaften als Teil der nicht-funktionalen Anforderungen nicht oder meist nur unzureichend von den Betreibern der Maschinen und Anlagen im Rahmen der Beschaffung gefordert. Im Vergleich zu den funktionalen Eigenschaften nehmen sie häufig eine zu geringe Relevanz bei der Bewertung von Angebotsalternativen ein, da bisher der Schutz gegen Angriffe oder Informationsabfluss, insbesondere auf Maschinen- und Anlagenebene, nicht in das Bewusstsein der Betreiber gerückt ist. Eine reine Absicherung nur auf höheren Schichten der Automatisierungspyramide im Rahmen des Perimeterschutzes vorzunehmen, fällt vor dem Hintergrund der beschriebenen Entwicklungen zusehends weg.

Die Bereitstellung der Maschinen und Anlagen erfolgt durch Integratoren, die Komponenten von Herstellern zusammenführen, um den gewünschten Funktionsumfang zu gewährleisten. Nicht-funktionale Securityeigenschaften werden nicht oder nur rudimentär angeboten.

Abbildung 1: Industrie 4.0 wird kundenspezifische Produkte in Losgröße 1 ermöglichen



Bei den Herstellern von Komponenten ist Ähnliches zu beobachten. Sie konzentrieren sich oft noch auf die geforderten Funktionen, während die nicht-funktionalen Securityeigenschaften wenig berücksichtigt werden. Aus der IT – und dies ist auf die Produktion übertragbar – wissen wir: Security wird nicht mit funktionalen Eigenschaften (also dem Sicherheitsprodukt und seinen Funktionen) alleine erreicht. Vielmehr das Gegenteil ist der Fall: Beschränkt sich ein Unternehmen nur auf die reine Investition in Security-Technologie, wird diese ab dem Zeitpunkt der Anschaffung schnell an Wirksamkeit verlieren.

Das Sicherheitsniveau wird am Ende durch das bestmögliche Zusammenwirken aller Beteiligten bestimmt. Internationale Standards, wie die zukünftig auch zertifizierbare IEC 62443, zielen genau darauf ab, mit Betrachtung der Rolle im Wertschöpfungsprozess jedem Partner seine zu erfüllenden Securityaufgaben zu definieren und die Übergänge vom Hersteller, Integrator und Betreiber auf Basis von Sicherheitslevels im Sinne eines Security-by-Design-Prozesses sicherzustellen.

Security ist Qualitätsmerkmal und Voraussetzung für die Kooperation zwischen Unternehmen – Wie kann sie gefördert werden?

Es ist in vielen Fällen zu beobachten, dass das größte Bewusstsein, wenn auch immer noch gering ausgeprägt, für die Notwendigkeit von Securityeigenschaften von Maschinen und Anlagen bei den Betreibern liegt.

Es könnte spekuliert werden, dass diese Interessenverteilung in den unterschiedlichen schützenswerten Gütern (Assets) der Beteiligten begründet ist. Die Frage lautet also, wer sieht welche Eigenschaft, welches Wissen als schützenswertes Gut an?

Das Herausstellungsmerkmal des Betreibers beruht häufig auf den Eigenschaften seines Produktes, die durch Entwicklung und Herstellung ermöglicht werden. Die Eigenschaften des Produktes sind offensichtlich und deren technische Realisierung ist in der Regel durch Schutzrechte geschützt. Die Herstellung der Produkte, also das Prozess-Know-how, ist jedoch in der Regel rechtlich nicht schutzfähig und wird daher geheim gehalten. Ebenso sind für den Betreiber die Qualität der produzierten Güter, die Produktivität oder Verfügbarkeit seiner Maschinen und Anlagen sowie alle Daten, die Rückschlüsse auf sein Geschäft erlauben, schützenswert.

Bei den Integratoren liegt das Know-how in der Verbindung von Komponenten mehrerer Hersteller. In vielen Fällen kommen auch eigene Komponenten hinzu. Vor diesem Hintergrund stellen bspw. die programmierten Schnittstellen, das Auslesen und die Verarbeitung der Sensorsignale und die Ansteuerung der Aktoren das Schützenswerte gut dar, da so die Fertigung in den garantierten Toleranzbereichen ermöglicht wird. Gleiches gilt für den Komponentenhersteller, der eventuell Merkmale seiner Komponente wie Regelparameter als schützenswert ansieht.

Jeder der Beteiligten ist nur bereit, Schutztechniken zu bezahlen, die seinen Schutzzielen entgegenkommen. Gemeinsames Interesse entwickeln die Geschäftspartner nur in den Punkten, in denen die Einhaltung der Anforderungen des einen vertraglich mit dem anderen vereinbart wird. Dies ist in der Regel bei den funktionalen Eigenschaften der Maschine oder Anlage der Fall: Der Betreiber der Anlage gibt die Toleranzbereiche bspw. für Drücke und Temperaturen vor und überprüft im Zuge der Abnahme deren Einhaltung. Werden die vereinbarten Randbedingungen nicht eingehalten oder kommt es im Gewährleistungszeitraum zu Abweichungen, kann die Abnahme verweigert oder die Nachbesserung verlangt werden. Der Integrator muss also investieren, um dem Betreiber ein den Vereinbarungen entsprechendes Produkt zur Verfügung stellen zu können, da ansonsten Verluste drohen. Diese Investitionen können sich auf sämtliche unternehmerische Bereiche beziehen. Dazu zählen insbesondere die notwendigen Kompetenzen der Mitarbeiter/-innen sowie die Fertigungskompetenzen und -kapazitäten. Wobei Letztere in der zukünftigen Industrie dynamisch durch die Bildung von Wertschöpfungsnetzwerken angepasst werden können (vgl. oben).

Vor diesem Hintergrund ist es notwendig, dass der Betreiber einer Maschine oder Anlage die Einhaltung seiner Schutzziele von den Integratoren einer neu zu beschaffenden Produktionseinrichtung verlangt, sie also in seinen Anforderungskatalog aufnimmt und in der Lage ist, die Einhaltung seiner Anforderungen zu prüfen und zu überwachen. Gleiches gilt für den Integrator im Beschaffungsprozess der Komponenten von den Herstellern. Darüber hinaus benötigt der Integrator die Kompetenzen, die Securityanforderungen des Betreibers in technische Lösungen zu transferieren, um die Securityeigenschaften der Produktionseinrichtung gewährleisten zu können.

3 Kompetenzen – Relevanz für Management & Beschäftigte

Welche Kompetenzen werden benötigt?

Eine zentrale Voraussetzung für eine erfolgreiche Einführung von Industrie 4.0 auf Basis eines berechtigten Vertrauens zwischen den Wertschöpfungspartnern stellen das Wissen und die Kompetenzen der Mitarbeiter/-innen dar. Die oberste Managementebene ist bei dieser Einführung von entscheidender Bedeutung. In ihrer Funktion als Unternehmenslenker müssen sie die Rahmenbedingungen für eine organisatorische und strukturelle Personalentwicklung schaffen. Wichtig dabei ist, dass die gesamte Belegschaft bei der Kompetenzentwicklung und Wissensvermittlung einbezogen wird.

Über die Planung, die Umsetzung und den Betrieb des Produktes hinweg tragen alle Mitarbeiter/-innen mit ihren Kompetenzen zur, im Securitysinne, sicheren Verwendung des Produktes bei. Das heißt: Security betrifft alle an der Wertschöpfung beteiligten Akteure.

Dazu erstellt z. B. die Produktion die funktionalen und nicht-funktionalen Anforderungen für neue Maschinen und Anlagen, gibt diese an den Einkauf weiter, und der Einkauf fordert vom Integrator das entsprechende Pflichten- und/oder Lastenheft ein. Dementsprechend sollte eine Interpretationskompetenz bspw. der relevanten Richtlinien auf der Bedarfsseite vorliegen, während auf der Angebotsseite die Kompetenz vorliegen muss, die Anforderungen des Kunden in Komponenten abzubilden. Dementsprechend können die notwendigen Kompetenzen zu den drei Kompetenzclustern Planungs-, Umsetzungs- und Betriebskompetenzen zusammengefasst werden, in denen die Akteure der Lieferketten und Wertschöpfungsnetzwerke Kompetenzen aufbauen und pflegen müssen, um das notwendige Vertrauen für eine unternehmensübergreifende Zusammenarbeit zu ermöglichen.

Grundlage für die Industrie 4.0 ist also eine durchgängige Kompetenzkette der beteiligten Akteure, durch die es möglich ist (vgl. Abbildung 2),

- in der Planungsphase die Anforderungen an die funktionalen und nicht-funktionalen Eigenschaften eines Produktes zu definieren (vgl. Abschnitt 2),
- die Anforderungen in technische Lösungen zu überführen und passende organisatorischen Maßnahmen zu planen,
- in der Umsetzungsphase die zugesicherten Eigenschaften der technischen Einrichtung bei der Abnahme des Produktes (Kundensicht) bzw. der Komponente (Integratorensicht) zu prüfen,
- die bereitgestellte technische Einrichtung in die vorhandene Infrastruktur und Organisation (Kundensicht) oder das entstehende System (Integratorensicht) unter Beibehaltung bzw. zur Erlangung des beabsichtigten Schutzniveaus zu integrieren,
- in der Betriebsphase die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Aufrechterhaltung des beabsichtigten Schutzniveaus für die Dauer des Betriebes, einschließlich der Ablösung, zu gewährleisten, und
- Kommunikationsschnittstellen zu definieren, damit potentielle Sicherheitsbrüche zeitnahe erkannt und Gegenmaßnahmen unten den beteiligten Unternehmen abgestimmt werden können.

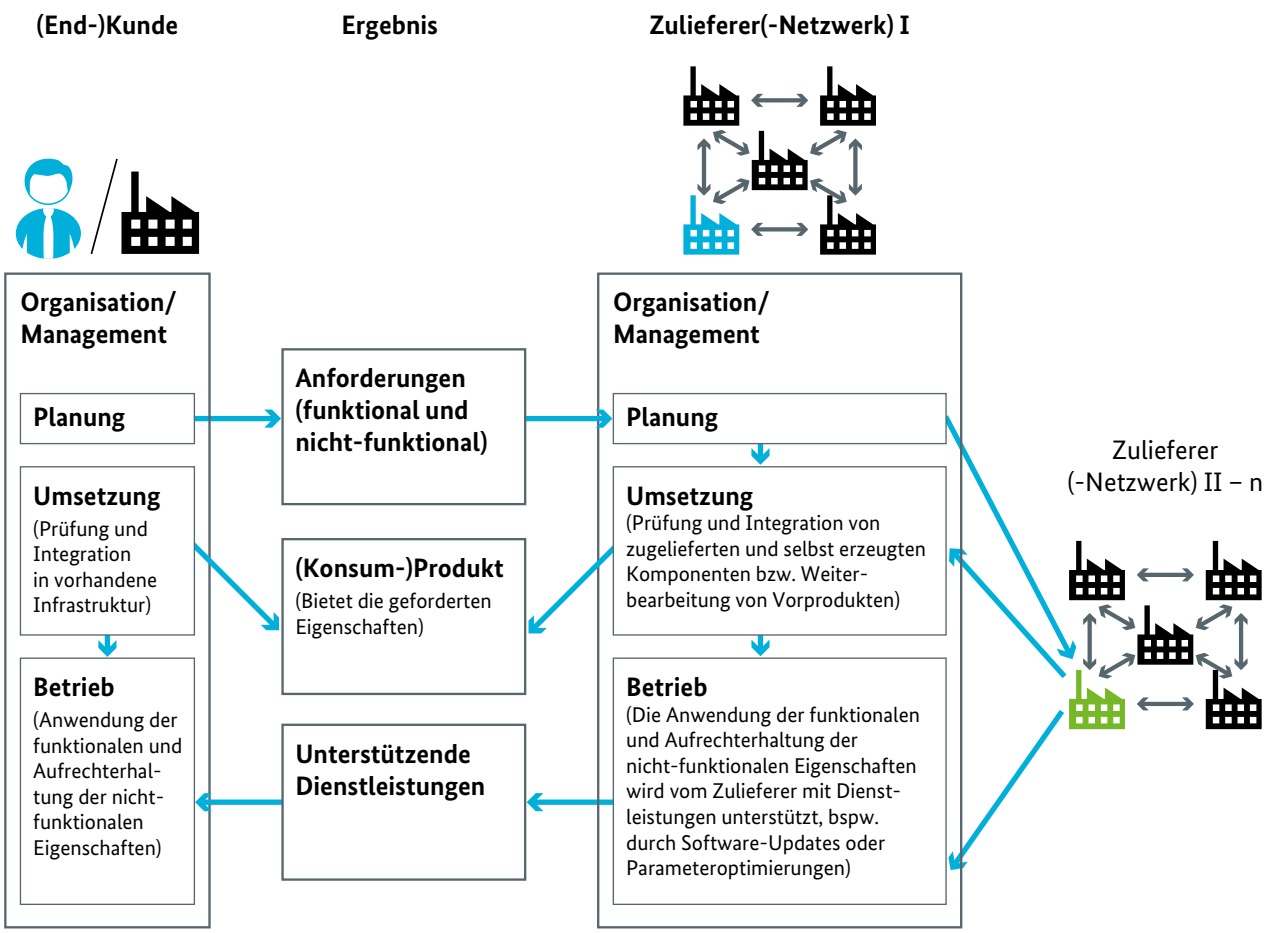
Wichtig ist, dass die Kompetenzen für die durchzuführenden Aufgaben auf jeder Lieferstufe vorhanden sind; ihre Lokalisation in der Lieferbeziehung ist nachrangig – die Kompetenzen können sogar durch externe Dienstleister ergänzt werden.

Grundlage ist eine Organisation, in der das Management, neben den typischen Zielen wie Verfügbarkeit und Qualität, Securityziele verfolgt und dieses Ziel mit allen Hierarchieebenen umsetzt, da erkannt wurde, dass eine nicht oder nicht ausreichend vorhandene Security dazu führt, dass an zukünftigen Wertschöpfungsnetzwerken nicht partizipiert werden kann und dass durch erfolgreiche Angriffe die etablierten Ziele nicht erreichbar werden.

Zudem zeichnet sich ab, dass zukünftig die gesetzlichen und regulatorischen Vorgaben auch im privatwirtschaftlichen Umfeld zunehmen werden und den Betreiber dazu treiben, notwendige Securitymaßnahmen zu ergreifen. Beispiele sind das IT-Sicherheitsgesetz, die Fortschreibung der ISO/IEC 27000-Reihe oder der IEC 62443.

Weitere Standards und Normen sind in der Entwicklung und werden den zukünftig einzuhaltenden Stand der Technik darstellen. Wird der Stand der Technik im Unternehmen nicht umgesetzt, so hat das direkte Auswirkun-

Abbildung 2: Zusammenwirken der Kompetenzen über die Lieferstufen hinweg



gen bspw. auf die Versicherungen sowie Haftungsaspekte. Schon heute herrscht häufig bei Versicherungen die Devise: „Versicherbarkeit ohne Plant Security ist nicht mehr gewährleistet".

Jeder Mitarbeiter und jede Mitarbeiterin des Unternehmens muss in der Lage sein, die in seinem/ihrem Arbeitsbereich und in der jeweiligen Lebenszyklusphase relevanten Securityanforderungen zu berücksichtigen. Ihm/ihr muss die Gelegenheit gegeben werden, die notwendigen Kenntnisse und Fertigkeiten zu erwerben und anzuwenden. Die Awareness aller Beschäftigter für mögliche Bedrohungen und das richtige Verhalten sind hier nur die Grundlage für weitergehende Aufgaben wie die Definition der Securityanforderungen in der Planungsphase, die Prüfung der Securityeigenschaften bei der Abnahme in der Umsetzungsphase oder die Aufrechterhaltung der Securityeigenschaften über die Betriebsphase hinweg.

Es ist davon auszugehen, dass von der Planungs- über die Umsetzungsphase bis hin zur Betriebsphase das notwendige (Security-)Expertenwissen abnimmt, während der Personalaufwand über die Phasen zunimmt. Wird das System von Anfang an richtig geplant, reduziert sich der Umsetzungs- und Betriebsaufwand bei gleichzeitig höherem Sicherheitsniveau wesentlich. Auch hier gilt: 80 % der Kosten werden in der Planung festgelegt. Das Management sollte, über alle Phasen hinweg, das Bewusstsein für die Bedeutung des Themas gleich hoch einschätzen, damit notwendige Maßnahmen gefördert und gestattet werden.

Anforderungsprofil eines Industrial Security Officer: „Kümmerer gesucht …“

Schon die heutige Vernetzung verlangt bereits nach einer Securityverantwortung für die Produktion, da bspw. die Verwendung von, aus der Office-IT bekannten, Technologien und Organisationen wie Clouddiensten oder ISMS in der Produktion auf Know-how-Defizite stößt.

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 Überblicks- und Verantwortungskompetenz erforderlich, deren Dringlichkeit mit zunehmendem Vernetzungsgrad steigt.

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

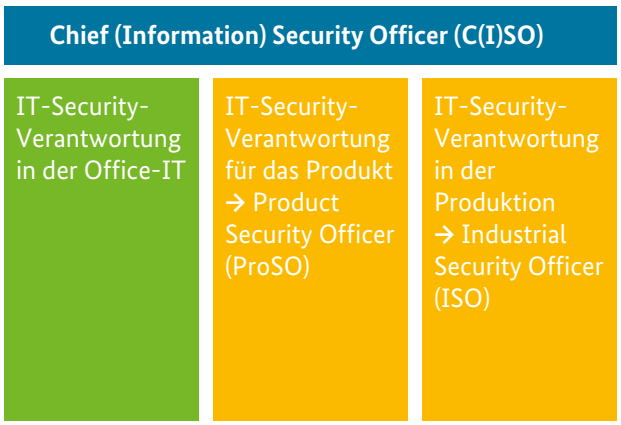
Es kann sich bspw. anbieten, eine eigene Stelle für dieses Aufgabenfeld im Sinne eines Chief (Information) Security Officer (C(I)SO) zu schaffen, der gleichermaßen für die Konzeption und Umsetzung der Sicherheitsmaßnahmen sowohl in Office-, Produktions-IT und der Produktentwicklung verantwortlich ist. 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 3).

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.

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

Abbildung 3: Aufgabenfelder eines Chief (Information) Security Officer

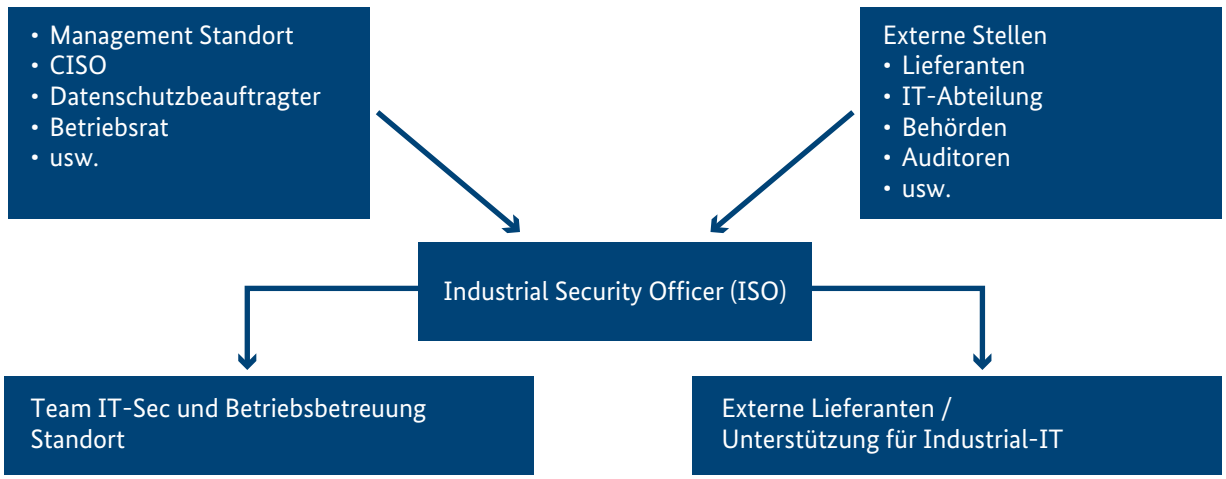


Experten mit einer umfassenden Qualifikation, die in der Lage sind, Industrie 4.0-Infrastruktur sicher zu entwickeln, aufzusetzen und zu managen, sind auf dem Arbeitsmarkt derzeit jedoch kaum zu finden. Denn die Anforderungen an solche Industrial Security Officer sind vielfältig: Sie müssen über IT, IT-Sicherheits-, Ingenieurs- und Managementkenntnisse sowie spezifische Soft Skills verfügen, wie sie in dieser Form und Konstellation bislang noch nicht ausgebildet werden.

Zudem wird es notwendig werden, organisatorische Stellen zu schaffen, die das notwendige Überblickswissen aufweisen und die Verantwortung für den im Securitysinne sicheren Betrieb der Produktion übernehmen.

Eine mögliche organisatorische Einbindung eines solchen Industrial Security Officer ist in Abbildung 3 dargestellt. Der Industrial Security Officer steht in diesem Beispiel (siehe Abbildung 4) in direktem Austausch mit dem Management und den ansonsten relevanten Funktionen wie dem Sicherheitsbeauftragten (Chief Information Security Officer (CISO)), dem Datenschutzbeauftragten und dem Betriebsrat. Wobei in KMU die ersten drei Funktionen häufig in Personalunion erfüllt werden und die neue Funktion nicht selten zu einer der drei Funktionen hinzutreten wird.

Abbildung 4: Organisatorische Einbindung eines Industrial Security Officer



Wie die Funktion im Einzelfall zugeordnet werden kann, ist sehr spezifisch. Gleichzeitig koordiniert der Industrial Security Officer die Schnittstellen zu den externen Partnern wie den Lieferanten und Wertschöpfungspartnern und führt die notwendigen Nachweise bspw. zu den ergriffenen Sicherheitsmaßnahmen ggü. Behörden und Auditoren.

Der Industrial Security Officer koordiniert zudem das Produktions-IT-Team und gewährleistet den sachgerechten Einsatz von IT-Securitymaßnahmen, ohne die Verfügbarkeit und Qualität der Produktion zu gefährden.

Ebenso übernimmt der Product Security Officer (ProSO) die Verantwortung für den Schutz der erzeugten Produkte über deren Lebenszyklus hinweg, angefangen bei der Produktkonzeption und Entwicklung über technische Dienstleistung während des Einsatzes beim Kunden, bspw. mit Updates der Software mit neuen Securityfunktionen, bis hin zur Auflösung oder Rücknahme.

Damit der Industrial Security Officer seine Aufgaben erfüllen kann, lassen sich folgende Kenntnisse und Kompetenzen des Experten als Bindeglied zwischen Office- und Produktions-IT ableiten, die in der Planungs-, Umsetzungs- und Betriebsphase unterschiedlich stark ausgeprägt zur Anwendung kommen.

Organisation

- Der Industrial Security Officer besitzt eine unabhängige und organisatorisch herausgehobene Stellung.
- Der Industrial Security Officer ist weisungsbefugt bezüglich Maßnahmen und Handlungen, welche die Sicherheitspolitik seines Aufgabenfeldes betreffen.
- Je nach Organisationsstruktur berichtet der Industrial Security Officer direkt an die Geschäftsleitung, oder indirekt über eine weitere Organisationsstelle wie z. B. einem zentralen IT-Sicherheitsbeauftragten oder CIO (Chief Information Officer).
- Die Geschäftsführung unterstützt den Industrial Security Officer bei der Wahrnehmung seiner sich aus dem Verantwortlichkeitsbereich ergebenden Aufgaben.
- Der Industrial Security Officer arbeitet mit anderen Verantwortlichen aus dem Gebiet der Informationssicherheit zusammen (z. B. Datenschutz, Werkschutz, Produktionsschutz, IT).
- Je nach Organisationsstruktur des Unternehmens müssen z. B. Aufgabenfelder der operativen Umsetzung, Einhaltung und der Durchführung von Maßnahmen zum Erhalt der Sicherheitspolitik personell unterstützt werden. Dazu können unterstützende Teams bzw. lokale Plant-Security-Koordinatoren eingesetzt werden.

Verantwortungsbereich/Aufgaben

- Aufbau und Betrieb einer lokalen Organisation zur Umsetzung der IT-Sicherheitsziele im industriellen Security-Umfeld.
- Durchführen der Entwicklung und Einführung einer unternehmensweiten Sicherheitspolitik, Handlungsleitlinien und Regelungen zur Absicherung des Erhalts der industriellen Sicherheit.
- Identifizieren von Risiken und Bedrohungen.
- Aufrechterhalten der Beziehungen mit lokalen und überregionalen Vertretern und Organisationen des Gesetzes sowie mit anderen Behörden.
- Überwachen der aus Sicherheitsverstößen resultierenden Maßnahmen & Kontrolle der Effektivität von Maßnahmen.
- Koordinieren von unabhängigen Sicherheitsaudits.
- Unterstützen und Promoten der Bewusstseinsbildung und Ausbildung für IT-Sicherheit.
- Vorabprüfung und Einbeziehen in geplante Migrations-, Veränderungs- oder Umbaumaßnahmen in System- oder Infrastrukturmaßnahmen.
- Koordinieren und Steuern von externen Beratern und Partnerfirmen, welche im Aufgabengebiet der Industrial Security tätig sind.
- Unterstützung des Managements bei IT-Sicherheitsfragen.

Befugnisse und Kompetenzen

- Ist in allen für die Informationssicherheit relevanten Themen rechtzeitig zu informieren (sowohl auf Nachfrage als auch unaufgefordert, soweit eine Relevanz für sein Aufgabengebiet besteht).
- Vorhaben und Änderungen, welche die Informationssicherheit berühren können (z. B. Migrations- oder Neuprojekte, Änderungen der IT-Infrastruktur, Änderungen von Rahmenbedingungen mit Auswirkung auf die Informationssicherheit) müssen frühzeitig in der Planungsphase mit dem Industrial Security Officer abgestimmt werden.
- Hat ein Mitsprache- und Vetorecht bei allen Entscheidungen, die seinen/ihren Verantwortungsbereich betreffen. (z. B. Initiierung von Projekten, Beschaffung von informationsverarbeitenden Systemen, Änderung von Geschäftsprozessen, Ausbildung von Beschäftigten).
- Hat direktes Vortragsrecht zur Geschäftsführung.
- Hat Zutrittsrecht zu allen Bereichen, in denen Informationstechnik seines Verantwortungsbereiches eingesetzt wird und damit zusammenhängende Daten verarbeitet werden, und zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden. Je nach Art der Daten muss er sich hierzu vorab mit dem Veranwortlichen des Daten- oder Produktschutzes abstimmen.
- Führt Prüfungen im Themenbereich der Informationssicherheit Verantwortungsbereichs-bezogen durch bzw. veranlasst Prüfungen durch unabhängige Dritte und überprüft so das aktuelle Informationssicherheitsniveau in seinem Aufgabenbereich.
- Ist Mitglied in Unternehmens-Ausschüssen zur Informationssicherheit.

Die wiederkehrenden Aufgaben in den Phasen Planung, Umsetzung und Betrieb sowie die zugehörigen Kompetenzcluster wurden im vorherigen Abschnitt eingeführt. Was dies in einem konkreten Beispiel bedeutet, soll an dem eingeführten Teilszenario Lieferkette einer Produktionseinrichtung (vgl. Abbildung 1, linker Teil) dargestellt werden.

In dem Teilszenario wirken der Systemintegrator, mehrere Komponentenhersteller und ein Kunde zusammen. Der Kunde fragt ein Produkt bei dem Systemintegrator an. Der Systemintegrator integriert ein passendes System aus zugelieferten Komponenten der Komponentenhersteller und zum Teil selbst hergestellten Komponenten und stellt es dem Kunden zur Nutzung in dessen Rahmenbedingungen zur Verfügung.

In der folgenden Tabelle sind beispielhafte Aufgaben in den Phasen Planung, Umsetzung und Betrieb zusammen mit den notwendigen Kompetenzen dargestellt.

Lfd.Nr.	Kenntnisse und Kompetenzen	Erläuterungen	Beispielhafte Aufgabe
	Grundkompetenzen		
G1	Risikomanagement	Kompetenz zur Auswahl und Gestaltung von Securitymaßnahmen auf Basis einer Bedrohungsanalyse und der Festlegung der Schutzziele	Feststellung der zu schützenden Unternehmenswerte (Assets) und die Erhebung sowie Dokumentation von Risiken, Gegenmaßnahmen und Aufwendungen ab der Planungsphase
G2	Rahmenbedingungen	Kenntnis der relevanten Gesetze, Normen und Standards im Securitybereich (IEC 62443, VDI 2875 und die DIN 2700-Reihe) und der spezifischen Gesetze, Normen und Standards für die eigene Produktion	Festlegung der Produktanforderungen (Kundenperspektive) der Produkteigenschaften (Integratorperspektive) in der Planungsphase
G3	Governance	Erstellung und Überprüfung der Einhaltung von Policies (Dienstleisterrichtlinien, technische Ausschreibungen, Prozesslandkarten)	Vertragsgestaltung unter Einhaltung der internen Compliance mit Dienstleistern und Überprüfung der externen Abstimmung zwischen Kunde und Lieferant für die Zusammenarbeit in Wertschöpfungsnetzwerken in der Umsetzungsphase
G4	Aufbau und Ablauforganisation Verständnis & Akzeptanz	Verständnis zum Zusammenwirken der Unternehmensbereiche und der Entscheidungswege Kompetenz, den Nutzen und die Notwendigkeit von Securitykonzepten und -maßnahmen auf Entscheider- und Anwendungsebene zu vermitteln und so Akzeptanz zu schaffen	Etablierung von regelmäßigem Austausch innerhalb der Aufbau- und Ablauforganisation mit dem Ziel der Harmonisierung
	IT-Kompetenzen		
I1	Software-Lifecycle	Kenntnis zur Notwendigkeit der Pflege der verwendeten Software und Kompetenz zur technischen Umsetzung unter den Randbedingungen der Produktion (vgl. G2)	Überwachung und Pflege der Produktions-IT in der Betriebsphase
I2	User / Rechte-Management	Kompetenz zur Konzeption und Umsetzung eines geeigneten User/Rechte-Managements unter den Randbedingungen der Produktion (Bspw. kann die Ablehnung eines Nutzers zur Reduzierung der Verfügbarkeit führen, vgl. G2)	Integration der neuen Produktionseinrichtung in der Umsetzungsphase und Pflege in der Betriebsphase
I3	Betriebssysteme	Kenntnisse zu technischen Vor- und Nachteilen der eingesetzten Betriebssysteme, Kompetenz zur Administration sowie Pflege (vgl. I1) und Kenntnisse zur Einsetzbarkeit/Kompatibilität bei den Systemkomponenten der Produktion (vgl. P2)	Bewertung der Alternativen in der Angebots-/Entwicklungsphase
I4	Netzwerke (Ethernet)	Kompetenz zur Konzeption und Umsetzung von Ethernet-Netzwerken einschließlich der Gestaltung von Schnittstellen und Übergängen (Conduits) zwischen Office- und Produktions-IT (vgl. P1)	Integration der neuen Produktionseinrichtung in der Umsetzungsphase
I5	Konfigurations-Management	Kompetenz zur Konzeption des Konfigurations-Managements, Änderung (Changemanagement)	Überwachung und Pflege der Produktions-IT in der Betriebsphase
I6	Angriffs-Muster & Bedrohungen	Kenntnis von Angriffsvektoren und deren Ansatzpunkten in der Produktion (vgl. P2)	Erstellung von Schutzkonzepten in der Planungsphase

Lfd.Nr.	Kenntnisse und Kompetenzen	Erläuterungen	Beispielhafte Aufgabe
I7	Sicherheitsmaßnahmen/ Lösungsansätze	Kompetenz zur Konzeption und Umsetzung von Sicherheitsmaßnahmen vor dem Hintergrund der Angriffsvektoren in der Produktion (vgl. I6)	Realisierung von technischen und organisatorischen Sicherheitsmaßnahmen in der Umsetzungsphase und deren kontinuierliche Überprüfung in der Betriebsphase
I8	Monitoring	Kompetenz zur Überwachung der Netzwerkkommunikation (Wer hat wann Zugriff auf welche Systemkomponenten (vgl. P2) zur Erkennung von Unregelmäßigkeiten und zur Abwehr von Angriffen	Erkennung von Angriffen auf die Produktions-IT in der Betriebsphase
I9	Forensik	Kompetenz zur Analyse von Securityvorfällen und zur Ableitung von Verbesserungsmaßnahmen	Erkenntnisse zu Angriffsmustern in die Planungsphase einbringen
	Produktionskompetenzen		
P1	Anforderungen der Produktion	Verständnis der Produktionsziele und deren Auswirkung auf die (mögliche) Gestaltung von Securitymaßnahmen, Auswirkungen von Securitymaßnahmen und deren Anwendbarkeit in der Produktion (Bspw. sind Updates nur während Stillstandszeiten bspw. während Wartung und Instandhaltung möglich)	Überwachung und Pflege der Produktions-IT in der Betriebsphase
P2	Systemkomponenten	Verständnis der im Produktionsumfeld eingesetzten Systemkomponenten wie PPS, MES, SPS sowie der Komponenten der Maschinen und Anlagen wie der verwendeten Kommunikationsschnittstellen und eingesetzten Sicherheitstechniken und des Nutzer- und Rechtemanagements als auch der Kommunikationsarchitektur in der Produktion (Zonenprinzip etc.)	Überwachung und Pflege der Produktions-IT in der Betriebsphase
P3	Bus-Systeme	Kenntnisse zu den Besonderheiten von Bus-Systemen in der Feldkommunikation der Produktion im Verhältnis zu Ethernet-Netzwerken (vgl. oben)	Integration der neuen Produktionseinrichtung in der Umsetzungsphase
P4	Instandhaltung	Kompetenz zur technischen Umsetzung von Instandhaltungsmaßnahmen (unter Berücksichtigung von P1, I1, I2)	Überwachung und Pflege der Produktions-IT in der Betriebsphase
P5	Audits & Zertifizierungen	Kenntnisse der notwendigen Audits und Zertifizierungen und deren Auswirkung auf die (mögliche) Gestaltung von Securitymaßnahmen, Auswirkungen von Securitymaßnahmen und deren Anwendbarkeit in der Produktion (Bspw. kann das Update der Steuerung zum Verlust der Zertifizierung im Sinne der Betriebssicherheit führen)	Nachweis des geforderten Sicherheitsniveaus der Produktions-IT, bspw. im Rahmen der Anbahnung der Zusammenarbeit in Wertschöpfungsnetzwerken
P6	Reporting, KPI-Entwicklung, KRI-Entwicklung, Überwachung	Kompetenz zur Konzeption von aussagekräftigen Kennzahlen für das Risikomanagement und zur Umsetzung eines zielgerichteten Reportings auf Basis der Überwachung (vgl. I9, I11)	Monitoring der Produktions-IT in der Betriebsphase

4 Fazit: Industrie 4.0 benötigt qualifizierte Beschäftigte und eine neu ausgerichtete Unternehmensorganisation

Erst Security ermöglicht eine Vertrauensbasis für das kooperative Arbeiten in Industrie 4.0, um verantwortlich Entscheidungen treffen zu können.

In Zeiten von Industrie 4.0 und Maschine-zu-Maschine-Kommunikation rückt mehr denn je der Mensch in den Mittelpunkt, insbesondere wenn die Technik an ihre Grenzen stößt.

Die Qualifikation der Beschäftigten entwickelt sich zum bestimmenden „kritischen Pfad".

Für die unternehmensübergreifende Zusammenarbeit in Wertschöpfungsnetzwerken ist Vertrauen die Voraussetzung. Um Vertrauen zu erlangen, müssen sicherheitsorganisatorische und sicherheitstechnische Maßnahmen angewendet werden. Für die Umsetzung dieser Maßnahmen werden Beschäftigte benötigt, die über die notwendigen Kompetenzen verfügen.

Die zunehmende Komplexität der Produktion erfordert einen umfassenden Einblick in betriebliche und überbetriebliche Strukturen. Der Qualifizierungsbedarf erstreckt sich über alle Hierarchiestufen von der Leitungsebene bis hin zur Werkbank. Digitale Transformation, neue Geschäftsmodelle und Industrie 4.0 erfordern neue Formen des Denkens, des Arbeitens, der Kooperation und letztendlich der Qualifikation des Personals. Dieser Qualifizierungsbedarf ist zeitnah zu decken, um an neuen, vernetzten Wertschöpfungsnetzwerken teilnehmen zu können und so wettbewerbsfähig zu bleiben.

AUTOREN:
Heiko Adamczyk, KORAMIS GmbH | Carsten Angeli, KUKA Roboter GmbH | Wolfgang Fritsche, IABG | Michael Jochem, Robert Bosch GmbH | Dr. Wolfgang Klasen, Siemens AG | Marcel Kisch, IBM Deutschland | Michael Krammel, KORAMIS GmbH | Lukas Linke, ZVEI e.V. | Torsten Nitschke, Phoenix Contact Software GmbH | Heiko Rudolph, admeritia GmbH | Michael Sandner, Volkswagen AG | Martin Schwibach, BASF SE | Thomas Strauch, Coriant R&D GmbH | Andreas Teuscher, Sick AG

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

www.plattform-i40.de