Hinweise des DIHK zum sicheren Einstieg in Industrie 4.0

Industrie 4.0 – aber sicher!

DIHK
Deutscher
Industrie- und Handelskammertag

Inhaltsverzeichnis

Einleitung

Diese Broschüre soll Mittelständlern helfen, sich sicherer in der Industrie 4.0 zu bewegen. Kleine Unternehmen – insbesondere im industriellen Mittelstand – zeichnen sich häufig dadurch aus, dass sie ein oder zwei spezielle Produkte anbieten, mit denen sie ein Alleinstellungsmerkmal haben – und sowohl im Land als auch außerhalb der Landesgrenzen Marktführer im Bereich dieser Nischenprodukte sind. Kleinere Unternehmen haben von Natur aus geringere Kapazitäten als größere Unternehmen, müssen aber genauso schnell voranschreiten, um ihre Technologieführerschaft nicht zu riskieren – und gleichzeitig die Sicherheit ihrer Daten und ihrer wertvollen Assets nicht zu vernachlässigen.

Die meisten Sicherheitsmaßnahmen sind recht einfach umzusetzen, und müssen nur angegangen werden. Dabei bietet es sich an, qualifizierte Partner hinzuzuziehen. Die Herausforderung ist oft, wann und wie die IT-Sicherheit in der vernetzten Produktion „starten" soll. Es von Anfang an richtig zu machen („Security by Design"), ist mittelfristig günstiger, kann jedoch ggf. die Digitalisierung verzögern. Das sollte einen aber nicht davon abhalten, pragmatisch mit ersten Maßnahmen für die Sicherheit anzufangen – die größten Risiken sind oft mit angemessenem Aufwand zu bewältigen.

Genau dies ist die Zielsetzung dieser Broschüre: machbare erste Schritte einfach vermitteln. Nicht im Fokus stehen hingegen – sicherlich auch wichtige, aber nicht immer und überall erforderliche – neue, spezielle IT-Sicherheits-Architekturen, Standards und Vorgehensweisen für Industrie 4.0; weiterführende Literatur hierzu findet sich am Ende dieser Publikation.

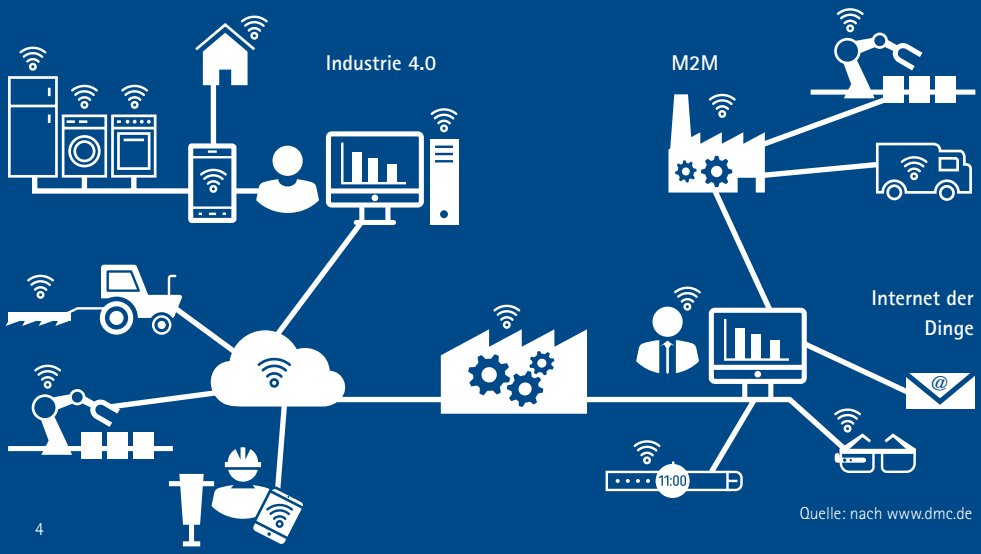
Schöne neue Welt

Die Miniaturisierung der Informationstechnologie verändert unsere Gesellschaft; die damit verbundenen Veränderungen sind aus unserem Alltag nicht mehr wegzudenken. IT-Komponenten ziehen in alle möglichen Gegenstände ein. Nicht nur Maschinen werden „schlauer" – auch alltägliche Gegenstände (Fernseher, Kaffeemaschinen, Zahnbürsten) können zunehmend mehr – und auch autark – dank Prozessoren und Netzwerken.

Während man bei der Vernetzung der Alltagsgegenstände vom „Internet der Dinge" spricht, bezeichnet man die im Wesentlichen gleiche Entwicklung in der Produktion, der Steuerung und Wartung von Industriegütern bis hin zur direkten Vernetzung von Maschinen miteinander („Machine-to-Machine", oder auch kurz M2M) mit „Industrie 4.0" oder „Internet der Dinge in Wertschöpfungsketten und Fabriken". Die so benannten Bereiche haben Übergangspunkte – die automatisierte Wartung von Haushaltsgeräten etwa, wobei die Maschine sich selbst beim Hersteller für eine Wartung anmeldet, könnte man etwa beiden Bereichen zurechnen.

Für Geschäftsführer

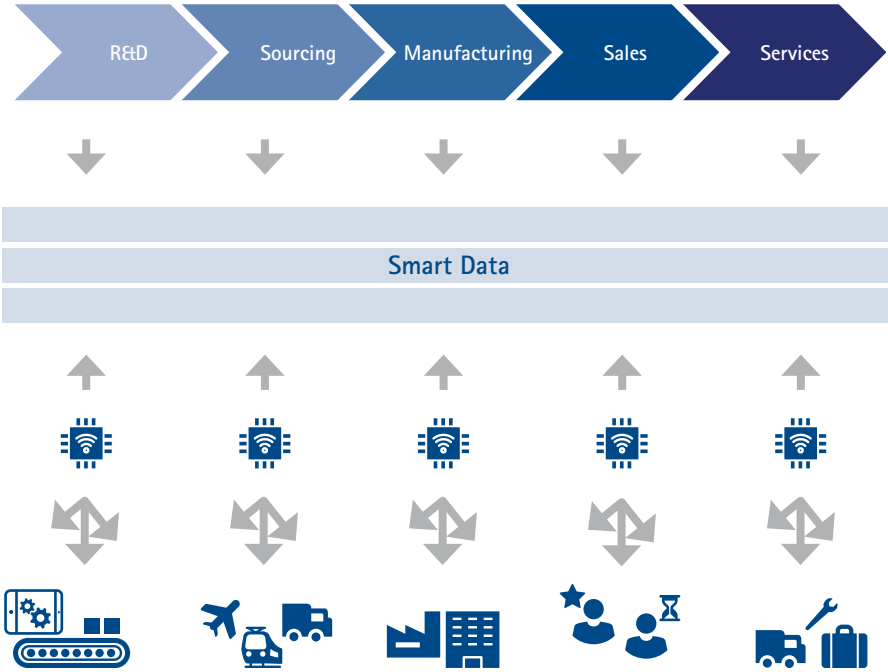
Industrie 4.0 erfordert Standardisierung und Datenbereitstellung. Dies wird den Maschinen-Markt erheblich verändern, Plattform-Betreiber werden eine zunehmende Rolle bei der Steuerung der Ökosysteme einnehmen.



Quelle: nach www.dmc.de

Neu gegenüber einer reinen Automatisierung der Produktion ist, dass erstens innerhalb von produzierenden Unternehmen Produktionsbereiche und Bürotätigkeiten überall, auch mobil vernetzt werden und zweitens eine Vernetzung der Geräte selbst (statt über so genannte Middleware) mit anderen Unternehmen auf vor- und nachgelagerten Wertschöpfungsprozessen erfolgt. Grundlage dafür sind u. a. eine erweiterte Sensorik, durch die auch nach der Ablieferung eines Produktes ein enger Kontakt vom Hersteller zu diesem bestehen bleibt, sowie eine Echtzeitanalyse und damit Optimierung der Daten. Dabei entstehen neue Geschäftsmodelle, insbesondere durch Plattformen, zum Beispiel für das Energiemanagement, eine vorausschauende Logistik oder eine objektgenaue Wartung. Ein wesentliches Ziel dabei ist es auch, die so genannte „Losgröße 1" zu erreichen – damit ist eine Individualfertigung zu Kosten der Serienfertigung gemeint.

Eine Voraussetzung für den flächendeckenden, omnipräsenten Einsatz von Informationstechnologie in der Produktion ist die Standardisierung von Komponenten – sowohl von Hardware als auch von Software. Nur dadurch können die Kosten für kleine Losgrößen auf ein angemessenes Maß reduziert werden.



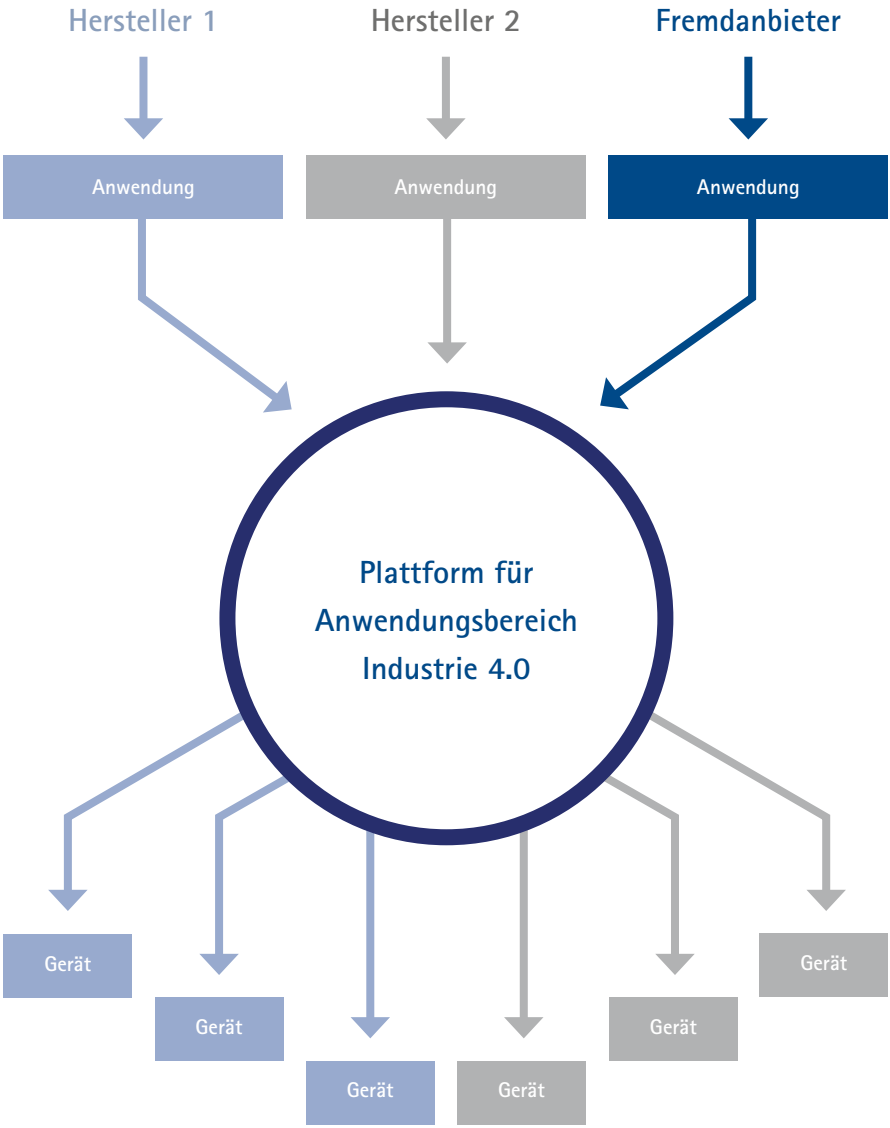
Verschiedene Anwendungsfälle, die mit Industrie 4.0 möglich werden. Quelle: nach www.serkem.de

Die Standardisierung ist zudem wesentlich für eine erfolgreiche Vernetzung: statt proprietärer Software-Lösungen, welche durch Hersteller entwickelt und verwaltet werden müssen, können Standard-konforme Geräte von beliebigen Dritt-Herstellern integriert werden. Das kennt man bereits aus dem Telekommunikations-Bereich. Dort hat die IP-basierte Telefonie proprietäre Telefonanlagen fast vollständig vom Markt verdrängt. Die Standardisierung hat darüber hinaus einen wichtigen Effekt: Das Auslesen von Daten bzw. die Steuerung der Geräte kann ohne detaillierte Kenntnis der Hardware erfolgen. Dies ermöglicht eine konsequente Trennung von Aufbau und physikalischer Inbetriebnahme von technischen Komponenten einerseits und der Steuerung der Geräte andererseits, was eine große Quelle von Optimierungen, Beschleunigungen und Einsparungen darstellen kann.

Die Standardisierung ist die Hauptvoraussetzung für eine erfolgreiche Vernetzung.

Die Trennung von Geräten und Inhalten hat aber deutlich weitgehendere Konsequenzen als nur Einsparungen: da die Standardisierung auch unternehmens- und herstellerübergreifend ist, verändern sich die Wertschöpfungsketten. Neue Marktteilnehmer betreten das Feld der Produktion und bieten durch das Bereitstellen von so genannten Plattformen einerseits Herstellern Zugang zu neuen Kunden, und andererseits Unternehmen Zugang zu neuen Mehrwert-Diensten. Im Bereich der Mobil-Telefone, Smartphones und Tablets hat diese Entwicklung bereits stattgefunden – Apple und Google beherrschen den Markt mit ihren App-Marktplätzen.

Mit den Plattformen einher geht eine Datensammlung und -analyse in bisher ungeahntem Maße: schon heute werden Bewegungsdaten von Smartphones, Nutzungsdaten von Fernsehern und Motordaten von Fahrzeugen gesammelt und ausgewertet. Den neuen, weitergehenden Möglichkeiten der Optimierung stehen Bedenken bezüglich Know-How-Schutz, Verlust der Wettbewerbsfähigkeit und – bei der Verarbeitung von personenbeziehbaren Daten – Datenschutz gegenüber. Industrie 4.0 sieht sich vor den gleichen Herausforderungen, etwa: Wie viele Daten meiner Sensoren will ich preisgeben? Wie groß ist der Nutzen für mein Unternehmen durch die Analyse der Maschinendaten meiner Kunden in Big Data Anwendungen durch Dritte, gerade im Vergleich zu meinen Konkurrenten – und wie groß mein Risiko dabei?



Effekt der Vernetzung:
Entstehung von Plattformen.

Gefahren durch die Vernetzung

Die Risiken durch die Computerisierung der Maschinen sind vielfältig; das Ausspähen von Maschinen-Konfigurationsdaten (für den Konkurrenten interessant), die Manipulation von Steuerungsinformationen (zur bewussten Fehlsteuerung, also Sabotage) oder auch nur eine Einflussnahme auf die Qualitätssicherung (etwa indem Prüfroutinen übergangen oder manipuliert werden) sind schon heute durch die Programmierbarkeit der Komponenten möglich – die Kenntnis über Befehlssätze, Schnittstellen und Zugangspunkte reicht für Spionage und Sabotage schon aus. Allerdings ist es dafür immer noch notwendig, physikalisch in die Produktion zu gelangen. Durch die Standardisierung und die damit verbundenen Vernetzungseffekte vergrößert sich das Risiko nun erheblich, denn sowohl das Wissen über die Steuerbarkeit einer Anlage oder eines Geräts als auch die Angriffspunkte um mit einer Maschine zu kommunizieren sind nun verbreitet verfügbar.

Für Geschäftsführer

Es gibt 4 Risiko-Gruppen bei Industrie 4.0, die auf jeden Fall berücksichtigt werden müssen:

- Spionage
- Sabotage
- Qualitätsprobleme
- Haftung, speziell bzgl. Produktsicherheit

Das Durchführen einer regelmäßigen Risikoanalyse ist Pflicht!

I. Sabotage

Durch die Vernetzung ist die Steuerung von Industrieanlagen prinzipiell von überall möglich. Saboteure können bei mangelnder Sicherheit die Anlagen leicht fernsteuern und manipulieren – das dafür erforderliche Wissen ist frei zugänglich. Es gibt sogar Suchmaschinen für aus dem Internet erreichbare Industrieanlagensteuerungen, damit sind diese schnell auffindbar. Die Schäden können erheblich sein: wird nur sukzessive und nur durch kaum merkliche, kleine Änderungen gesteuert, kann das zu produzierende Industriegut nicht mehr oder nicht mehr mit der erforderlichen Qualität hergestellt werden, ohne dass dies sofort entdeckt wird.

II. Spionage

Ein weiteres Risiko stellt die Industriespionage dar. Wissen über neue Produkte, neue Produktionsverfahren der Konkurrenz bis hin zu Konfigurationsdaten von Maschinen können über die Vernetzung zugänglich gemacht werden. Durch die standardisierten Protokolle bedürfen individuelle Angriffe zum unbemerkten „Abhören" und „Absaugen" keiner besonderen Kenntnisse mehr – damit ist der Spionage durch Konkurrenten Tür und Tor

geöffnet. Manche Staaten betreiben dies professionell (dann nennt man das Wirtschaftsspionage) und versorgen die eigenen Unternehmen mit strategisch interessanten Informationen.

III. Qualitätsmängel

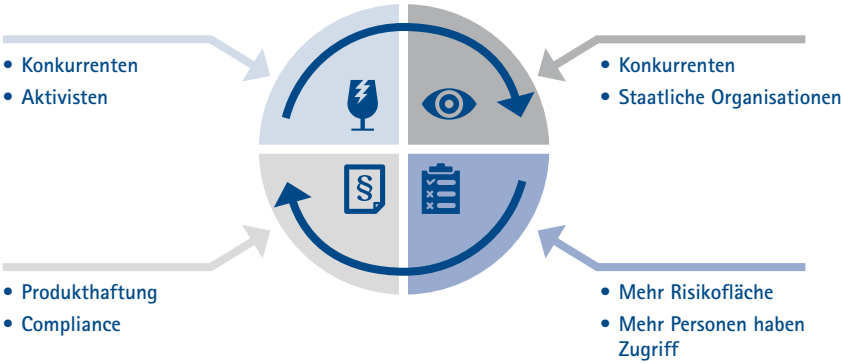
Durch die Vernetzung von Maschinen und Anlagen entsteht aber auch ein neues Qualitätsrisiko: wie kann nun bei steigender Vernetzung nachgewiesen werden, dass die Produkte den Produktsicherheitsanforderungen und sonstigen Qualitätsanforderungen genügen? Mehr Standardisierung und Vernetzung bedeutet auch, dass a priori mehr legitimierte Mitarbeiter und Kooperationspartner auf die Produktionswerkzeuge zugreifen können (evtl. sogar sollen, um die Produktivität zu steigern) – und somit in die Produktion eingreifen können. Dies wird aber in den meisten Fällen gar nicht kontrolliert – ein Qualitätsnachweis ist damit deutlich aufwändiger geworden.

IV. Haftung

Letztlich erhöht damit die Vernetzung bei Industrie 4.0 nicht nur Wettbewerbsrisiken, sondern auch Compliance- und Haftungsrisiken eines produzierenden Unternehmens, denn zunehmend fordern Gesetze und Verträge entsprechende Sicherheitsmaßnahmen.

V. Abhängigkeit

Darüber hinaus ist eine verlässliche, ausreichend leistungsfähige Internet-Anbindung erforderlich. Die Funktionsfähigkeit von Industrie 4.0 hängt in hohem Maße davon ab.



Gefahren durch die Vernetzung

Wie kann sich ein Unternehmen vorbereiten?

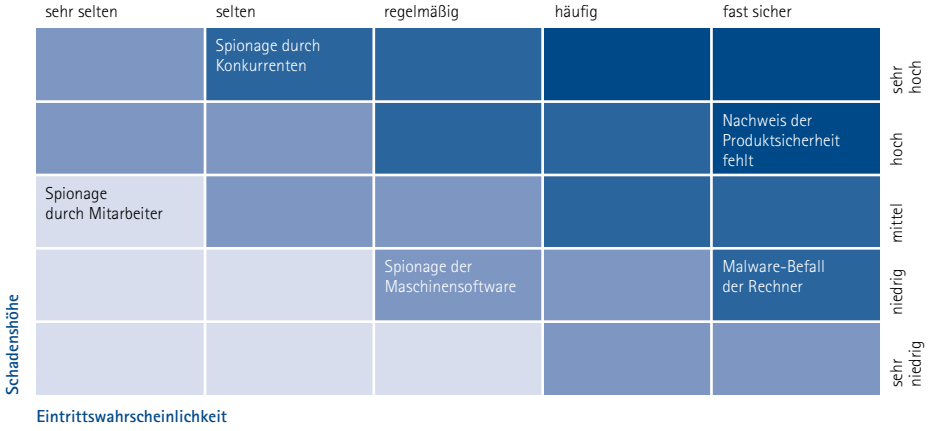
Zuallererst ist es wichtig, sich der Risiken bewusst zu werden, welche durch die Vernetzung der Industrie- und Produktionsanlagen entstehen. Dafür bietet es sich an, einen Workshop mit allen verantwortlichen Personen durchzuführen, und sie im Rahmen eines Brainstormings zu fragen, was gerade nicht passieren darf. Zuerst wird der dadurch auftretende Schaden geschätzt, und dann mit Hilfe eines Experten bewertet, wie wahrscheinlich dies passiert, auch durch die Vernetzung der Systeme (z. B. wie oft innerhalb von 3 Jahren). Die Ergebnisse werden auf einer Risikomatrix nach Schadenshöhe und Eintrittswahrscheinlichkeit aufgetragen.

Für Geschäftsführer

Die wichtigsten Sicherheitsaufgaben der Geschäftsleitung auf einen Blick:

- Risiken ermitteln
- Beauftragten benennen
- IT-Sicherheits-Richtlinie für die Produktion veröffentlichen
- Sicherheitsanforderungen an Zulieferer festlegen

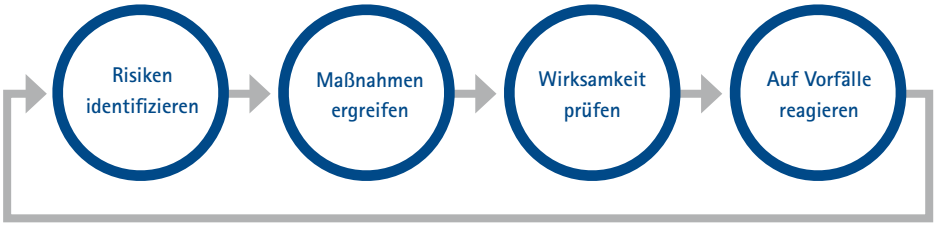
Für die höchsten Risiken (rechts oben) muss eine Risikostrategie her: es muss jeweils entschieden werden, ob das Risiko überwälzt werden kann (z. B. durch eine



Beispiel für eine Risikomatrix. Die Zahlen repräsentieren jeweils ein identifiziertes Risiko.

Versicherung), minimiert werden kann, oder ob die Geschäftsleitung bereit ist, das Risiko zu akzeptieren (dann bietet sich eine Rücklage in angemessener Größenordnung an). Sollte keine dieser Optionen möglich sein, dann muss das Risiko vermieden werden – und damit auch möglicher Weise die Elemente der Vernetzung, die das Risiko erst so groß machen.

Eine Risikoanalyse sollte jährlich durchgeführt werden. Um diese vorzubereiten, und die Maßnahmen zur Minimierung zu kontrollieren, sollte ein Verantwortlicher definiert werden. Am besten ist dafür der Informationssicherheitsbeauftragte geeignet. Sofern bereits ein so genanntes Informationssicherheits-Managementsystem (ISMS), also ein Managementsystem analog zum Qualitätsmanagement, nur eben für Informationssicherheit, im Einsatz ist, sollte die IT-Sicherheit in der Produktion mit in den Geltungsbereich aufgenommen werden. Ein ISMS ist etwa erforderlich, wenn das Unternehmen zu einer kritischen Infrastruktur gehört; es ist aber auch Stand der Technik bei der Beherrschung von IT-Sicherheitsrisiken im Kontext von GmbH-Gesetz und KontraG, und wird auch zukünftig von der EU-Datenschutzgrundverordnung gefordert.



Aspekte eines ISMS – das Management-System ist auch für Industrie 4.0 anwendbar!

Damit die Risikolage beherrschbar bleibt, müssen die Mitarbeiter in der Produktion gewisse Regeln einhalten, etwa dass keine fremde Hardware ungeprüft angeschlossen werden darf, oder dass die Fernwartung durch den Lieferanten nur über eine gesicherte Verbindung durchgeführt werden darf; die genauen Vorgaben sollten mit einem Experten auf der Basis der Risikoanalyse erstellt werden und in Form einer IT-Sicherheits-Richtlinie für die Produktion[1] allen Mitarbeitern mitgeteilt werden.

Für Informationssicherheitsbeauftragte

IT-Sicherheits-Richtlinien für die Produktion können sich stark von Unternehmen zu Unternehmen unterscheiden – diese müssen auf das jeweilige Unternehmen ausgerichtet werden.

[1] z. B. VDMA Leitfaden Industrie 4.0 Security

Vieles kann gerade ein KMU nur mit Unterstützung durch Lieferanten und Partner erreichen. Im Industrie 4.0-Umfeld ermöglichen Mittelständler Ihren Lieferanten prinzipbedingt weitgehenden Einfluss auf ihre Maschinen und Daten. Nicht immer hat der Lieferant dabei jedoch das gleiche Risikoverständnis wie sein Kunde.

IT-Sicherheits-Risiken propagieren sich entlang der Lieferkette – in beide Richtungen!

Man sollte daher alle Lieferanten, die mit der IT des Unternehmens verbunden sind, vertraglich verpflichten, Sicherheitsvorgaben einzuhalten, und das Unternehmen über wichtige Veränderungen der Lage sofort zu informieren, indem man die Sicherheitsvorgaben in die Rahmenvereinbarungen mit den Lieferanten aufnimmt.

Dies gilt insbesondere für alle IT-Dienstleister, und speziell die Lieferanten von Maschinen und deren Software. Die Verwendung von Sicherheitsvorgaben erlaubt, die Risiken, die durch den Lieferanten entstehen, beherrschen zu können – siehe den Abschnitt „Forderungen an den Software- oder Maschinen-Anbieter".

Für Informationssicherheitsbeauftragte

Jedes Unternehmen sollte – zumindest sporadisch – prüfen, dass seine Lieferanten sich auch an die Sicherheitsvorgaben halten. Für diese Prüfung können spezialisierte Dienstleister beauftragt werden.

Eine Sache muss die Geschäftsführung selbst angehen: die Verantwortlichen in der Produktion lassen sich ungern von Dritten reinreden, und die zusätzlichen Sicherheitsmaßnahmen, die vom Informationssicherheitsbeauftragten gefordert werden, sind oft auch mit Verzögerungen oder etwas komplizierteren Abläufen verbunden. Damit die Sicherheit „greift", müssen die Verantwortlichen mitziehen.

Für Geschäftsführer

Die zusätzlichen Anforderungen können die Produktionsabläufe verändern. Die Produktionsleiter müssen dies unterstützen. Das sicherzustellen ist Chefsache.

Mindestens jährlich sollte die Risikoanalyse erneut durchgeführt bzw. auf erforderliche Anpassungen untersucht werden. In der Folge sollte dann die IT-Sicherheitsrichtlinie in der Produktion angepasst und – wie auch die Einhaltung der Sicherheitsvorgaben durch die Lieferanten – auf Einhaltung geprüft werden (etwa durch Stichproben).

Folgen für das Produktionsnetz

Neben den organisatorischen Maßnahmen aus dem letzten Kapitel sind einige grundlegende technische Vorkehrungen für einen Basisschutz erforderlich. Die meisten Angriffe benötigen einen netzbasierten Zugang. Dementsprechend kann man schon sehr viel erreichen, wenn das Netz abgesichert wird.

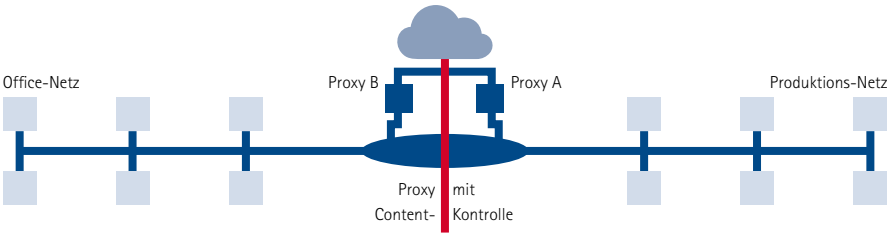
Zuallererst muss das Netz, in dem die Produktionsmaschinen laufen, von anderen Computernetzen getrennt sein. Viel Schadsoftware wird über die Arbeitsrechner der Mitarbeiter eingeschleppt, daher darf insbesondere das Büro-Netzwerk keine beliebige Verbindung zum Produktionsnetzwerk haben.

Die Maschinen dürfen niemals „direkt" im Internet stehen. Damit ist gemeint, dass sie „von außen" nicht direkt ansprechbar bzw. sichtbar sind. Anfragen an die Maschinen müssen immer über Proxies laufen, damit die Anfragen und die entsprechenden Antworten gepuffert und so auf schadhafte Inhalte kontrolliert werden können (derartige Funktionalitäten liefern so genannte „Application Level Firewalls"). Zudem ist es damit für Angreifer deutlich schwerer, eine Rückmeldung von eingeschleustem Schadcode oder auf durchgeführte Angriffe zu bekommen.

Für Produktionsleiter

Apropos Netz: Viele intelligente Maschinen verwenden schon heute Funktechniken mit eigenen Frequenzbereichen – mit dem Ergebnis, dass sich heute vielfach schon unterschiedliche Maschinen gegenseitig behindern. Zudem hat ein Unternehmen in diesem Fall keinerlei Kontrolle über die Kommunikation von und zu seinen Maschinen.

Es sollte daher soweit wie möglich vermieden werden, dass Maschinen in der Produktion eigene Funkverbindungen aufbauen – statt dessen sollten alle idealer Weise WLAN mit WPA2 verwenden. Der Zugriff auf Produktionsmaschinen darf niemals direkt vom Arbeitsplatzrechner aus möglich sein – viel besser ist es, den Zugriff über so genannte Remote Desktops zu realisieren, so genannte PCs, die in Produktionsnetzwerk stehen, und auf deren Bildschirm über das Netz zugegriffen wird.



Office- und Produktionsnetz sollten möglichst getrennt sein und nur über Proxies verbunden.

Noch schwerer wird es für Angreifer, wenn man für eingehende Kommandos (z. B. Bestellungen) und ausgehende Informationen (z. B. Statusinformationen) unterschiedliche Internet-Anschlüsse verwendet – denn dann ist eine Steuerung von Maschinen mit direktem Antwortverhalten nicht möglich.

Fernwartung sollte idealer Weise von innerhalb des eigenen Netzes gestartet (oder zumindest bestätigt) und optimaler Weise durch einen eigenen Mitarbeiter durch Sichtkontrolle begleitet werden. Alternativ können entsprechende vertragliche Regelungen getroffen werden, um das betriebswirtschaftliche Risiko zu minimieren. Kleine und mittlere Unternehmen können in der Regel keine Angriffe selbst erkennen – die dafür erforderliche Fachkenntnis bindet oft zu viele Ressourcen. Um dennoch von Angriffserkennung zu profitieren und geeignete Alarme zu bekommen, beauftragt man den eigenen Netzwerkdienstleister mit der Angriffserkennung – alternativ eine spezialisierte Firma, die entsprechende Sensoren im Netzwerk platzieren und überwachen kann.

Für Produktionsleiter

Vorsicht bei Queue- / Integrationssystemen: Es gibt gerade in größeren Installationen spezielle Rechner, die zwischen den einzelnen Systemen hin- und herübersetzen, da sie nicht die gleiche Sprache sprechen. Diese sind besonders zu schützen, da sie einen neuralgischen Angriffspunkt darstellen (z. B. zumeist Zugriff auf alle anderen Systeme haben). Und: nicht genutzte Zugänge sollten gelöscht werden!

Zudem sollte eine Verwaltung der Maschinen und der zugehörigen IT-Systeme eingeführt („Configuration Management Data Base - CMDB") und regelmäßig geprüft werden, ob die Systeme im Netzwerk auch dazu passen (und keine fremden, auch keine virtuellen, Systeme auftauchen). Die Software der Maschinen muss auch stets möglichst aktuell sein, daher müssen – sofern verfügbar – für Software-Updates entsprechende Wartungsfenster eingeplant werden, in denen idealer Weise die Software-Updates auch getestet werden. Ist das nicht möglich, so ist die Absicherung des Netzwerks umso wichtiger.

Schließlich sollten alle Verbindungen zwischen Maschinen sowie zwischen Maschinen und anderen Computern verschlüsselt und authentifiziert ablaufen. Nur in dokumentierten und genehmigten Ausnahmefällen darf davon abgewichen werden, etwa wenn die Echtzeitfähigkeit dadurch gefährdet wäre (das ist aber nur selten wirklich der Fall). Die dafür erforderlichen Identitäten der Maschinen (Kennungen, Passwörter, Zertifikate) werden am besten mit einem entsprechenden Identitätsmanagementsystem verwaltet.

Analog zum Brandschutz sollte ein Notfallplan vorbereitet werden, der sicherstellt, dass auf Meldungen über Schwachstellen und tatsächliche Angriffe angemessen reagiert werden kann. Übungen sollten regelmäßig durchgeführt werden, um in Notfallsituationen mögliche Schäden schnell begrenzen zu können. Zentrale Anlauf- und Steuerungsstelle ist idealer Weise der Informationssicherheitsbeauftragte.

Forderungen an den Software- oder Maschinen-Anbieter

Die moderne Fabrik erfordert ständige Optimierungen – diese finden zunehmend im Software-Bereich statt. In den folgenden Fällen sollte auf die Sicherheit Ihrer Maschinen, Systeme und Daten geachtet werden:

- beim Kauf von Maschinen (inzwischen werden kaum noch Maschinen ohne Software-Unterstützung ausgeliefert),
- bei der Beauftragung von Software-Entwicklung oder -Anpassung rund um Ihre Maschinen,
- bei der Nutzung von Industrie 4.0-Plattformen und -Diensten.

Für Informationssicherheits-beauftragte

Es ist ein wichtiger Erfolgsfaktor, bei der Beauftragung von Leistungen rund um die Maschinen mit einbezogen zu werden. Ein Katalog von Sicherheitsanforderungen zur vertraglichen Vereinbarung mit Lieferanten ist sehr hilfreich.

Dabei ist am Wichtigsten, dass man die Anforderungen an den Vertragspartner vertraglich regelt, etwa in einem so genannten Security Service Level Agreement.

Eine solche vertragliche Vereinbarung über Sicherheitsaspekte sollte mindestens die folgenden Aspekte abdecken:

- Der Dienstleister hält alle sicherheitsrelevanten Systeme (Firewalls, Windows Domänen Controller etc.) sowie alle Systeme, die für das Unternehmen betrieben werden, aktuell.
- Der Dienstleister verwendet ausschließlich sichere Kommunikation (Verschlüsselung der Verbindung mit Standard-Protokollen wie TLS oder IPSEC, Authentifizierung mit sicheren Passwörtern mit mindestens 12 Zeichen) – wenn er sich mit den Systemen des Unternehmens verbindet, aber auch etwa wenn er selbst Fernwartung für die Administration seiner Systeme einsetzt.
- Der Dienstleister setzt nur in IT-Sicherheit qualifiziertes Personal ein.
- Der Dienstleister informiert das Unternehmen unverzüglich über Veränderungen der Sicherheit, etwa, wenn Sicherheitslücken in der Maschinensoftware bekannt werden, oder wenn eigene Systeme gehackt wurden.

Zudem ist es erforderlich, dass auch Lieferanten des Dienstleisters die gleichen Sicherheitszusagen machen, wenn sie die Sicherheit der Maschinen direkt oder indirekt beeinflussen können.

Die Supply-Chain-Risikopropagation trifft auch für die Software in Ihren Maschinen zu!

Darüber hinaus sind die Systeme dann leichter zu sichern, wenn sie Standard-Komponenten mit etablierten Sicherheitsprotokollen verwenden, statt selbst entwickelter Protokolle und eventuell sogar Sprachen. Man sollte sich vom Lieferanten zeigen lassen, wie er die „ISA 99"-Sicherheitsarchitektur erfüllt – das ist ein branchenübergreifender Sicherheitsstandard für Industrie 4.0.

Auch ist zu bedenken, dass eine leistungsfähige Internet-Anbindung Voraussetzung für den erfolgreichen Einsatz von Industrie 4.0 ist – aber was passiert, wenn das Internet mal „ausfällt"? Sollte es einen Notfallplan „ohne Internet" geben, so muss die Software der Maschinen diesen Plan auch unterstützen.

Die gleiche Argumentation gilt auch für die Kunden: es ist damit zu rechnen, dass Kunden ähnliches fordern – insbesondere dann, wenn das Unternehmen auch selbst Maschinen baut, und diese „Industrie 4.0 ready" macht.

Schließlich sollte man Vorsorge tragen, dass Schwachstellen und Sicherheitsvorfälle bei Kunden sich nicht negativ auf das eigene Unternehmen auswirken. Eine vertragliche Regelung und damit Verschiebung der Haftung ist in den meisten Fällen nicht möglich.

Exkurs: Für Maschinen-Software-Entwickler

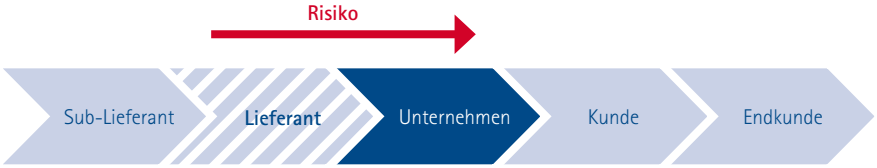
Vielleicht wird in Ihrem Unternehmen die Software zur Steuerung oder Auswertung der Maschinen selbst geschrieben – oder das Unternehmen ist ein Dienstleister, welcher die Maschinen mit Software ausstattet. In diesem Fall sollten die folgenden Aspekte berücksichtigt werden.

Zuallererst müssen die Anforderungen, die in dem vorigen Abschnitt besprochen wurden, selbst erfüllt werden. Insbesondere die sichere Kommunikation zum Kunden,

Für Software-Entwicklungsleiter

Die wichtigsten Sicherheitsaufgaben auf einen Blick:

- Programmierer in „sicherer Software-Entwicklung" schulen
- Support, z. B. Patches, einplanen
- Betriebsanforderungen des Kunden berücksichtigen
- Kunden über mögliche Sicherheitsprobleme informieren



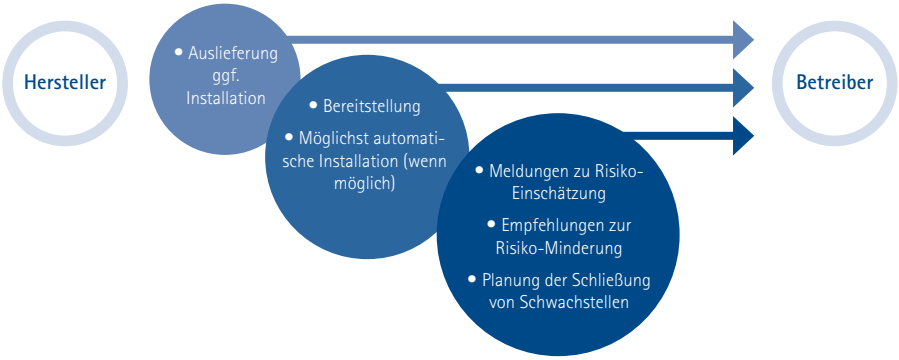
Als Software- und Maschinenlieferant hat man erheblichen Einfluss auf die Risikolage bei seinen Kunden.

und den Umgang mit Sicherheitsvorfällen und Schwachstellen in Software sollte zur Standardvorgehensweise gehören. Denn nur dann kann der Kunde sein Risiko richtig einschätzen – ansonsten ist er im Blindflug.

Für Software-Entwickler im Maschinenumfeld sind aber noch weitere Aspekte wichtig. Viele Aspekte können von der „Standard-IT" übernommen werden, um sichere Software entwickeln zu können. Dazu gehört etwa:

- Von vornherein sollte vorgesehen sein, dass Maschinensoftware auch gepatcht werden können muss, d. h. dass es einen vertrauenswürdigen Prozess geben muss, mit dem neue, überarbeitete oder auch von Schwachstellen bereinigte Software zeitnah und sicher eingespielt werden kann.

- Selbst entwickelte Sicherheitskonzepte sind sehr komplex! Die Wahrscheinlichkeit, dass man dabei Fehler macht, ist sehr hoch.



Neben Patches gehören Informationen zu Schwachstellen zu den wichtigsten Support-Leistungen.

Wo immer möglich sollten unabhängig geprüfte, etablierte Sicherheitsprotokolle, und idealer Weise sogar gut getestete Programmbibliotheken verwendet werden[2]. Dies gilt auch für Passwort-Prüfung und –Verwaltung!

- Die eigenen Entwicklungsprozesse müssen abgesichert sein, damit Hacker sich nicht schon frühzeitig über das Einbringen von Hintertüren in die Software-Entwicklung einschleichen können (sichere Ablage des Quellcodes, gesicherter Netzzugang, Berechtigungskonzepte).

- Die Software sollte aus Sicherheitsgründen ausschließlich die für die Ausführung ihrer Aufgaben erforderlichen Berechtigungen haben (keine Admin-Rechte), damit im Falle eines Angriffs die Berechtigung nicht für einen Angriff auf weitere Anwendungen oder Rechner genutzt werden kann.

- Bei der Maschine-zu-Maschine-Kommunikation sollten möglichst keine Benutzer-Passwort-Kombinationen zur sicheren Authentifizierung der Komponenten verwendet werden, da deren Verwaltung schnell komplex wird und nicht mehr beherrscht werden kann[3]. Verwenden Sie stattdessen Zertifikate für die Authentifizierung und verschlüsselte Kommunikation zwischen den einzelnen Komponenten.

- Die Software-Entwicklung sollte nach einer Methodik des „Secure Software Engineering" durchgeführt werden – es gibt einige Vorgehensmodelle, wie etwa Microsoft's „Secure Development Lifecycle", oder „OWASP OpenSAMM", oder die (zertifizierbaren) Common Criteria (ISO 15408).

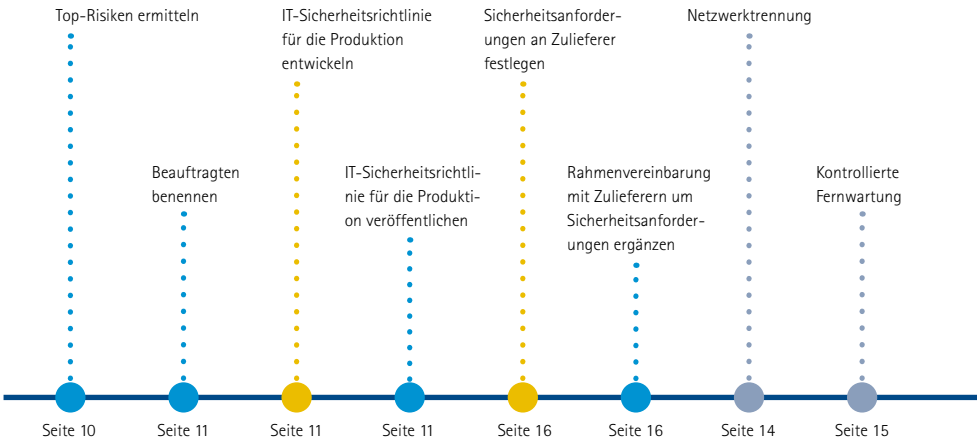
Auf jeden Fall sollten die Entwickler der Software für Maschinen und Anlagen regelmäßig auf Sicherheit geschult werden, und dies nach dem neuesten Stand.

---

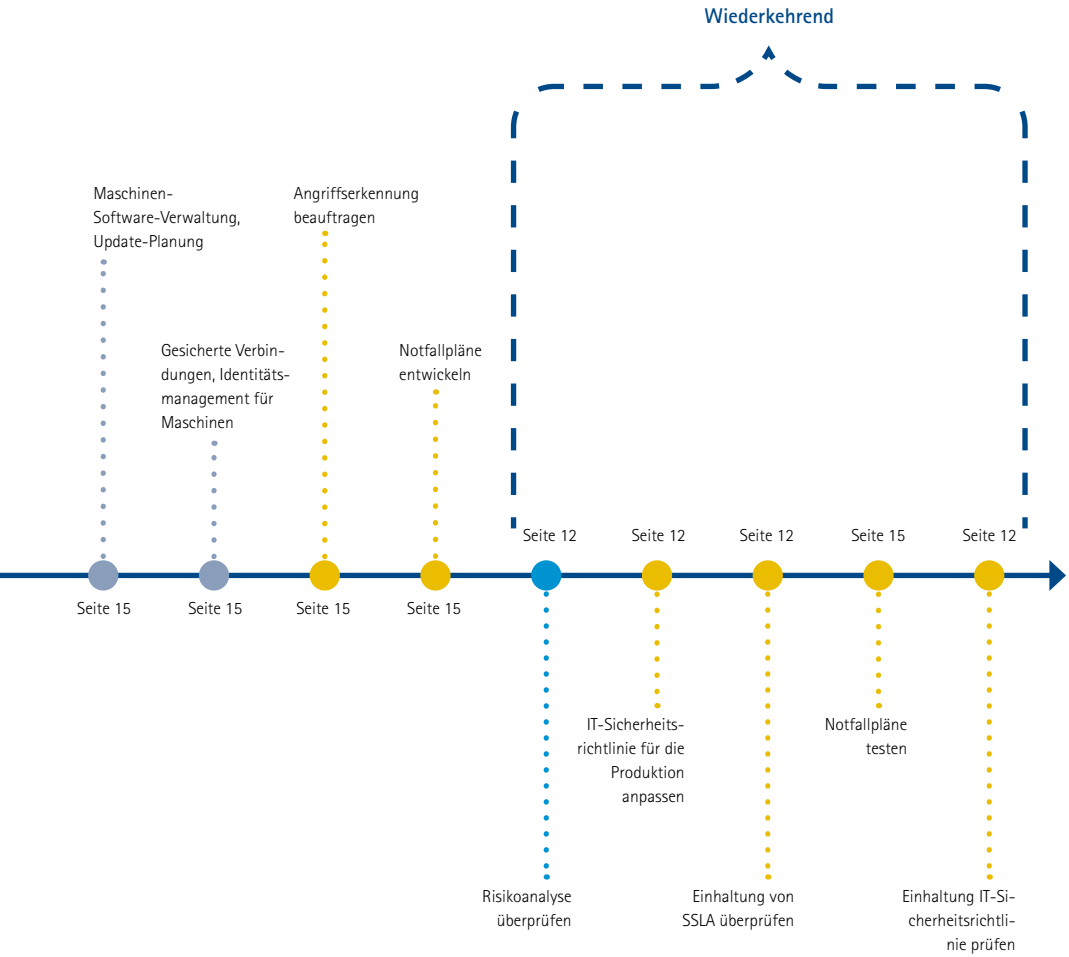
[2] Eine Auswahl findet sich z. B. bei www.owasp.org / [3] Empfehlenswert sind statt dessen Konzepte wie „Föderation von Identitäten", wie sie mit den Standard SAML und OAuth verfolgt werden.

Zusammenfassung der Aufgaben nach Verantwortlichkeit

Hier finden Sie noch einmal zusammengefasst die wichtigsten Aktivitäten in zeitlicher Reihenfolge (ohne Software-Entwicklung):



- **Steuerung / Geschäftsführung**
- **Technik / Produktionsleiter**
- **Organisation / IS-Beauftragter**


Wiederkehrend
Maschinen-Software-Verwaltung, Update-Planung
Angriffserkennung beauftragen
Gesicherte Verbindungen, Identitätsmanagement für Maschinen
Notfallpläne entwickeln
Seite 15
Seite 15
Seite 15
Seite 15
Seite 12
Seite 12
Seite 12
Seite 15
Seite 12
IT-Sicherheitsrichtlinie für die Produktion anpassen
Notfallpläne testen
Risikoanalyse überprüfen
Einhaltung von SSLA überprüfen
Einhaltung IT-Sicherheitsrichtlinie prüfen

Weiterführende Literatur

Wenn Sie sich in dieses Thema weiter einarbeiten möchten, empfehlen wir folgende Arbeiten:

BDEW: BDEW Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. Mit Ausführungshinweisen und Checkliste. www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge

BDEW: Technische Empfehlungen für den sicheren Datenaustausch in der Marktkommunikation. www.bdew.de/internet.nsf/id/it-sicherheitsempfehlunge

BMWI: Abschlussbericht der Studie IT-Sicherheit für die Industrie 4.0. www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0-langfassung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

BSI: ICS Security Kompendium. Zwei Varianten: für Betreiber sowie für Hersteller und Integratoren. www.bsi.bund.de/ICS-Security-Kompendium

Harvard Business Review: Michael E. Porter, James E. Heppelmann: Wie smarte Produkte den Wettbewerb verändern. Hardvard Business Review 12/2014.

ISA/IEC: IEC 62443 – Industrial Automation and Control Systems Security. http://isa99.isa.org

Plattform Industrie 4.0: Wegweiser IT-Security in der Industrie 4.0. www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/wegweiser-it-security.pdf?__blob=publicationFile&v=12

VDMA: VDMA Studie: Status Quo der Security in Produktion und Automation 2013/2014. VDMA e.V., Abt. Informatik.

VDMA: VDMA Fragenkatalog „Industrial Security". Oktober 2014. VDMA e.V., Abt. Informatik, pks.vdma.org/security

VDMA: VDMA Leitfaden Industrie 4.0 Security. April 2016. VDMA e.V., Abt. Informatik. Nur für Mitglieder.

VDI: VDI/VDI 2182 Informationssicherheit in der industriellen Automatisierung. 2011. Mit Anwendungsbeispielen (SPS-Hersteller – Umformpresse-Anlagenbauer – Betreiber Presswerk – LDPE-Reaktor-Integrator – LDPE-Reaktor-Anlagenbetreiber – LDPE-Prozessleitsystem-Hersteller). 2013–2016 www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/fachbereiche/industrielle-informationstechnik/gma-fa-522-security

Herausgeber/Copyright:
© Deutscher Industrie- und Handelskammertag | Berlin | Brüssel
DIHK Berlin: Hausanschrift: Breite Straße 29 | Berlin-Mitte

Redaktion/Durchführung:
Prof. Dr. Sachar Paulus, paulus.consult; Michael Kowalski, DIHK;
Dr. Katrin Sobania, DIHK

Gestaltung/Grafiken:
Jana Eger

Stand:
November 2016

Download:
Das PDF zu Broschüre. Jetzt downloaden per QR-Code
oder unter www.dihk.de/sichere-industrie

DIHK Deutscher Industrie- und Handelskammertag