Competence Center Industrial Security

Industrial Security im Maschinen- und Anlagenbau

Ergebnisse der VDMA-Studie und Handlungsempfehlungen

Inhalt

Vorwort

Steffen Zimmermann

Der Maschinen- und Anlagenbaubau ist eine wichtige Schlüsselbranche und Motor für die deutsche Wirtschaft. Mit einem Umsatz in 2018 von rund 232 Milliarden Euro und rund 1,3 Millionen Beschäftigten ist die Branche der größte industrielle Arbeitgeber und einer der führenden deutschen Industriezweige insgesamt. Die Produkte und Dienstleistungen des Maschinen- und Anlagenbaus genießen weltweit hohes Ansehen. Nahezu 80 Prozent der deutschen Produktion gehen in den Export.

Die Industrial Security hat in den letzten Jahren immer stärker an Bedeutung gewonnen. Nicht zuletzt durch Ereignisse wie Stuxnet, WannaCry und NotPetya[1] hat sich auch die öffentliche Wahrnehmung der „Industrial Security“ erhöht.

Die vorliegende Studie gibt einen vertieften Einblick in den aktuellen Status zur Industrial Security des deutschen Maschinen- und Anlagenbaus. Darüber hinaus wurden zu jedem Themengebiet praxisnahe Handlungsempfehlungen des VDMA-Arbeitskreises Industrial Security ergänzt, um die Unternehmensführung und in den Unternehmen beauftragte Personen für Industrial Security bei der Umsetzung zu unterstützen.

Steffen Zimmermann
VDMA Competence Center Industrial Security
Leiter des VDMA Arbeitskreises Industrial Security

1 https://www.heise.de/newsticker/meldung/Nach-NotPetya-Angriff-Weltkonzern-Maersk-arbeitete-zehn-Tage-lang-analog-3952112.html

Management Summary

Nach 2013 hat der VDMA mit Unterstützung weiterer Partner eine erneute Befragung zur Industrial Security unter produzierenden Unternehmen in Deutschland durchgeführt, deren Ergebnisse in der vorliegenden Studie veröffentlicht sind. Dabei geht es vorrangig um die Fragen, welche Kompetenzen die Unternehmen diesbezüglich aufgebaut haben, welche Standards und Maßnahmen zum Einsatz kommen, welche Bedrohungen aus aktueller Sicht das größte Risiko darstellen und welche Auswirkungen Security-Vorfälle verursacht haben.

Die wichtigsten Ergebnisse im Überblick.

- Rund 60 Prozent der Unternehmen rechnen für die kommenden Jahre mit einer Steigerung der Security-Vorfälle im eigenen Unternehmen.
- Von Security-Vorfällen betroffene Unternehmen verzeichnen zumeist Kapitalschäden (50 Prozent) und Produktionsausfälle (31 Prozent). Safety-relevante Auswirkungen (Gefährdung von Mensch oder Umwelt) sind in den vergangen zwei Jahren erfreulicherweise nicht registriert worden.
- Zu den Bedrohungen mit der höchsten Risikoeinschätzung gehören nach wie vor „Menschliches Fehlverhalten und Sabotage“ (Platz 1) und das „Einschleusen von Schadsoftware“ (Platz 2). Unter anderem neu hinzugekommen in die Liste der Top 10 Bedrohungen ist „Social Engineering und Phishing“ auf Platz 3, das von Unternehmen mit mehr als 1.000 Mitarbeiter sogar als besonders risikoreich beurteilt wird.
- Mittlerweile kennen 83 Prozent der Unternehmen einen der gängigen Security-Standards und knapp die Hälfte (41 Prozent) wendet diese auch an. Insbesondere mangelndes Know-how ist jedoch noch ein Hindernis für den Einsatz, vornehmlich bei kleineren Unternehmen (bis 250 Mitarbeiter) wird dieser Umstand deutlich.
- Bei der Etablierung eines Risikomanagements im Produktionsumfeld gibt es noch Handlungsbedarf. Erst 41 Prozent haben ein solches eingeführt. Die gezielte Abschätzung von Ausfallkosten bei Security-Vorfällen spielt nach wie vor für rund drei Viertel der Unternehmen keine Rolle.
- Vom IT-Sicherheitsgesetz zum Schutz kritischer Infrastrukturen (KRITIS) sind die befragten Unternehmen bisher nicht direkt betroffen. Nur etwa ein Fünftel wird aufgrund der Tätigkeit als Servicedienstleister, Komponentenlieferant oder Integrator davon berührt.
- Nur 3 Prozent der Unternehmen können sich bisher ein Security-Gütesiegel als „generell verpflichtendes Entscheidungskriterium“ für den Produkteinkauf vorstellen.

Die nachfolgenden Seiten vermitteln einen detaillierten Einblick in die Ergebnisse der Befragung und unterbreiten geeignete Handlungsempfehlungen.

1 Industrial Security – Schutz der Maschine vor dem Menschen

Industrial Security ist der Schutz technischer Systeme in Produktion, Fertigung und Intralogistik vor prinzipiell unbekannten Angriffen und Störungen mit dem Ziel, den Geschäftsprozess im Betrieb aufrecht zu erhalten. Als technische Systeme gelten dabei Maschinen und Anlagen, deren industrielle Steuerungskomponenten, Netzwerkkomponenten, Sensoren und Aktoren sowie die mit den Systemen verbundenen Dienste.

Ursache von Angriffen und Störungen technischer Systeme sind Menschen oder die Umgebung (Umwelt) des Systems. Zum besseren Verständnis lässt sich dies auf „Schutz der Maschine vor dem Menschen“ reduzieren.

Zwei Sichtweisen – ein Thema

Für den Maschinen- und Anlagenbau gibt es zwei unterscheidbare Sichtweisen auf die Industrial Security. Die Sicht als Anwender und Betreiber möglichst zuverlässiger Anlagen sowie die Sicht als Hersteller und Integrator von Maschinen und Anlagen.

Die Security in der Produktion, auch als „OT Security“ bekannt, betrachtet Maßnahmen für eine zuverlässige, robuste und vertrauenswürdige Vernetzung von Maschinen und Anlagen in der eigenen Produktion und Fertigung des Maschinen- und Anlagenbaus (Betreibersicht).

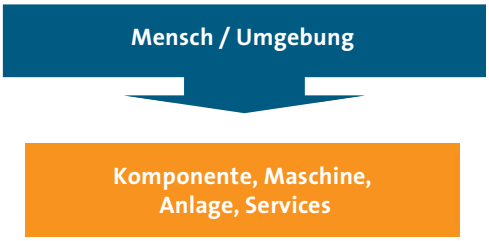
Bei der Security von Maschinenbauprodukten („Product Security“) geht es um technische und organisatorische Schutzmaßnahmen von Maschinen, Anlagen und deren Komponenten, digitalen Dienstleistungen und Geschäftsprozessen über den gesamten Produktlebenszyklus (Hersteller- und Integratorsicht), von Design und Konstruktion bis zur Außerbetriebnahme.

OT Security:
Schutz der eigenen Produktions- und Fertigungsumgebung,
um Verfügbarkeit des eigenen Geschäftsprozesses sicher zu stellen.

➠ Rolle als Anwender, Betreiber

Product Security:
Schutz der zu verkaufenden Produkte
vor prinzipiell unbekannten Angriffen, um den Geschäftsprozess des Kunden sicher zu stellen.

➠ Rolle als Hersteller, Zulieferer oder Dienstleister



2 Allgemeines zur VDMA-Studie

Verständnis der Industrial Security

Im Rahmen dieser Studie ist die Bezeichnung „Industrial Security“ als Prozess zu verstehen, der den Schutz vor

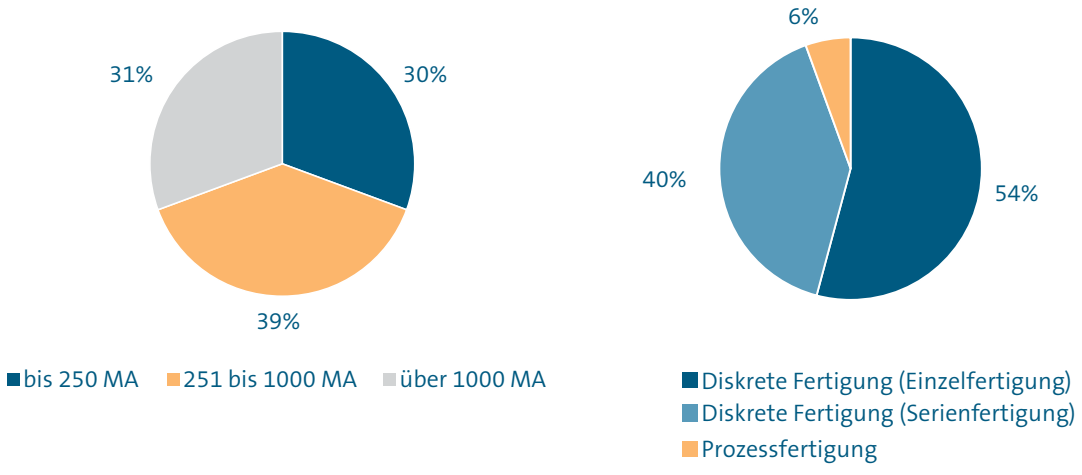
- Ausfall,
- Know-how-Abfluss und Spionage sowie
- Manipulation von Maschinen, Anlagen und Industriedaten

sicherstellen soll. Alle Fragen haben sich, soweit nicht anders hervorgehoben, ausschließlich auf die Security von Maschinen und Anlagen bezogen. Dazu ist die Erhebung vorrangig an die Verantwortlichen für Produktionseinrichtungen der Unternehmen adressiert worden. Security-Vorfälle aus dem „Office-Umfeld“ sind nur dann von Relevanz gewesen, wenn sie auch Auswirkungen auf Maschinen oder Anlagen gezeigt haben.

Teilnehmerstruktur

An der Studie haben insgesamt 66 Unternehmen teilgenommen. Vier davon besitzen keine eigene Produktions- oder Fertigungsumgebung. Deren Antworten werden deshalb in den weiteren Betrachtungen nicht mitberücksichtigt. Von den 62 produzierenden Firmen hat die Mehrheit eine diskrete Fertigung (94 Prozent). Lediglich 6 Prozent sind Prozessfertiger. Die Verteilung der Unternehmensgrößen in der Studie ist in der Abbildung 1 dargestellt.

Verteilung der Betriebsgrößen und Fertigungsarten



N = 62

Abbildung 1

Quelle: VDMA-Report Industrial Security

3 Beauftragte Personen für Industrial Security

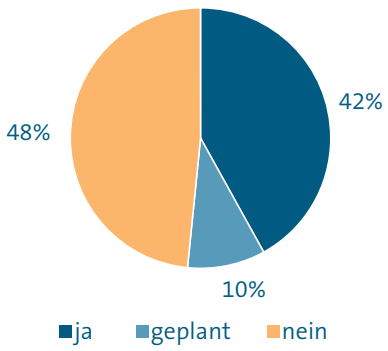
Industrial Security ist von zentraler Bedeutung für alle Unternehmen, die im Produktionsbereich (inkl. Lager und Logistik) programmierbare Systeme (z.B. Personal Computer, Tablets, Speicherprogrammierbare Steuerungen, Bedienterminals) einsetzen. Um zielgerichtet einen ausreichenden Schutz dieser Systeme zu erreichen, bedarf es einer klaren Beauftragung eines oder mehrerer qualifizierter Mitarbeiter durch die Firmenleitung.

Nach wie vor gibt es bei der Mehrzahl der Maschinen- und Anlagenbauer noch keinen Beauftragten für die Security in der Produktion (58 Prozent). Allerdings planen bis 2020 rund 10 Prozent der Befragten, in diesem Bereich „nachzurüsten“. In Unternehmen mit mehr als 1.000 Mitarbeitern haben mittlerweile schon 68 Prozent der Unternehmen Personen für die Industrial Security beauftragt (2013: 46 Prozent) und weitere 5 Prozent planen, dies in den kommenden Jahren zu tun.

Dabei setzen die Unternehmen mittlerweile ausschließlich auf die Kompetenz der eigenen Mitarbeiter. Gegenüber 2013 hat sich der Fokus damit nun eindeutig auf die Eigenkompetenz der Unternehmen verschoben. Damals hatten noch 20 Prozent der Befragten externe Dienstleister beauftragt.

Bei Unternehmen mit weniger als 1.000 Mitarbeitern ist überwiegend nur ein Mitarbeiter für die Industrial Security verantwortlich. Einen verstärkten zusätzlichen Kompetenzaufbau in diesen Unternehmen ließen die Studienergebnisse für den Zeitraum seit 2014 nicht erkennen. Großunternehmen mit über 1.000 Mitarbeitern haben dagegen kräftig aufgestockt. Mehr als die Hälfte der Firmen, die über einen Security-Beauftragten verfügen, hat seit 2014 speziell für dieses Aufgabenfeld zusätzliche Mitarbeiter angeworben.

Haben Sie in Ihrem Unternehmen beauftragte Personen für die Security in der Produktion*?



N = 62; *Hierzu zählen auch vor- und nachgelagerte Prozesse wie z.B. Lager- und Logistikprozesse, die von eingesetzten Maschinen und Anlagen im Unternehmen abhängig sind sowie der Entwicklungsprozess für die Produkte bei Herstellern von Maschinen, Fahrzeugen etc.

Abbildung 2 Quelle: VDMA-Report Industrial Security

Organisatorisch ist der Security-Beauftragte mehrheitlich der IT-Abteilung zugeordnet. Besonders Großunternehmen mit mehr als 1.000 Mitarbeitern setzen zu mehr als 90 Prozent auf dieses Modell. In vielen Fällen (57 Prozent) übernimmt der IT-Sicherheitsverantwortliche (ISB/CISO) diese Aufgabe und übt damit eine Doppelfunktion aus. Besonders in Unternehmen mit weniger als 250 Mitarbeitern wird dies praktiziert. Größere Unternehmen können aufgrund der höheren Anzahl von IT-Mitarbeitern eher auf ein Kooperationsmodell setzen und die Aufgaben auf mehrere Schultern verteilen.

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Experten aus IT und Produktion sollten bei Security-Fragen Hand in Hand arbeiten, in beiden Unternehmensbereichen sollte es jeweils einen Ansprechpartner geben. Diese sollten auf gleicher Ebene zusammenarbeiten. Für safety-relevante Fragestellungen sollten entsprechende Experten hinzugezogen werden.
- Die mit dem Thema beauftragte(n) Person(en) sollte(n) sowohl auf Ingenieur- als auch Informatikwissen zurückgreifen können, um eine Adaption von bestehenden Prozessen, Technologien und Lösungen für die Produktionsumgebung zu ermöglichen. Das BSI[2] und die Plattform Industrie 4.0[3] haben entsprechende Dokumente hierzu veröffentlicht.
- Grundlagenwissen für Industrial Security können VDMA-Mitglieder im VDMA Campus bei University4Industry[4] kostenfrei erwerben.
- Durch gestiegene rechtliche Anforderungen in Datenschutz und Datenaustausch (z.B. EU-DSGVO, IT-Sicherheitsgesetz 2.0) raten wir zu einer gemeinsamen Betrachtung von IT-Security und Industrial Security.

2 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_123.pdf

3 https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/i40-security-aus-und-weiterbildung.html

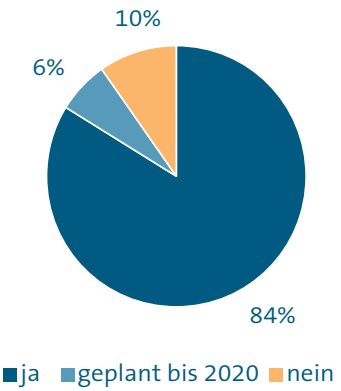
4 https://www.university4industry.com/vdma

4 Einsatz von Security-Richtlinien

Eine Security-Richtlinie beschreibt in kurzen und klaren Worten die internen Vorgaben, Aufgaben und Verantwortlichkeiten eines Unternehmens oder eines Unternehmensbereichs. Die Richtlinie ist ein Management-Dokument, das durch die Geschäftsleitung beschlossen und umgesetzt werden muss. Mit einer verbindlichen Richtlinie soll dabei zunächst das Bewusstsein für die Notwendigkeit und Einhaltung aller der Produktionssicherheit dienenden Maßnahmen gefördert werden. Darüber hinaus ist es erforderlich, dass sie auch ein Mindestmaß von Aufgaben und Pflichten enthält, deren Erfüllung für die Gewährleistung und Aufrechterhaltung eines angemessenen Security-Niveaus unabdingbar ist.

Im Office-Umfeld setzen bereits 84 Prozent der befragten Unternehmen eine Security-Richtlinie ein. Auch wenn es zwischen den verschiedenen Betriebsgrößen noch gewisse Unterschiede gibt, zeigen sich hier bereits eine hohe Sensibilisierung für das Thema und Akzeptanz von notwendigen organisatorischen Maßnahmen.

Gibt es im Unternehmen eine Security-Richtlinie für die Office-IT (E-Mail, Web-Server, etc.)?

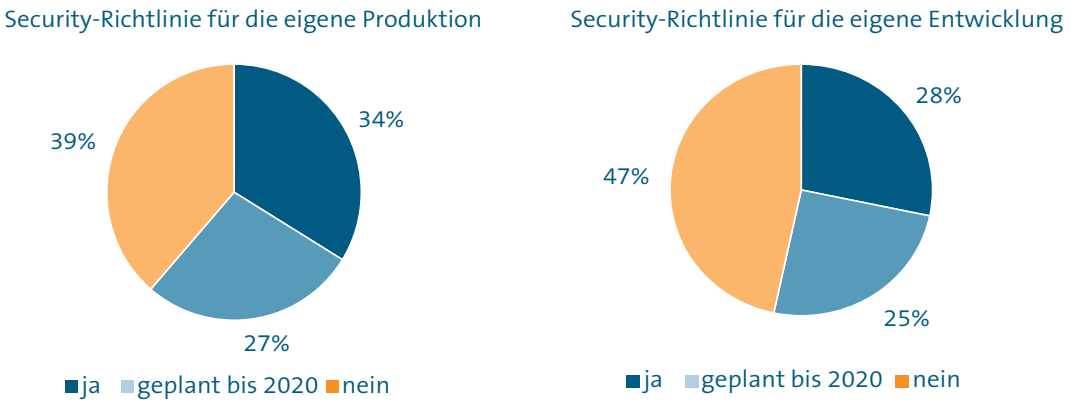


N = 62

Abbildung 3

Quelle: VDMA-Report Industrial Security

Gibt es im Unternehmen eine Security-Richtlinie für die eigene Produktion oder Produktentwicklung?



N = 62

Abbildung 4

Quelle: VDMA-Report Industrial Security

Redaktionstipp

Unternehmen, die bisher noch keine Richtlinie im Büroumfeld haben, können Vorlagen und Dokumente aus dem „VDMA Leitfaden zur Informationssicherheit Teil 2: Informations-Sicherheits-Management-System – ISMS“[5] dafür nutzen.

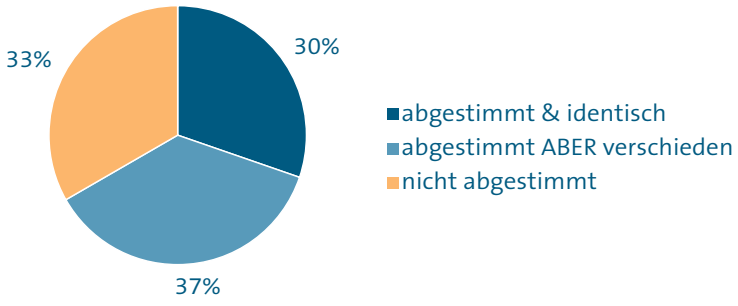
Erwartungsgemäß ist die Verbreitung von Security-Richtlinien im Produktionsumfeld (34 Prozent) und in der Produktentwicklung (28 Prozent) gegenüber dem Office-Umfeld deutlich geringer. Aber der hohe Anteil von geplanten Security-Richtlinien in den Unternehmen bis 2020 lässt hoffen, dass auch in der Produktion und Produktentwicklung die Durchdringung dann auf über 50 Prozent ansteigt. Insbesondere durch die direkten Auswirkungen auf die Kerngeschäftsprozesse der Maschinen- und Anlagenbauer ist eine ganzheitliche Security-Betrachtung wichtig, die sowohl das Office-Umfeld als auch die Produktion und die Produktentwicklung umfasst.

5 http://www.vdmashop.de/Informatik-und-Technik/Leitfaden-zur-Informationssicherheit-Teil-2---download.html

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Die Security-Richtlinie für die Produktion sollte eigenständig und mit der Security-Richtlinie für das Office-Umfeld abgestimmt sein, um sich ggf. zu ergänzen und nicht zu widersprechen.
- Mitarbeiter in der Produktion sollten auf die Bedürfnisse der Produktion angepasste Security-Schulungen erhalten (Kompetenz und Awareness schaffen).
- Security ist ein Prozess. Es sollte schrittweise mit der Einführung begonnen und das Schutzniveau nach und nach gesteigert werden. Für die Erstbetrachtung hat der Arbeitskreis den Fragenkatalog „Industrial Security – Einfach anfangen.“ entwickelt. [6]
- Richtlinien finden ihren Weg in den Arbeitsalltag, wenn sie die Arbeit unterstützen, einfach anwendbar sind und die eigentliche Tätigkeit nicht behindern. Sie sollten daher den Anwendern transparent zur Verfügung stehen, die Anwender sollten geschult sein und sie sollten nach ihren Verbesserungsvorschlägen gefragt werden. Bei Schulungen sollte zudem auf die Hintergründe für Maßnahmen eingegangen und die Notwendigkeit dargelegt werden.

Ist die Security-Richtlinie für die Produktion mit derjenigen für die Produktentwicklung und/oder „Office-IT“ abgestimmt?



N = 33; Hinweis: Hier wurden alle Antworten der Unternehmen, die eine Security-Richtlinie im Einsatz haben bzw. diesen planen, berücksichtigt.

Abbildung 5 Quelle: VDMA-Report Industrial Security

6 https://itatautomation.vdma.org/documents/105867/8303780/VDMA%20Fragenkatalog%20Security_2014_final.pdf

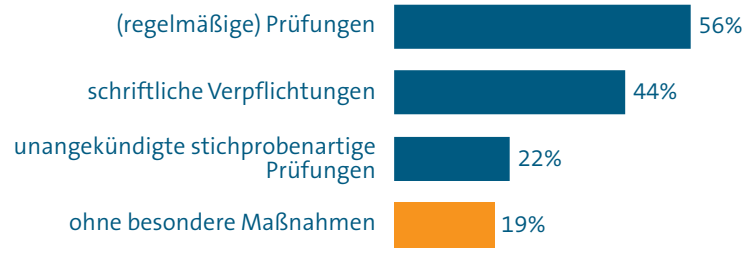
Die Abstimmung von parallel existierenden Security-Richtlinien für Büro- und Produktionsumgebung ist wichtig, damit organisatorische Lücken aufgezeigt sowie Synergieeffekte erzeugt werden und technische Maßnahmen sich ideal ergänzen können. Die Einhaltung dieser Richtlinien sollte ebenfalls regelmäßig geprüft werden.

Sind die Security-Richtlinien für Büroumfeld, Produktion und Produktentwicklung identisch, so ist davon auszugehen, dass ein Großteil der Richtlinien ursprünglich aus dem Büroumfeld stammt. In diesen Fällen enthalten die Richtlinien oft nur wenig spezifische Aspekte für die Security in der Produktion. Dies fällt besonders bei mittelgroßen Unternehmen (251 bis 1.000 Mitarbeiter) auf, die zu mehr als 50 Prozent abgestimmte und identische Richtlinien einsetzen.

Bei rund einem Drittel der Unternehmen sind die Security-Richtlinien immer noch unabgestimmt. Besonders kleine Unternehmen (bis 250 Mitarbeiter) weisen einen Nachholbedarf auf. Für eine gut funktionierende Abstimmung ist die Einbindung aller betroffenen Parteien wichtig, sowohl der Mitarbeiter aus den verschiedenen Unternehmensbereichen als auch des Datenschutzbeauftragten und des Betriebsrats.

Erfreulicherweise zeigt sich bei den Prüfungen zur Einhaltung der Security-Richtlinie für die Produktion ein deutlich positiver Trend. Rund 56 Prozent (2013: 33 Prozent) führen bereits (regelmäßige) Prüfungen durch. Zusätzlich wird dies noch durch schriftliche Verpflichtungen und unangekündigte stichprobenartige Prüfungen unterstützt.

Wie wird die Einhaltung der Security-Richtlinie für die Produktion organisatorisch sichergestellt?



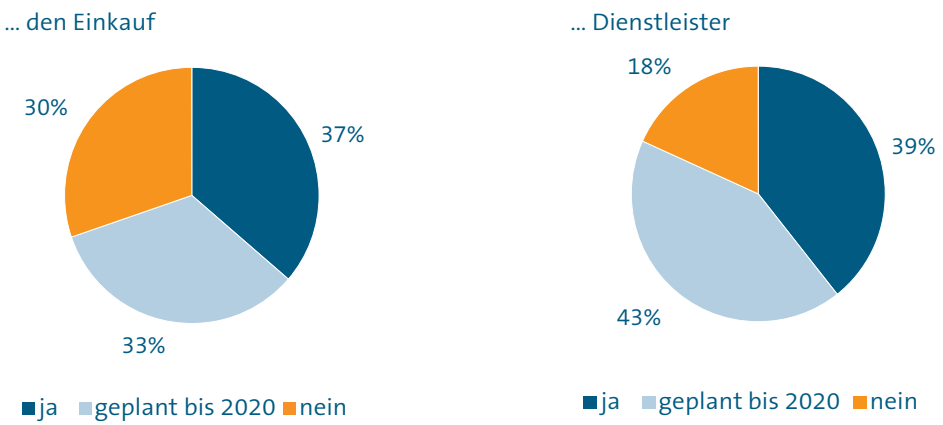
N = 32; Mehrfachnennungen möglich; Hinweis: Hier wurden alle Antworten der Unternehmen, die eine Security-Richtlinie im Einsatz haben bzw. diesen planen, berücksichtigt.

Abbildung 6 Quelle: VDMA-Report Industrial Security

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Die Security-Richtlinien müssen regelmäßig, mindestens jährlich, auf ihre Eignung überprüft werden.
- Richtlinien müssen gelebt werden. Flankierende Maßnahmen für alle Mitarbeiter und ggf. Vertragspartner sind daher notwendig, zum Beispiel regelmäßige Awareness-Schulungen oder Erinnerungen an wichtige Grundsätze und Aspekte der Security-Richtlinie nach Vorfällen.
- Die Eignungsprüfung der Richtlinie kann folgende Punkte umfassen: Aktualität, Vollständigkeit, Umsetzung der Anforderungen, Kompatibilität zwischen IT und Produktion.
- Zur Sensibilisierung sollten zusätzliche unangekündigte Stichproben/Übungen durchgeführt werden, beispielsweise zum Umgang mit mobilen Datenträgern (USB, Laptops), Remote Service, Ransomware, Bring Your Own Device oder Funkschnittstellen in der Fertigung.

Gilt die Security-Richtlinie für die Produktion auch für ...?



N = 33

Abbildung 7

Quelle: VDMA-Report Industrial Security

Redaktionstipp

Der „VDMA Leitfaden zur Informationssicherheit, Teil 1: Mitarbeitersensibilisierung“ gibt wertvolle Anregungen aus der Sicht der Office-IT. [7]

Beim Einkauf von Komponenten, Maschinen oder Anlagen sollten Security-Anforderungen und damit verbundene Risiken mitberücksichtigt werden und zwischen Produktion und IT abgestimmt sein. Zudem gibt es in speziellen Abnehmerbranchen des Maschinenbaus Security-Anforderungen an Zulieferer, die auch für den Einkauf und den Betrieb der eigenen Produktionsanlagen mit Berücksichtigung finden müssen (z.B. TISAX im Automotive-Bereich [8]). Rund 70 Prozent der befragten Unternehmen mit einer Security-Richtlinie haben Security-Anforderungen in ihre Einkaufsbedingungen integriert oder planen die Erweiterung des Geltungsbereiches auf die Beschaffung bis 2020. Darüber hinaus hat die Security-Richtlinie für die Produktion in vielen Unternehmen (rd. 40 Prozent) bereits auch ihre Gültigkeit für externe Dienstleister wie Anlagenhersteller oder Servicetechniker. Bis 2020 wollen dann sogar mehr als 80 Prozent der Unternehmen dies realisieren. Besonders in Bezug auf eine gemeinsame kontinuierliche Weiterentwicklung der Industrial Security ist eine Verbreitung und Anwendung der Richtlinie auch außerhalb des eigenen Unternehmens bei Herstellern und Integratoren vorteilhaft.

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Eine Security-Richtlinie richtet sich vorrangig an Mitarbeiter und errichtet Leitplanken für den sicheren Betrieb. Zudem sollten spezifische Anforderungen an Dienste und Geräte formuliert werden, die mit der Produktion und/oder dem Produktionsnetzwerk temporär in Verbindung stehen (z.B. Fernwartung, Servicetechniker) oder dauerhaft vernetzt sind. Ein Blick in die IEC 62443-2-4 bietet Hilfe bei den Formulierungen der Anforderungen an Dienstleister. [9]
- Security-Richtlinien sind Grundsatzpapiere, die nicht auf Geräteebene heruntergebrochen werden sollten.
- Bei der Auswahl neuer Geräte sowie bei der Planung und Umsetzung von Anlagen sollten Anforderungen der Industrial Security mitberücksichtigt werden (z.B. gemäß Leitfaden „Industrie 4.0 Security“, VDMA-Einheitsblatt 66418 [10] oder IEC 62443).
- Bestehende Produktionsanlagen wurden oft ohne Betrachtung der Security-Anforderungen beschafft. Für diese muss deshalb vor technischen Änderungen eine Risikoanalyse mit Blick auf Security durchgeführt und angemessene Schutzmaßnahmen umgesetzt werden.

7 https://www.vdmashop.de/Informatik-und-Technik/Leitfaden-zur-Informationssicherheit---Teil-1--Sensibilisierung.html

8 https://enx.com/tisax/

9 https://www.vde-verlag.de/standards/1800319/e-din-iec-62443-2-4-vde-0802-2-4-2017-01.html

10 Das VDMA Einheitsblatt 66418 liegt aktuell nur in der Entwurfsversion vor.

5 Risikomanagement

Das Risikomanagement für Industrial Security koordiniert die Risikoanalyse, die Risikoeinschätzung, Risikobewertung und Risikobehandlung der Produktionsumgebung. Da Managementsysteme oftmals einen ähnlichen Aufbau haben ist es sinnvoll, Schnittmengen gemeinsam zu behandeln (QM, Functional Safety Management, Risikomanagement, Informationssicherheitsmanagement etc.).

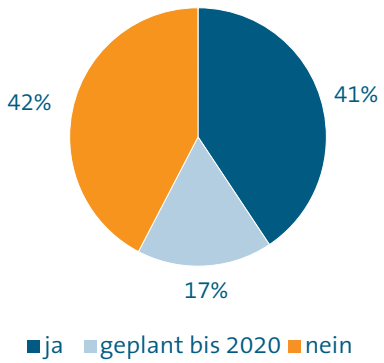
Bisher haben im Durchschnitt 41 Prozent der befragten Unternehmen im Produktionsumfeld ein Risikomanagement eingeführt. Vorreiter sind in diesem Fall die großen Unternehmen (über 1.000 Mitarbeiter) mit 58 Prozent. Einen deutlichen Nachholbedarf zeigen dagegen noch die mittelgroßen Unternehmen (251 bis 1.000 Mitarbeiter). Der heutige Anteil von 26 Prozent soll sich bis 2020 aber verdoppeln.

Auch wenn noch kein vollständiges Risikomanagement etabliert wurde, ist mit einer Risikoanalyse bereits der Anfang gemacht, um die Bedrohungslage besser einschätzen zu können.

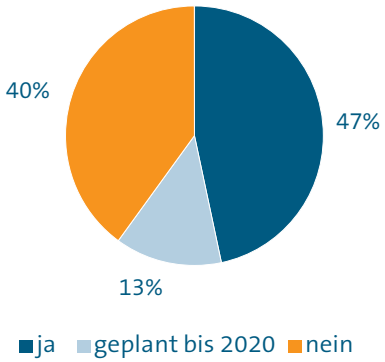
Rund die Hälfte der Teilnehmer (47 Prozent) hat eine entsprechende Analyse schon durchgeführt und verfügt in neun von zehn Fällen über einen vollständigen oder zumindest teilweisen Einblick in die Bedrohungslage für die eigene Produktionsumgebung. Bei den Unternehmen, die ihr Risiko noch nicht eingehender betrachtet haben, ist dagegen nur jeder dritte Teilnehmer der Meinung, dass er die eigene Bedrohungslage vollständig oder teilweise kennt.

Risikomanagement und Risikoanalyse

Ist im Produktionsumfeld des Unternehmens ein Risikomanagement etabliert?



Wurde eine Risikoanalyse im Unternehmen durchgeführt?



N = 59 (60)

Abbildung 8

Quelle: VDMA-Report Industrial Security

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Die Standardreihe ISO 31000 stellt die Basis für eine strukturierte Etablierung und den Betrieb eines Risikomanagements dar. Sie enthält die notwendigen Hilfestellungen zur Analyse, Schadensbegrenzung, vorbeugenden Risikoabwehr und zum Berichtswesen zu übergeordneten Managementsystemen. Zum Beispiel kann für die Risikoanalyse die ISO 31010 herangezogen werden.
- Der BSI Grundschutz bietet mit dem 2017 neu veröffentlichten Baustein „IND: Industrielle IT“ eine Betrachtung typischer Gefährdungen und deren Behandlung. [11]
- Risiken müssen für die Büro- und die Produktionsumgebung aufgrund Ihrer Spezifika getrennt voneinander betrachtet und bewertet werden. Nur so lassen sich spezifische Maßnahmen adäquat ableiten, betreiben und pflegen. Für safety-relevante Fragestellungen sollten entsprechende Experten hinzugezogen werden.

11 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_2_4_Maschine.html

6 TOP 10 Bedrohungen

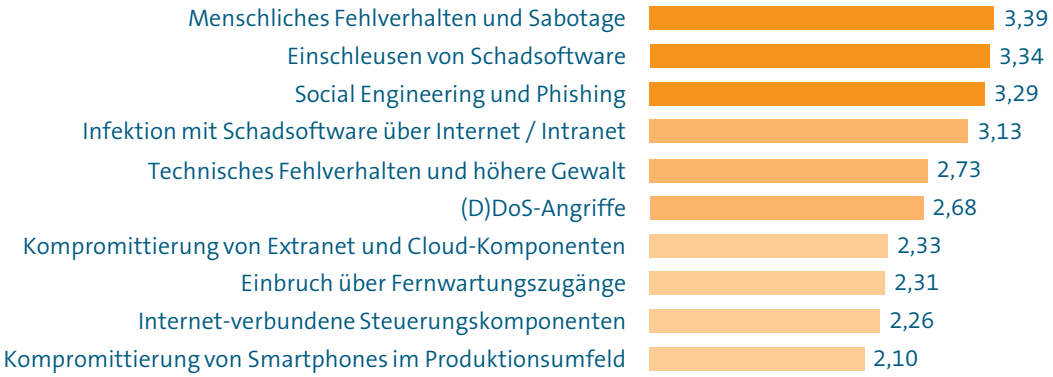
Ausgehend von dem im Jahr 2016 veröffentlichten Dokument des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die „TOP 10 Bedrohungen für Industrial Control Systems“ wurden die Teilnehmer zu einer Einschätzung des Eintritts der aufgeführten Bedrohungen im eigenen Unternehmen aufgefordert. Die subjektiv wahrgenommene Bedrohungslage bei den befragten Unternehmen ergibt im Vergleich zur allgemeinen Einordnung des BSI erneut ein differenziertes Bild.

Das BSI sieht auf den vordersten Plätzen folgende fünf Bedrohungen (höchste zuerst):

- Social Engineering und Phishing
- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Einbruch über Fernwartungszugänge
- Menschliches Fehlverhalten und Sabotage

Die befragten Unternehmen schätzen die Bedrohungslage im Durchschnitt eher als „mittel“ ein. Den höchsten Wert mit rund 3,4 erreicht dabei „Menschliches Fehlverhalten und Sabotage“. Je nach Unternehmensgröße zeigt sich allerdings eine unterschiedliche Beurteilung der Bedrohungslage. Die Einschätzung der Bedrohungslage ist dabei sowohl von verfügbaren Schutztechnologien als auch unternehmensspezifischen Erfahrungen abhängig. Insofern stellt die vorliegende Beurteilung der TOP 10 Bedrohungen eine gewichtete Bewertung der Risiken dar.

Wie schätzen Sie die Eintrittswahrscheinlichkeit für folgende Bedrohungen im Unternehmen ein?



N = 60 bis 62; Weitere Erläuterungen zum Thema sind im BSI-Dokument vom 01.08.2016 zu finden [12]

Abbildung 9 Quelle: VDMA-Report Industrial Security

12 https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news_ICS_top10_update_24082016.html

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Da die größte Sorge offensichtlich die menschlichen Faktoren betrifft, sind organisatorische Maßnahmen, allen voran Schulungen, als wichtigste Maßnahmen zu erkennen.
- Organisatorische Maßnahmen allein reichen nicht aus. Diese sollten durch technische Vorkehrungen unterstützt werden.
- Aktuell verfügbare Hardening-Methoden in Betriebssystemen zur Erkennung von Schadcode (White-/Blacklisting) reichen nicht aus. Der Einsatz technischer Kontrollen (Monitoring, Anomaly Detection) oder Isolationsmaßnahmen sowohl an Netzwerkübergängen zwischen IT und Produktion als auch bei der Anbindung von Fremdgeräten (Techniker-Laptop für Wartungszwecke und Fernwartungszugängen) ist zu prüfen.

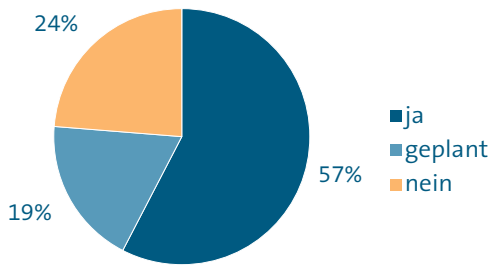
7 Security-Vorfälle

Dass die Anzahl der Security-Vorfälle in Zukunft zurückgeht, ist für die Mehrheit der Studienteilnehmer unwahrscheinlich. Mehr als 90 Prozent der befragten Unternehmen erwarten ein gleichbleibendes oder ansteigendes Niveau. Mit einer wachsenden Anzahl von Vorfällen gehen auch negative Auswirkungen einher, die die Maschinen- und Anlagenbauer bereits heute in mehr als zwei Dritteln aller Fälle verzeichnen.

Die aktuell von den Unternehmen angegebenen Vorfälle spiegeln mit hoher Wahrscheinlichkeit nicht die tatsächliche Anzahl an Vorkommnissen wieder. Denn erst 57 Prozent der Teilnehmer haben Maßnahmen ergriffen, um Security-Vorfälle zu erkennen. Neben der Tatsache, dass aus Compliance-Gründen oder der Angst vor Imageverlust eine Entscheidung gegen die Meldung von Security-Vorkommnissen gefällt wird, können Unternehmen auch nur Vorfälle angeben, die entdeckt wurden. Zudem ist nicht immer klar, ob ein entsprechender Security-Vorfall vorliegt - es fehlt an klaren Definitionen.

Im Vergleich zu 2013 sind mit 47 Prozent vorrangig erstmals zufällige externe Einflüsse (z.B. durch ungerichtete E-Mails mit Viren, WannaCry, Phishing) für Security-Vorfälle verantwortlich gewesen. Besonders mittlere Unternehmen (251 bis 1.000 Mitarbeiter) waren in den vergangenen zwei Jahren davon stark betroffen. Auf den Plätzen folgen als Ursachen die „Innentäter“ mit 38 Prozent und die gezielten externen Einflüsse mit 26 Prozent. Letztere konnten mehrheitlich durch die Unternehmen nicht zurückverfolgt werden. Ein Grund mag darin liegen, dass bei knapp der Hälfte der betroffenen Unternehmen (45 Prozent), die gezielt „attackiert“ wurden, keine externen Beratungsstellen wie Verfassungsschutz, spezialisierte Sicherheitsdienstleister oder Polizeibehörden hinzugezogen wurden.

Haben Sie Maßnahmen in Ihrem Unternehmen ergriffen, um Security-Vorfälle zu erkennen?



N = 47

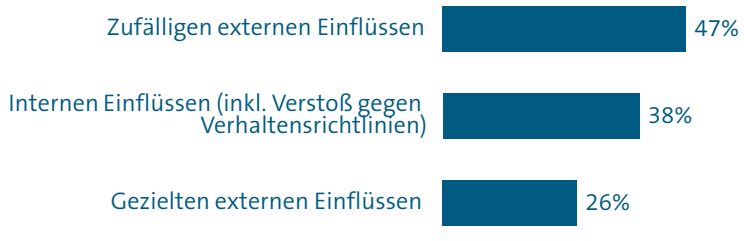
Abbildung 10 Quelle: VDMA-Report Industrial Security

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat 2012 unter anderem für den Austausch von Meldungen zu Security-Vorfällen die „Allianz für Cybersicherheit“ gegründet. Auch wenn diese zentrale Meldestelle mittlerweile deutlich bekannter geworden ist (2013: 39 Prozent, 2019: 70 Prozent), hat dort bisher nur ein kleiner Anteil der Unternehmen (7 Prozent) entsprechende Vorfälle gemeldet. Zumeist wurden von den Studienteilnehmern fehlende relevante Vorfälle als Begründung angeführt.

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Netzwerküberwachungsmaßnahmen (z.B. IDS) und eine regelmäßige Auswertung von Logfiles sind empfohlen. Detektionsmaßnahmen führen zu höheren Entdeckungsraten von Angriffen. Dies bedeutet somit einen höheren organisatorischen Aufwand für die Behandlung der entdeckten Angriffe.
- Es muss sowohl geschultes Personal als auch ausreichend Zeit für die Erkennung und Behandlung von Vorfällen zur Verfügung stehen.
- Beim Umgang mit Security-Vorfällen können externe Beratungsstellen hinzugezogen werden. Folgende unabhängige Stellen können wir empfehlen:
  - Zentrale Ansprechstellen Cybercrime (ZAC) der Polizeien der Länder und des Bundes für die Wirtschaft [13]
  - Allianz für Cybersicherheit (ACS)[14]
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)[15]
  - Landesämter und Bundesamt für Verfassungsschutz [16]

Haben Sie Security-Vorfälle im Unternehmen in den vergangenen zwei Jahren aufgrund von ... identifiziert?



N = 47

Abbildung 11 Quelle: VDMA-Report Industrial Security

13 https://www.bka.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
14 https://www.allianz-fuer-cybersicherheit.de
15 https://www.bsi.bund.de
16 https://www.verfassungsschutz.de/de/service/landesbehoerden

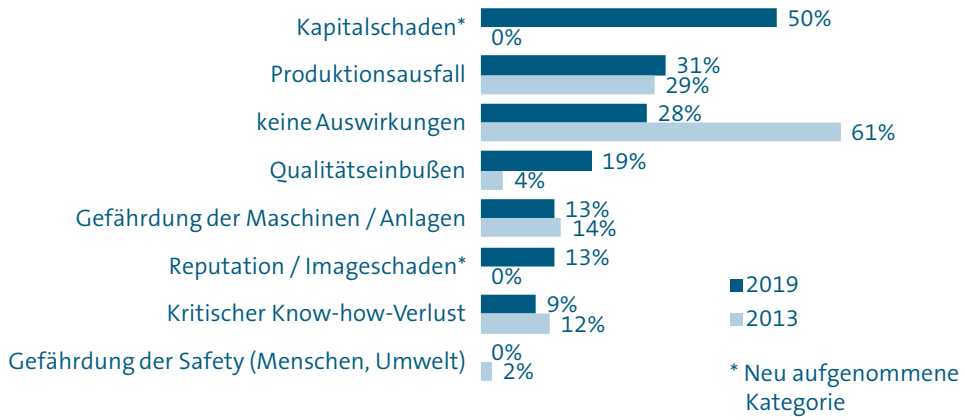
Treten Security-Vorfälle ein, dann sind die Auswirkungen oft weitreichend. So werden bei jedem zweiten Unternehmen bereits heute entsprechende Kapitalschäden verursacht. An zweiter und dritter Stelle folgenden mit 31 Prozent der Produktionsausfall und mit 19 Prozent Qualitätseinbußen. Auch Imageschäden haben 13 Prozent der Unternehmen in diesem Zusammenhang schon erlitten. Positiv ist allerdings, dass es in den vergangenen Jahren keinen Safety-Vorfall gab, der auf einen Security-Vorfall zurückzuführen ist.

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Jeder (mögliche) Vorfall verursacht einen Schaden. Deshalb ist es wichtig zu ermitteln, wie hoch die schadhaften Auswirkungen sind und wie wahrscheinlich ein (wiederholtes) Auftreten ist. Insbesondere der Schutz des für das eigene Unternehmen geschäftskritischen Know-hows (z.B. Konstruktionsdaten, Kostenkalkulation, Rezepturen, Quellcode) als auch die Aufrechterhaltung des Geschäftsbetriebs sollten im Vordergrund stehen.
- Risiken sind individuell. Eine pauschale Betrachtung mit vorgefertigten Tabellen wird nur eingeschränkt zur Absicherung des Unternehmens beitragen. Diese können jedoch helfen den richtigen Weg vorzubereiten. Als hilfreich für die Risikobetrachtung der eigenen Produktionsumgebung gilt die IEC 62443-2-1 sowie die IEC 62443-2-4.
- Werden Systeme unverändert über längere Zeiträume betrieben, können diese unsicher werden, z.B. durch entdeckte Schwachstellen in Betriebssystem oder Anwendungssoftware. Es besteht daher die Verantwortung des Betreibers, Systeme aktuell zu halten. Dazu sollten Systemverantwortliche Hinweise zu Schwachstellen (Advisories) von Herstellern und Dienstleistern einfordern.
- Informationen über Schwachstellen und deren Behebung liefern CERTs. Industrienah sind dabei das ICS-CERT [17] (USA), CERT@VDE [18] (D) oder CERTs von VDMA-Mitgliedern wie Siemens [19], Draeger [20], KRONES [21], etc.
- Systemverantwortliche sind darauf zu verpflichten, regelmäßige Prüfungen nach Advisories (Warnungen) aus vertrauenswürdigen Quellen vorzunehmen. Werden bekannte Schwachstellen von Herstellern nicht „geschlossen“, so müssen andere Maßnahmen ergriffen werden, um Risiken für den eigenen Geschäftsbetrieb zu minimieren (z.B. Virtualisierung, Kapselung, Deaktivierung, Wechsel des Produkts/Anbieters).
- Eine aktive Mitarbeit in Austauschgruppen zu geschäftskritischen Anwendungen ist empfohlen. Dies können User Groups, Herstellerforen oder Security-Veranstaltungen sein. Der VDMA bietet hierzu Arbeitskreise und Erfahrungsaustausche an. Weitere Informationen sind zu finden unter: **industrialsecurity.vdma.org**

17 https://ics-cert.us-cert.gov
18 https://cert.vde.com/de-de
19 https://www.siemens.com/global/de/home/produkte/services/cert.html
20 https://static.draeger.com/security/
21 https://shop.krones.com/shop/de/de/securitypatchdownloadformpage

Wie haben sich die Security-Vorfälle ausgewirkt?



N = 32; Mehrfachnennungen möglich

Abbildung 12

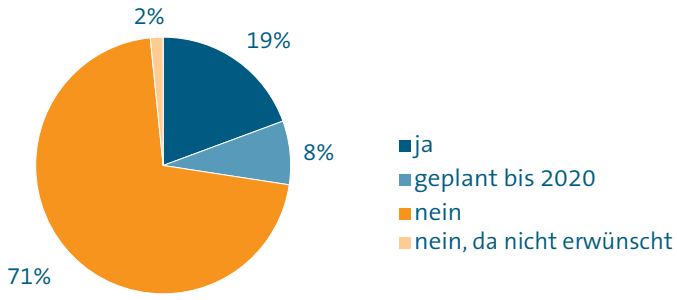
Quelle: VDMA-Report Industrial Security

Trotz der zahlreichen, vor allem auch finanziellen Auswirkungen gibt es nur wenige Unternehmen (19 Prozent), die eine Berechnung oder Abschätzung der Ausfallkosten bei Security-Vorfällen vornehmen. Dies liegt fast nie daran, dass eine Ermittlung nicht gewünscht wäre, sondern hat andere Gründe:

- fehlende Ressourcen,
- mangelndes Wissen oder
- systematische Schwierigkeiten.

In der Praxis ist es einfacher, Schäden qualifiziert darzustellen als diese zu quantifizieren, zumal Folge- bzw. Parallelkosten durch „Kollateralschäden“ nur schwer zu beziffern sind.

Gibt es in Ihrem Unternehmen eine Berechnung/Abschätzung zu Ausfallkosten bei Security-Vorfällen (z.B. Kosten pro Ausfallstunde)?



N = 62

Abbildung 13

Quelle: VDMA-Report Industrial Security

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Ausfallkosten sollten nicht in das Security-Budget einfließen. Das Budget sollte insbesondere die Aufwendungen für den Erhalt des Geschäftsbetriebs umfassen. Ausfallkosten entstehen pro Vorfall und können ähnlich wie Elementarschäden durch Versicherungen abgedeckt werden. Hilfestellung für maschinenbauspezifische Anforderungen bietet hierzu die VSMA [22].
- Hauptanliegen nach einem Systemausfall ist ein schneller Wiederanlauf bzw. eine schnelle Wiederherstellung eines vertrauenswürdigen Zustands. Diese Resilienz lässt sich mit Hilfe einer Business Impact Analyse (BIA) aufwandsbezogen berechnen und optimieren. Aus Security-Sicht ist es zudem wichtig, ob der Vorfall ein einmaliges oder sich wiederholendes Ereignis darstellt. Sich wiederholende Ereignisse wirken sich auf das Security-Budget aus.
- Zudem sind nicht nur die direkten Aufwände eines möglichen Produktionsausfalls (z.B. vorfallinitiierter Stopp, Wiederinbetriebnahme), zu betrachten, sondern auch mögliche Aufwände für die Ursachenfeststellung und -beseitigung zu beziffern.
- Für die langfristige Betrachtung sollte ein Notfallkonzept/-plan erstellt, eingeführt und gepflegt werden. Hilfestellung bietet dafür der BSI-Standard 100-4 „Notfallmanagement“ [23].

22 https://www.vsma.de/vdma-branchenloesungen/vdma-cyberpolice/

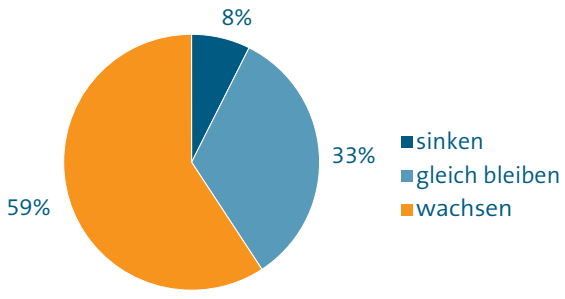
23 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html

Mit der zunehmenden Vernetzung und Digitalisierung in den Unternehmen werden auch Security-Vorfälle weiter zunehmen. Bei den befragten Großunternehmen (über 1.000 Mitarbeiter) rechnen 82 Prozent damit, dass sie zukünftig verstärkt mit entsprechenden Vorfällen konfrontiert werden. Demgegenüber sehen bei den kleinen Unternehmen (bis 250 Mitarbeiter) allerdings nur 33 Prozent der Teilnehmer diese Tendenz – die Mehrheit „hofft“ auf ein gleichbleibendes Niveau. Um diesem Trend entgegenzuwirken sind organisatorische und technische Maßnahmen erforderlich.

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Zunächst sollten Security-Vorfälle beispielsweise mit Hilfe von technischen Maßnahmen (z.B. IDS, Anomalie Detection) zuverlässiger erkannt werden. Dies führt zwangsläufig zu einem Anstieg der erkannten Security-Vorfälle. Dadurch ist eine Anpassung von bereits erfolgten Risikoeinschätzungen notwendig. Bestehende Maßnahmen sind den neu bewerteten Risiken anzupassen, so dass langfristig die Anzahl der Security-Vorfälle reduziert werden kann.
- Strategie und Schutzmaßnahmen müssen regelmäßig überprüft werden, um neue Bedrohungen zu erkennen und Schwachstellen nicht erst nach dem nächsten Schadensfall zu schließen. Insbesondere mit dem Internet verbundene Komponenten und Systeme sollten dahingehend dauerhaft überwacht werden.

Wird sich die Anzahl der Security-Vorfälle in Ihrem Unternehmen verändern?



N = 54

Abbildung 14 Quelle: VDMA-Report Industrial Security

- Internet-basierte Dienste (z.B. Shodan), in denen eigene Systeme, Anwendungen und IP-Adressen hinterlegt werden können, stellen eine gute Unterstützung dar. Auch die Überwachung von Common Vulnerability Scoring Systems (z.B. NIST NVD) ist empfohlen, insbesondere bei der Nutzung von Open Source Software.
- Die Überwachung der unternehmenseigenen E-Mail-Konten lässt sich zuverlässig, sicher und kostenfrei unter Einbindung des Dienstes „Have I Been Pwned“ von Troy Hunt realisieren.[24]
- Security-Experten sind weltweit gefragt. Es ist daher für viele VDMA-Mitglieder schwierig, offene Stellen adäquat zu besetzen. Daher sollten Unternehmen auf gezielte Aus- und Weiterbildungen für Security Wert legen. Eine Möglichkeit Basiswissen aufzubauen, stellen die digitalen Lernmodule von University4Industry [25] dar. Die Module richten sich sowohl an Experten als auch Einsteiger und wurden gemeinsam mit dem VDMA Arbeitskreis Industrial Security entwickelt.
- Der Aufbau von Security-Know-how kann auch für das sichere Design von Industrie 4.0-fähigen Maschinen und Anlagen genutzt werden. Für Security-Verantwortliche ein nicht zu unterschätzender Vorteil bei Budget-Verhandlungen.
- Das MBI erarbeitet gemeinsam mit wissenschaftlichen Instituten eine Schulung für Produktentwickler der Maschinen- und Anlagenbauer. Wir informieren Sie gerne darüber.[26]
- Insbesondere für größere Unternehmen stellt ein ISMS für die Produktionsumgebung den „Königsweg“ dar. Für mittelständische Unternehmen ist es im Gegensatz dazu wichtig, überhaupt mit Industrial Security zu beginnen. Die oben genannten Maßnahmen sind erste Anregungen das Richtige zu tun. Dauerhaft betrachtet, ist die IEC 62443-2-1 die erste Wahl:
  - Maßnahmen zur Erkennung von Security-Vorfälle etablieren.
  - Systematisches Vorgehen nach PDCA (Plan-Do-Check-Act).
  - Regelmäßige Überprüfung von Strategie und Schutzmaßnahmen.
  - Aufbau von Kompetenz und Know-how.

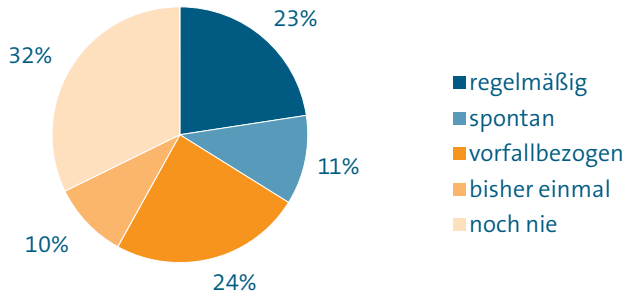
24 https://haveibeenpwned.com/DomainSearch
25 https://www.university4industry.com/vdma
26 Melden Sie sich hierzu bitte bei Frau Catherine John, Maschinenbau-Institut GmbH, catherine.john@vdma.org

8 Security-Prüfung im Maschinen- und Anlagennetzwerk

Die vorhandenen Systeme (Maschinen, Anlagen, Netzwerk) sind bestmöglich zu dokumentieren und regelmäßig zu aktualisieren. Eine entsprechende Security-Prüfung der Anlage im Vergleich zur Dokumentation stellt außerdem sicher, dass die organisatorischen und technischen Maßnahmen noch zur Maschine bzw. Anlage passen.

Trotz einer vorhandenen Security-Richtlinie für die Produktion überprüfen noch zu wenig Unternehmen die Security im Maschinen- und Anlagennetzwerk regelmäßig (23 Prozent). Sowohl vorfallbezogene (24 Prozent) und spontane Prüfungen (11 Prozent), als auch einmalige Prüfungen deuten eher auf Reaktion statt Aktion hin. Eine Richtlinie darf jedoch kein Alibidokument sein. Eine einfache Übernahme von Security-Prüfungen aus dem Büroumfeld ist ungeeignet, die Prüfungen müssen an die Anforderungen der Produktion angepasst werden. Die Auswahl des richtigen Test-Partners ist dabei von größter Bedeutung.

In welchen Abständen wird die Security im Maschinen- und Anlagennetzwerk überprüft?



N = 62

Abbildung 15

Quelle: VDMA-Report Industrial Security

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Industrial Security orientierte Tests, die die Robustheit der Maschine oder Anlage zum jeweiligen Testzeitpunkt belegen (z.B. Penetration Tests), machen nur vor deren Auslieferung an Kunden oder in dafür kontrollierten Umgebungen im Einsatz Sinn. Diese Tests sind auch eine Aufgabe im Sinne der Richtlinie VDI/VDE 2182 (Informationssicherheit in der industriellen Automation) sowie IEC 62443.
- Tests von Maschinen und Anlagen im laufenden Betrieb sollten grundsätzlich unterlassen werden, da diese häufig zu ungeplanten Stillständen oder teilweise Safety-Gefährdungen führen. Schwachstellen- oder Port-Scans sind eingeschränkt möglich, sollten aber mit Hersteller und Betriebsverantwortlichen abgestimmt werden.
- Regelmäßige Prüfungen des Sicherheitsniveaus bestehen aus:
  - Technischem Audit
  - Social Engineering Test
  - Code Review
  - Schwachstellenanalyse
  - Logfile-Analyse
  - Integritätsprüfung von Soft- und Hardware
- Suchen Sie sich Partner, die entsprechende Erfahrungen im Bereich Industrial Security vorweisen können. Der VDMA Fachverband Software und Digitalisierung bietet dazu im Branchenführer „Mehrwert durch Software“ eine Übersicht an.[27]

27 https://sud.vdma.org/viewer/-/v2article/render/21090253

9 Organisatorische Schutzmaßnahmen

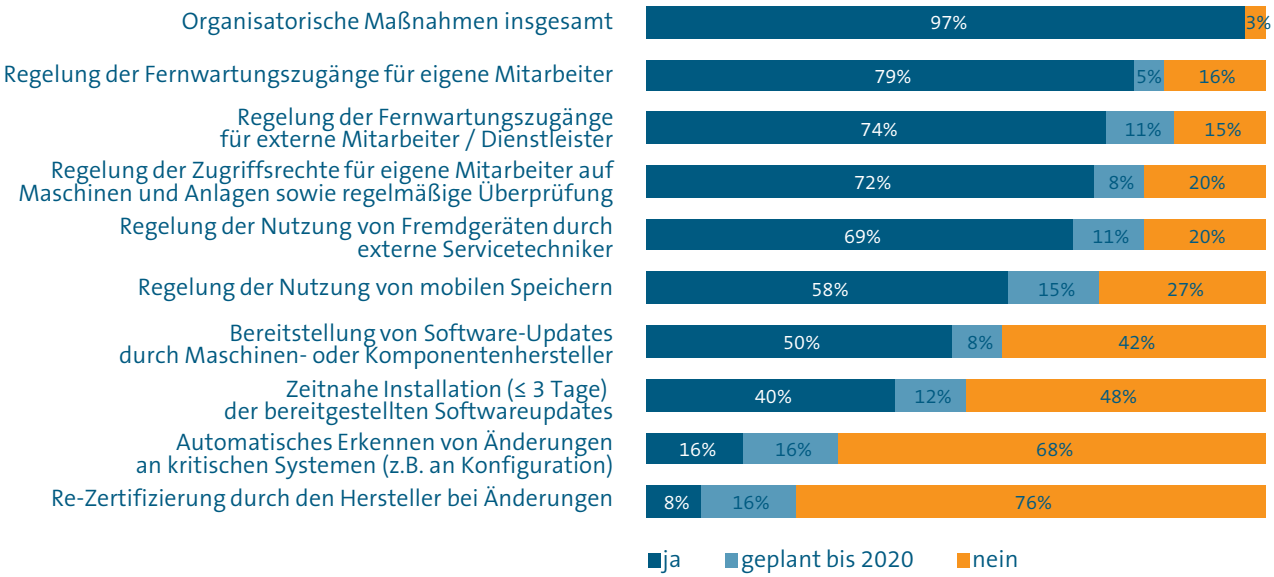
Organisatorische Maßnahmen sind die Grundvoraussetzung, um menschliches Fehlverhalten im gesamten Lebenszyklus einer Anlage zu minimieren und somit Fehler zu vermeiden. Für spezielle Bereiche, in denen konkrete Regelungen notwendig sind, müssen gegebenenfalls gesonderte Richtlinien und Maßnahmen genutzt werden. Außerdem führen organisatorische Maßnahmen meist mit geringerem Aufwand zu einem höheren Nutzen als technische Maßnahmen.

Bereits 97 Prozent der Unternehmen wenden organisatorische Maßnahmen an. Dabei ist ein breites Spektrum an Sicherheitsmaßnahmen in Gebrauch (siehe Abbildung 16). Die jeweiligen Aktivitäten sollten dabei in Relation zur unternehmensspezifischen Bedrohungslage stehen.

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Alle Mitarbeiter sollten auf die Einhaltung von organisatorischen Schutzmaßnahmen verpflichtet werden. Das gilt auch für externe Dienstleister, mit denen entsprechende vertragliche Vereinbarungen geschlossen werden.
- Die Einhaltung der organisatorischen Regelungen sollte regelmäßig geprüft und bei schwerwiegenden Vorfällen sanktioniert werden. Insbesondere Führungskräfte sollten ihrer Vorbildfunktion gerecht werden und keine Sonderrechte erhalten.
- Für die Einhaltung der organisatorischen Schutzmaßnahmen sind den Verantwortlichen und Betroffenen genügend Ressourcen (Zeit, Budget) zur Verfügung zu stellen, insbesondere für den Erhalt der Kompetenz und die Anpassung an veränderte Rahmenbedingungen.

Welche organisatorischen Maßnahmen wurden ergriffen, um sich vor Security-Vorfällen in der Produktion zu schützen?



N = 58 bis 62

Abbildung 16

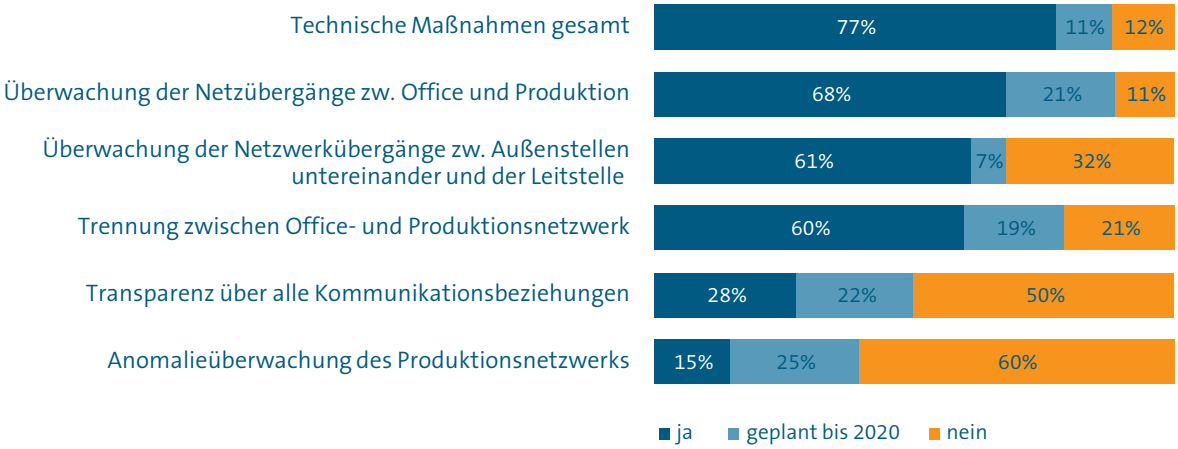
Quelle: VDMA-Report Industrial Security

10 Technische Schutzmaßnahmen

Technische Maßnahmen zum Schutz von Produktion, Maschinen und Anlagen dienen der Unterstützung von organisatorischen Maßnahmen, können diese jedoch nicht ersetzen. Schwierig ist zudem, dass gängige Maßnahmen der IT-Sicherheit in der Produktionsumgebung oft nicht direkt angewendet werden können.

Beim Einsatz der technischen Maßnahmen zeigt sich ein etwas diffuses Bild. Fast 80 Prozent der Unternehmen nutzen bereits technische Maßnahmen, aber typische Maßnahmen, wie die Trennung zwischen Office- und Produktionsnetzwerk, werden erst bei 60 Prozent der Teilnehmer angewandt. Insgesamt zeigen die Antworten jedoch, dass ein breites Spektrum an Sicherheitsmaßnahmen in Gebrauch oder für die Zukunft geplant ist. Da Umsetzung und Betrieb technischer Maßnahmen sowohl die Office-IT als auch die Produktions-IT betreffen, ist eine Abstimmung zwischen beiden Bereichen besonders wichtig.

Welche technischen Maßnahmen wurden ergriffen, um sich vor Security-Vorfällen in der Produktion zu schützen?



N = 58 bis 62

Abbildung 17

Quelle: VDMA-Report Industrial Security

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Die Segmentierung der Netze und Absicherung der Schnittstellen sollten Standardmaßnahmen sein.
- Alle Übergänge zu anderen Netzen sollten bekannt sein und kontrolliert werden, besonders auch die „Turnschuhschnittstellen“ (= temporäre Überbrückung der Air-Gaps).
- Netzwerktopologien sollten dokumentiert und regelmäßig aktualisiert werden.
- Die Kompetenz der mit der Netzwerksicherheit befassten Personenkreise muss sichergestellt sein. Bei der Einstellung von System-Administratoren sollte darauf geachtet werden, dass diese Schulungsnachweise zur Industrial Security vorlegen. Anerkannte Zertifikate für den Bereich der IT-Security sind u.a. CISSP, CISM, CISA, TISP. Weiterbildungen für spezifische Systemfragen bieten z.B. das SANS-Institut, die Fraunhofer Academy, University-4Industry und die Allianz für Cybersicherheit.
- Die Netzwerksicherheit muss als ganzheitliches Problem verstanden werden, welches durch Lösungen bestehend aus Hardware, Software, Maßnahmen und Beratung permanent und immer wieder überprüft werden muss.
- Häufig werden die Ressourcen nur in die Überwachungsmaßnahmen investiert. Dabei reicht es nicht, nur in die technischen Voraussetzungen zu investieren, sondern es müssen auch Ressourcen für Konfiguration, Auswertung und angemessene Reaktion auf Vorfälle eingeplant werden.
- Technische Maßnahmen unterstützen und ergänzen organisatorische Maßnahmen. Technische Maßnahmen bedürfen auch der Systemunterstützung für den gesamten Nutzungszeitraum der Anlage (z.B. Logfiles, Patches müssen zur Verfügung stehen).

11 Security-Standards

Derzeit gibt es eine große Anzahl an länder- und branchenspezifischen Normen, Richtlinien und Empfehlungen zur Security. Auch wenn keines dieser Papiere einen rechtlich verpflichtenden Status hat, so bilden sie doch den Stand der Technik ab und können in vertraglichen Vereinbarungen herangezogen werden. Normen und Standards haben im Maschinen- und Anlagenbau eine große Bedeutung. Der Maschinenbau als Integrator von Komponenten, komplexen Maschinen und Anlagen ist dabei auf das standardisierte Zusammenspiel der einzelnen Komponenten angewiesen.

Im Rahmen der Studie wurden folgende Standards abgefragt:

ISO/IEC 27000er Reihe
Die Normenreihe besteht aus mehreren Teilen (bisher mehr als zwanzig Dokumente), die ein Managementsystem der Informationssicherheit beschreiben. Sie bleibt jedoch sehr abstrakt und generisch. Eine Definition der zu schützenden Werte und die darauf basierende Risikoanalyse wird von den Unternehmen im Rahmen der ISO/IEC 27001 (Basisdokument) selbst durchgeführt. Die ISO 27001 und 27002 wurden zuletzt im Jahr 2013 überarbeitet. [28]

BSI Grundschutz
Der IT-Grundschutz des BSI [29] bietet eine für KMU bewährte Herangehensweise und eine umfangreiche Sammlung an Anforderungen und Umsetzungshinweisen. Diese können auch für eine Risikoanalyse herangezogen werden. In der aktuellen Fassung als „IT-Grundschutz-Kompendium“ wurden erstmals spezifische Bausteine für industrielle Komponenten (IND) [30] hinzugefügt.

VDI/VDE 2182
Ein möglichst knapp gehaltener Leitfaden, der ein allgemeines Vorgehensmodell beschreibt. Im Zentrum steht die Betrachtung der Sichtweisen von Hersteller, Integrator und Endanwender. Sechs Beispielblätter beschreiben diese drei Perspektiven jeweils für die Prozessautomation und die Fabrikautomation. Das Vorgehensmodell wird in die IEC 62443 integriert.[31]

IEC 62443
Ein sehr ausführliches komplexes Werk, das vollumfänglich die Sichtweisen aller Beteiligten der Security in der Automation betrachtet (Hersteller, Integrator, Betreiber, Dienstleister). Teile dieses Standards sind bereits veröffentlicht, andere in der Veröffentlichung und wiederum andere bereits veraltet. Der VDMA hat zur IEC 62443 einen Leitfaden veröffentlicht.[32] Die IEC Standardreihe wird als Grundlage für Security im Bereich Industrie 4.0/IoT angesehen und ist in Teilen bereits zertifizierbar (Produkte, Prozesse).[33]

Gegenüber 2013 ist es erfreulich, dass die Bekanntheit von Security-Standards (2013: 57 Prozent, 2019: 83 Prozent) deutlich zugenommen hat. Nachholbedarf zeigt sich allerdings noch bei der Anwendung der Standards. Lediglich rund 40 Prozent der Unternehmen nutzen einen der oben genannten Standards in der Praxis. Nach wie vor besteht das Problem, dass es für den Maschinen- und Anlagenbau nicht den EINEN Security-Standard gibt. Wenn ein Unternehmen technische und organisatorische Maßnahmen nutzt, sollten sich diese aber an standardisierten Vorgehensweisen orientieren.

28 https://www.iso.org/isoiec-27001-information-security.html

29 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

30 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_Uebersicht_node.html

31 https://www.vdi.de/technik/fachthemen/mess-und-automatisierungstechnik/richtlinien/

32 https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/vdma-security-automation.html

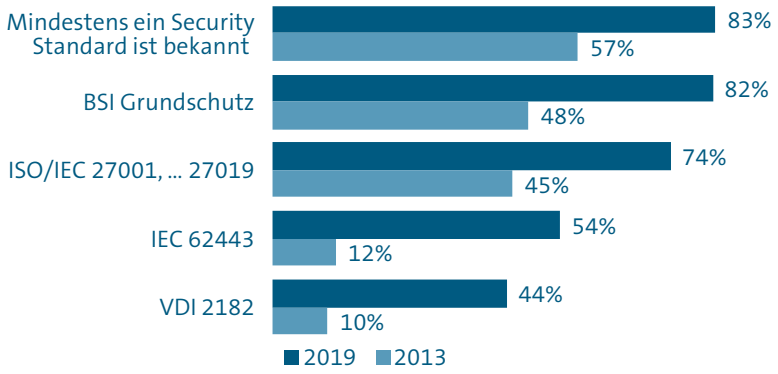
33 https://www.dke.de/de/themen/it-security/it-sicherheit-in-der-automation

Die höchste durchschnittliche Durchdringung in der Anwendung verbuchen mit 30 Prozent der BSI IT-Grundschutz und mit 26 Prozent die ISO/IEC-27000er-Reihe. Bei Unternehmen mit weniger als 250 Mitarbeitern wenden bisher jedoch nur 6 Prozent der Studienteilnehmer einen der beiden Standards an. Vor allem die mangelnde Kenntnis über Standards verhindert in kleineren Unternehmen oft noch eine entsprechend höhere Nutzung.

Der IT-Security-basierte Standard BSI IT-Grundschutz hat den Vorteil einer bereits integrierten allgemeinen Risikobetrachtung und spezielle Bausteine für Maschinen und Anlagen. Die ISO 27000er-Reihe ist international weit verbreitet und wird häufig von Großkunden verpflichtend eingefordert. Darüber hinaus ist sie in bestehende Risikomanagementsysteme gut integrierbar.

Die IEC 62443 ist als internationaler Security-Standard für industrielle Automations- und Steuerungssysteme (IACS) zwar teilweise noch in Erarbeitung, stellt aber aus Sicht des VDMA Arbeitskreises Industrial Security die zukünftige Grundlage für Industrial Security dar. Unternehmen ist es daher angeraten, sich intensiv mit diesem Standard zu befassen.

Welche IT-Security Standards sind Ihnen bekannt?



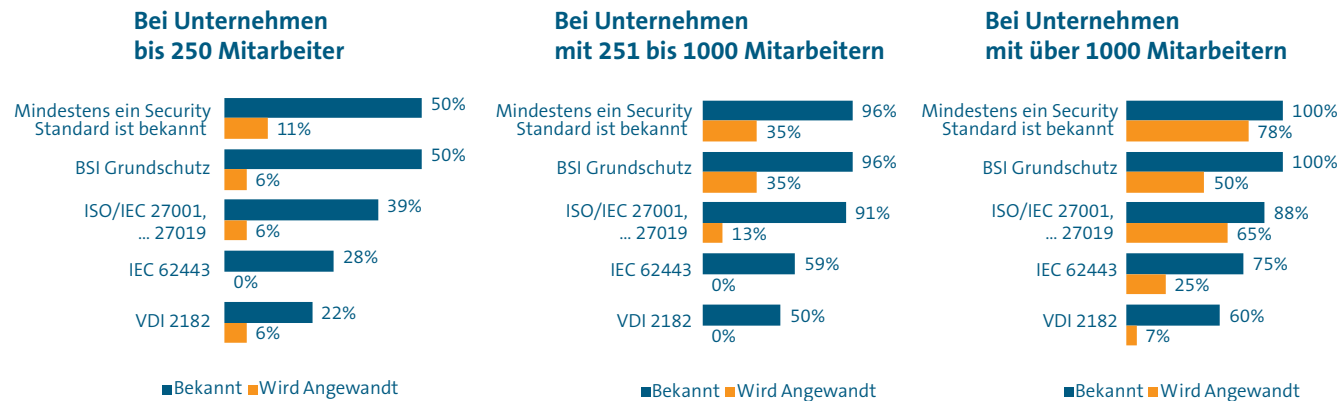
N = 55 bis 59

Abbildung 18

Quelle: VDMA-Report Industrial Security

Welche Security Standards sind Ihnen bekannt?

(nach Betriebsgrößen unterschieden)



N = 55 bis 59

Abbildung 19

Quelle: VDMA-Report Industrial Security

Handlungsempfehlungen des Arbeitskreises Industrial Security

- Es wird empfohlen, für die eigene Security-Konzepterstellung die oben genannten Security Standards als Basis oder Anregung zu verwenden. Unabhängig davon bieten folgende Dokumente einen guten Einstieg:
  - VDMA „Fragenkatalog Industrial Security: Einfach anfangen.“ [34]
  - Leitfaden IEC 62443: Der Weg durch die IEC 62443. [35]
  - ICS Security Kompendium (BSI) [36]
  - VdS Quick Check Security [37]
- Als kostenfreie Tools für die standardisierte Umsetzung werden empfohlen:
  - LARS: Light and Right Security (BSI) [38]
  - Verinice (SerNet GmbH) [39]

34 https://itatautomation.vdma.org/documents/105867/8303780/VDMA%20Fragenkatalog%20Security_2014_final.pdf

35 https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/vdma-security-automation.html

36 https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/ICS/ics_node.html

37 https://vds.de/de/cyber/quick-check

38 https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/ICS/Tools/LarsICS/LarsICS_node.html

39 https://verinice.com/

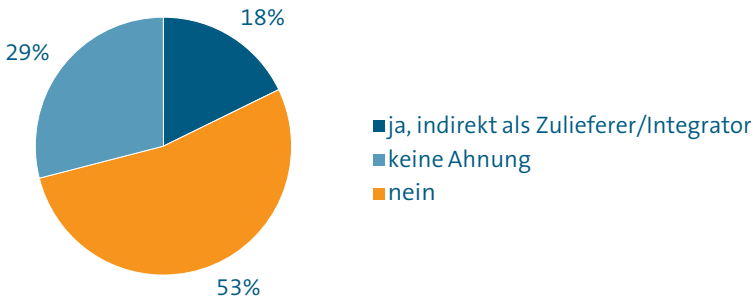
12 Zukunft der Industrial Security

IT-Sicherheitsgesetz zum Schutz kritischer Infrastrukturen

Bisher ist keines der befragten Unternehmen nach derzeitiger Definition direkt vom IT-Sicherheitsgesetz zum Schutz kritischer Infrastrukturen (KRITIS) betroffen. Lediglich 18 Prozent der Studienteilnehmer sehen sich aufgrund Ihrer Funktion als Zulieferer, Integrator oder Servicedienstleister indirekt mit den Anforderungen konfrontiert. Allerdings zeigt die Studie auch, dass besonders bei kleinen Unternehmen (bis 250 Mitarbeiter) häufig noch Unkenntnis herrscht, ob sie direkt oder indirekt davon berührt sind.

Sind Unternehmen indirekt vom IT-Sicherheitsgesetz betroffen, so haben sie in den meisten Fällen bereits entsprechende Maßnahmen (82 Prozent organisatorische, 64 Prozent technische Maßnahmen) durchgeführt. Allerdings erwarten neun von zehn Unternehmen in der Zukunft noch weitere Maßnahmen.

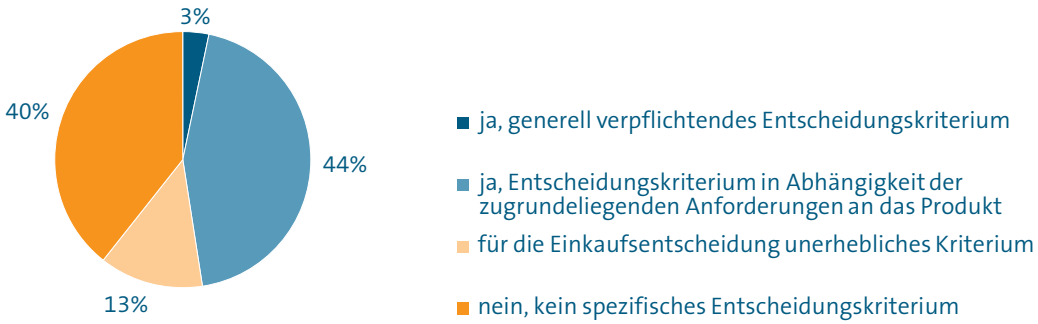
Ist Ihr Unternehmen vom IT-Sicherheitsgesetz zum Schutz kritischer Infrastrukturen betroffen?



N = 62

Abbildung 20 Quelle: VDMA-Report Industrial Security

Wäre für Ihr Unternehmen ein Security-Gütesiegel ein Entscheidungskriterium für den Produkteinkauf?



N = 61

Abbildung 21

Quelle: VDMA-Report Industrial Security

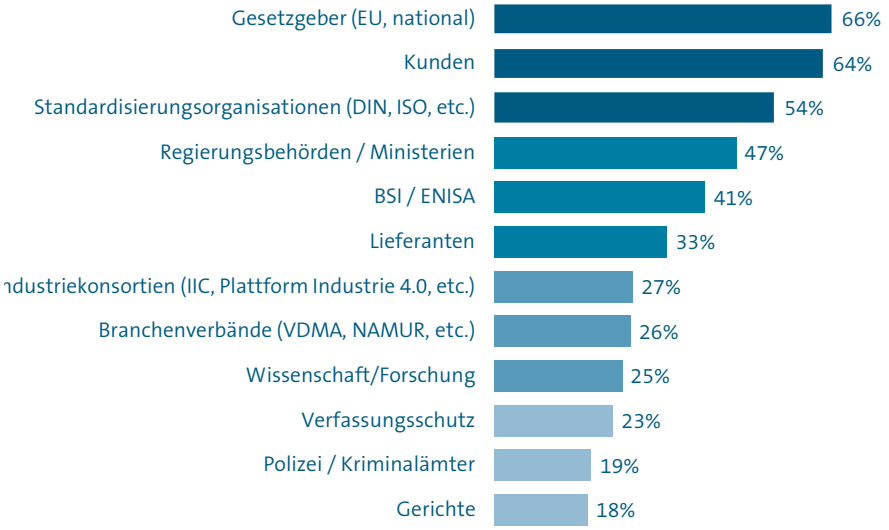
Security-Gütesiegel

Ein Gütesiegel für die „geprüfte“ Security-Qualität von industriellen IT-Systemen, vernetzten Komponenten und Maschinen steht für die Einkäufer von Integratoren und Betreibern aktuell nicht zur Debatte. Nur drei Prozent der befragten Unternehmen können es sich bisher als „generell verpflichtendes Entscheidungskriterium“ für den Produkteinkauf vorstellen. Mehr als die Hälfte der Studienteilnehmer sieht es als unerhebliches beziehungsweise nicht spezifisches Entscheidungskriterium an.

Anforderungen und Unterstützung zur Industrial Security

Die meisten Teilnehmer erwarten zukünftig weitere Anforderungen an die Industrial Security. Besonders die nationale und internationale Gesetzgebung (66 Prozent), Kunden (64 Prozent) und Standardisierungsorganisationen wie DIN oder ISO werden hierbei als Treiber gesehen. Unterstützung suchen die produzierenden Unternehmen vorrangig bei den Branchenverbänden der Hersteller, Lieferanten und Betreiber von Maschinen und Anlagen (85 Prozent), gefolgt von Zulieferern sowie Industriekonsortien.

Von wem erwarten Sie zukünftig Anforderungen zur Industrial Security?

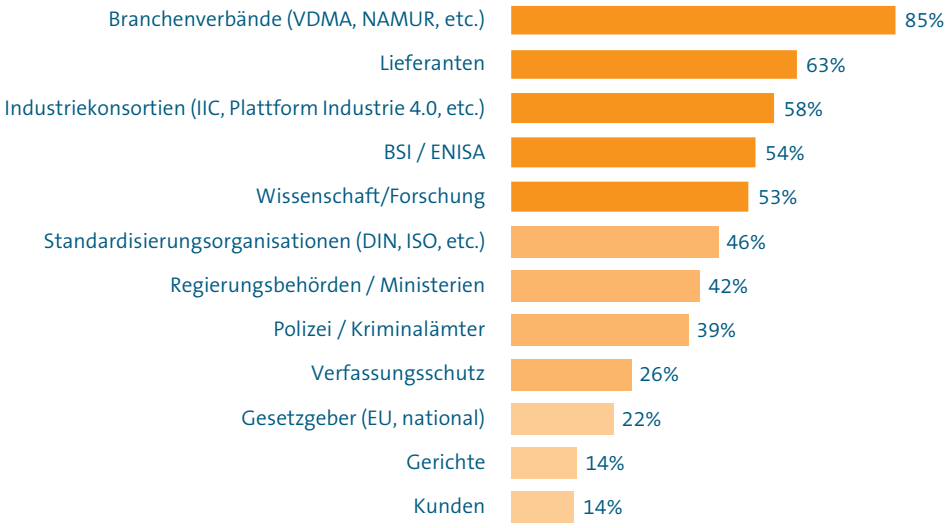


N = 56 bis 61

Abbildung 22

Quelle: VDMA-Report Industrial Security

Von wem erwarten Sie zukünftig Unterstützung zur Industrial Security?



N = 56 bis 61

Abbildung 23

Quelle: VDMA-Report Industrial Security

13 Unterstützung durch den VDMA

Der VDMA bietet Mitgliedsunternehmen umfassende Unterstützung zu Security. Im Mittelpunkt steht hierbei die Hilfe zur Selbsthilfe, zum Gedankenaustausch sowie zur politischen Unterstützung auf nationaler und internationaler Ebene. Mehrere Gremien zu Security, umfassende Publikationen und Veranstaltungen stehen Mitgliedern offen.

Das VDMA Competence Center Industrial Security (CCIS) bündelt die Verbandsaktivitäten des VDMA zur Informationssicherheit, zu Security in der Produktion und zur Security in den Maschinenbauprodukten. Das Competence Center ist erster Ansprechpartner für Mitglieder, Behörden und Politik. Es leistet zudem die fachliche Beratung und Unterstützung der VDMA Fachverbände.

industrialsecurity.vdma.org

Folgende Arbeitskreise pflegen den Gedankenaustausch und Wissensaufbau im VDMA.

VDMA Arbeitskreis „Cybersecurity“

Aufgaben:	Beratung, Steuerung und Beschlussfindung zur Cybersecurity-Politik
Teilnehmer:	Benannte VDMA-Mitglieder aus den VDMA Fachverbänden, je nach Themenstellung Fachexperten des VDMA zu Recht, Normung, Forschung, Politik oder Regulierung
VDMA-Kontakt:	Thomas Kraus, Abteilung Technik, Umwelt, Nachhaltigkeit
Vorsitzender:	Markus Werthschulte, Festo AG & Co. KG, Esslingen

VDMA Arbeitskreis „Industrial Security“

Aufgaben:	Erarbeitet Leitlinien und Praxishilfen für die Industrial Security
Teilnehmer:	Maschinen- und Anlagenbauer, Betreiber, Automatisierer, Dienstleister, Security-Spezialisten, Bundesamt für Sicherheit in der IT (BSI)
VDMA-Kontakt:	Steffen Zimmermann, Competence Center Industrial Security

VDMA Arbeitskreis „Informationssicherheit“

Aufgaben:	Erarbeitet Leitlinien und Praxishilfen der IT- und Informationssicherheit
Teilnehmer:	CISOs und IT-Sicherheitsbeauftragte der Maschinen- und Anlagenbauer
VDMA-Kontakt:	Steffen Zimmermann, Competence Center Industrial Security
Vorsitzender:	Rolf Strehle, Voith GmbH, Heidenheim

VDMA Arbeitskreis „Cybersecurity in der Landtechnik“

Aufgaben:	Begleitung und Adaption der ISO 21434 Cybersecurity Engineering
Teilnehmer:	VDMA-Mitglieder des Fachverbandes Landtechnik
VDMA-Kontakt:	Dr. Hermann Buitkamp, Fachverband Landtechnik
Vorsitzender:	Thomas Ehl, Claas KGaA mbH, Harsewinkel

VDMA Arbeitskreis „IT-Sicherheit in der Gebäudeautomation“

Aufgaben:	Erfahrungsaustausch, Überarbeitung des VDMA Einheitsblatts 24774
Teilnehmer:	VDMA-Mitglieder des Fachverbands Automation + Management für Haus + Gebäude, VDMA Competence Center Industrial Security, BSI
VDMA-Kontakt:	Thomas Müller, Fachverband Automation + Management für Haus + Gebäude

VDMA Projektgruppe „Digitalisierung Energie“

Aufgaben:	Austausch zu Cybersecurity für Energieerzeugungsanlagen, u.a. KRITIS, Smart Meter Gateway (SMGW), Remote Service und Condition Monitoring
Teilnehmer:	VDMA-Mitglieder des Fachverbands Power Systems
VDMA-Kontakt:	Sebastian Steul, Fachverband Power Systems

Positionen des VDMA zu Security

Cybersecurity: Integraler Bestandteil eines EU-Binnenmarktes
VDMA 2017, Deutsch/Englisch

Zentrales VDMA-Diskussionspapier zur Gestaltung eines europäischen Rahmens für Industrial Security. Das Paper beschreibt grundlegende Herausforderungen und bietet Empfehlungen für erste Schritte und Prinzipien, um aus Sicht des Maschinen- und Anlagenbaus eine transparente, nachhaltige und stabile Security-Politik zu realisieren. Im Fokus: Das New Legislative Framework.

https://euro.vdma.org/viewer/-/article/render/20571551

Industrie 4.0: Wandel gestalten, Potenziale nutzen
VDMA 2014

Die Digitalisierung durch das Internet verändert die Lebens- und Arbeitswelt nachhaltig. Auch die Produktion wird digitalisiert – genannt Industrie 4.0. Diese Entwicklung bietet dem deutschen Maschinen- und Anlagenbau alle Chancen, seine führende Position auszubauen. Ob die Industrienation Deutschland Industrie 4.0 zum Geschäftsmodell machen kann, hängt nicht nur von den Unternehmen ab. Wichtige Rahmenbedingungen müssen mit Politik und Gesellschaft vereinbart werden.

Potenzial von Industrie 4.0 für Europa nutzen
VDMA 2015, Deutsch/Englisch

Der Maschinen- und Anlagenbau entwickelt neue Lösungen für die Industrie 4.0. Damit kann der Industriestandort Europa wachsen. Die Politik muss sich dafür aber stärker auf die industriepolitischen Aspekte der Digitalisierung konzentrieren. Nur wenn die Unternehmen auf dem europäischen Markt gute Rahmenbedingungen finden, können sie den Weg zu Industrie 4.0 gehen und neben Wohlstand und Beschäftigung auch die europäische Idee voranbringen.

Industrial Security: Sichere Maschinen und Anlagen
VDMA 2015, Deutsch/Englisch

Steht die Produktion, geht bares Geld verloren. Fallen kritische IT-Infrastrukturen wie in Krankhäusern oder bei Energieversorgern aus, stehen Menschenleben auf dem Spiel. Informationstechnik in Produktionssystemen sowie Maschinen und Anlagen vor Sabotage, Spionage oder Manipulation zu schützen, ist Aufgabe der „Industrial Security“.

Diese und weitere Positionspapiere des VDMA finden Sie unter
https://berlin.vdma.org/kurzpositionen

Publikationen zu IT-Security / Informationssicherheit

Leitfaden Informationssicherheit,
Teil 1: Mitarbeitersensibilisierung

VDMA 2009
Preis: Euro 44,00
VDMA-Mitglieder: Euro 22,00
ISBN: 978-3-8163-0575-0

https://www.vdmashop.de/Informatik-und-Technik/Leitfaden-zur-Informationssicherheit--Teil-1--Sensibilisierung.html

Leitfaden Informationssicherheit,
Teil 2: ISMS, Dokumente und Vorlagen

VDMA 2013
Preis: Euro 50,00
VDMA-Mitglieder: kostenfrei
EAN: 4250697518395

https://www.vdmashop.de/Informatik-und-Technik/Leitfaden-zur-Informationssicherheit-Teil-2---download.html

Leitfaden Informationssicherheit,
Teil 3: Elektronischer Informationsaustausch mit Externen und deren Anbindung

VDMA 2016
Preis: Euro 44,00
VDMA-Mitglieder: 22,00
ISBN: 978-3-8163-0686-3

https://www.vdmashop.de/Informatik-und-Technik/Leitfaden-zur-Informationssicherheit--Teil-3--Elektronischer-Informationsaustausch-mit-Externen-und-deren-Anbindung.html

Status Quo VPN & Datenaustausch in China

VDMA 2018
Kostenfrei, nur für VDMA-Mitglieder

Mit diesem Faktenpapier werden Erfahrungen von VDMA und nicos AG zusammengeführt, um gemeinsam zum Verständnis über das „VPN-Verbot in China“ beizutragen. Das Papier gibt allgemeine Hinweise, aktuelle Einschätzung sowie Handlungsempfehlungen.

https://industrialsecurity.vdma.org/viewer/-/v2article/render/26756886

Publikationen zu Industrial Security / Industrie 4.0 Security

Leitfaden Industrie 4.0 Security
VDMA 2016

Der Leitfaden umfasst 83 Sicherheitsanforderungen in 17 Bereichen für den sicheren Produktlebenszyklus von Maschinen und Produktionsanlagen. Darüber hinaus umfassen die Anforderungen die Prüfung von Gefahren und Risiken vor der Inbetriebnahme, die Verwaltung von Cyber-Risiken während des Betriebs und die Aufrechterhaltung der Sicherheitsfunktion während des gesamten Produktlebenszyklus von angeschlossenen Maschinen und Systemen.

https://industrialsecurity.vdma.org/viewer/-/v2article/render/26240836

Leitfaden Security: Der Weg durch die IEC 62443
DIN/NAM/VDMA 2016

Richtlinie für Anlagenerrichter, die Sicherheitsmaßnahmen in Ihre Produkte integrieren wollen, basierend auf den international anerkannten IEC 62443 Standards. Das Dokument empfiehlt Herstellern und Integratoren Schritte und Maßnahmen für eine IEC 62243-Exemplarische Vorgehensweise, wenn es darum geht, „Security Level 2“ zu erreichen.

https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/vdma-security-automation.html

Industrial Security – sicher in die digitale Zukunft
VDMA 2017

Beiträge von VDMA-Mitgliedern sowie Behörden zur Industrial Security, u.a. Security by Design, IEC 62443, Aus- und Weiterbildung, Cyberversicherung, Landtechnik, IUNO-Projekt, etc.

Auf Anfrage bei Biljana Gabric erhältlich.

Industriedaten: Verantwortung und Chancen tarieren
VDMA 2017

Im Betrieb intelligenter, vernetzter Systeme entstehen wertvolle und hochsensible Industriedaten. Der Austausch dieser Daten ermöglicht neue Geschäftsmodelle, verspricht mehr Produktivität und Effizienz. Gleichzeitig muss der Datenschutz für Arbeitnehmer und Nutzer gewährleistet sein.

https://www.vdma.org/v2viewer/-/v2article/render/18176171

Fragenkatalog Industrial Security – Einfach anfangen.
VDMA 2014

Einstiegshilfe in die Auswahl und Bewertung von Security-Maßnahmen für Produktionsumgebungen. Der Fragenkatalog dient der erstmaligen Betrachtung mit Hilfe von 33 Fragen. Das Ziel ist es, bereits nach 20 Minuten einen ersten Überblick zu erhalten.

https://industrialsecurity.vdma.org

INS-Studie „Security in Automation“
DIN/NAM/VDMA 2014

Vergleich und Bewertung von nationalen und internationalen Normen und Standards für Automations- und Produktionssicherheit, z.B. IEC 62443, ISO/IEC 27001, BSI Grundschutz, VDI 2182.

https://industrialsecurity.vdma.org

Studie „Status Quo der Security in Produktion und Automation“
VDMA 2013

Fakten und Grafiken zur Industrial Security. Befragung und Auswertung einer Umfrage unter VDMA-Mitgliedern mit dem Schwerpunkt Industrial Security. Zudem gibt es zu allen Ergebnissen praxisnahe Handlungsempfehlungen des Arbeitskreises Industrial Security.

https://industrialsecurity.vdma.org

Publikationen zu Produkt- und Know-how-Schutz

Studie Produktpiraterie 2018
VDMA 2018

71 Prozent der VDMA-Mitgliedsunternehmen sind direkt von Produkt- oder Markenpiraterie betroffen, ein Verlust von 7,3 Milliarden Euro pro Jahr. Die Volksrepublik China bleibt unbestrittenen auf Platz 1 der Top-Fälscher weltweit und ist im Maschinen- und Anlagenbau das Herkunftsland von 82 Prozent aller gefälschten Produkte.

https://industrialsecurity.vdma.org/viewer/-/v2article/render/26240978

Branchenführer „Produkt- und Know-how-Schutz“
VDMA 2016

Informationen und Hintergrundwissen über Produktpiraterie, Security und Know-how-Schutz.

https://industrialsecurity.vdma.org

Leitfaden „Produkt- und Know-how-Schutz“
VDMA 2013

Sprache: Deutsch oder Englisch
Preis: kostenfrei

Anleitung zum erfolgreichen Einsatz von Schutzmaßnahmen inkl. praxisnaher Beispiele.

https://industrialsecurity.vdma.org

INS-Studie „Status Quo des Know-how-Schutzes im Maschinen- und Anlagenbau“
DIN/NAM/VDMA 2013

Preis: kostenfrei

Übersicht der Know-how-Schutz-Aktivitäten von VDMA-Mitgliedern.

https://industrialsecurity.vdma.org

INS-Studie „Kennzeichnung und Identifizierung von Maschinenbauprodukten“
DIN/NAM/VDMA 2011

Preis: kostenfrei

Auflistung und Klassifizierung von Kennzeichnungs- und Identifizierungstechnologien in Bezug auf Condition Monitoring, Logistik und Produktpiraterie.

https://industrialsecurity.vdma.org

Redaktionskreis

Steffen Zimmermann
VDMA Competence Center Industrial Security

Guido Reimann
VDMA Software und Digitalisierung

Hans-Peter Bock
TRUMPF Werkzeugmaschinen GmbH + Co. KG

Stefan Ditting
HIMA Paul Hildebrandt GmbH

Heinz-Uwe Gernhard
Robert Bosch GmbH

Jens Mehrfeld
Bundesamt für Sicherheit in der Informationstechnik

Wolfgang Stadler
SICK AG

Florian Straßer
@-yet GmbH

Bernd-Ulrich Wittwer
Weidmüller Interface GmbH & Co. KG

Helmut Wirth
Renk Aktiengesellschaft

VDMA Competence Center Industrial Security
Lyoner Straße 18
60528 Frankfurt am Main
Internet: industrialsecurity.vdma.org

VDMA
Competence Center Industrial Security
Lyoner Straße 18
60528 Frankfurt am Main

Kontakt
Steffen Zimmermann
Telefon +49 69 6603-1978
E-Mail steffen.zimmermann@vdma.org

VDMA
Software und Digitalisierung

Kontakt
Guido Reimann
Telefon +49 69 66 03-1258
E-Mail guido.reimann@vdma.org

industrialsecurity.vdma.org
sud.vdma.org

DesignStudio