VDMA

Kompetenz in

Industrial Security

Inhaltsverzeichnis

1. Definition von Industrial Security

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 des Systems (Umwelt). Zum besseren Verständnis lässt sich dies auf „Schutz der Maschine vor dem Menschen“ reduzieren.

Industrial Security ist als Prozess zu verstehen, der den Schutz vor Ausfall, Know-how-Abfluss, Spionage sowie Manipulation von Maschinen, Anlagen und Industriedaten sicherstellen soll. Security-Vorfälle aus dem „Office-Umfeld“ (IT-/Cybersecurity) sind zusätzlich von Relevanz, wenn sich Auswirkungen auf Maschinen oder Anlagen zeigen.

2. 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* („OT Security“) 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

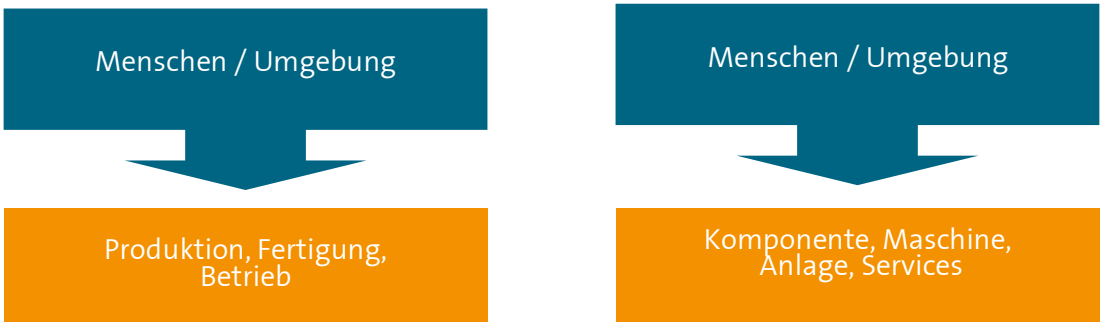


Abbildung 1: Sichtweisen auf die Industrial Security

3. Relevante Regulierung zu Cybersecurity in Europa

Nach aktuellem Stand gibt es in Europa gesetzlich verpflichtenden Anforderungen an den Maschinen- und Anlagenbau, Cybersecurity umzusetzen. Anforderungen kommen derzeit insbesondere von Kundenbranchen Automotive (TISAX, UNECE) sowie Betreibern kritischer Infrastrukturen. Darüber hinaus verlangen Einkäufer von Produktionssystemen immer häufiger die Erfüllung von Vorgaben in ihren Einkaufsbedingungen. Auch bei Fernwartung oder Nutzung von datenzentrierten Diensten fordern Kunden die Einhaltung entsprechender Vorgaben auf Basis einschlägiger Normen und Standards (z.B. nach IEC 62443). Im VDMA Arbeitskreis „Industrial Security" wurde für diese Zwecke ein Supply Chain Security Lastenheft erarbeitet, dass Mindestanforderungen für die Beschaffung von Maschinen und Anlagen auf Basis der IEC 62443 standardisiert.
Verpflichtungen für die Umsetzung von Cybersecurity sind derzeit im europäischen Umfeld in Arbeit und ergeben sich aus den folgenden Gesetzen und Vorhaben:

Geltungs-bereich	Bezeichnung	Status	Betroffen-heit	IT Security	OT Security	Product Security
Deutschland	**IT-Sicherheitsgesetz 2.0**	Aktiv 28.05.2021		x		(x)
Deutschland	**NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-gesetz (NIS2UmsuCG)**	Referenten-entwurf 03.07.2023		x	x	(x)
EU	**Funkanlagenrichtlinie – Delegierter Rechtsakt** Umsetzungsfrist 01.08.2024	Inkraft seit 01.02.2022 hEN in Arbeit				x
EU	NIS2 Richtlinie (Umsetzung in Deutschland durch das NIS2UmsuCG)	Inkraft seit 16.01.2023 Umsetzungsfrist 10/2024		x	x	(x)
EU	Cyber Resilience Act	Abstimmung EP, Start Tilog 10/ 2023		(x)		x

Zu den Regulierungen hat der VDMA entsprechende Informationen veröffentlicht und begleitet diese in den jeweiligen Gremien. Eine **regelmäßig aktualisierte Übersicht** über den Status der Regulierung und die Betroffenheit ist auf Anfrage beim VDMA verfügbar.

Besonderes Augenmerk sollten Unternehmen des Maschinen- und Anlagenbaus auf die NIS2 Richtlinie und den Cyber Resilience Act legen. Auch wenn die Verpflichtungen aus den Regulierungen noch einige Jahre entfernt sind, müssen Grundlagen für interne Prozesse und Verfahren zügig geschaffen werden. Insbesondere durch die Vielzahl an betroffenen Unternehmen und Produkten ist mit einer Knappheit an Ressourcen auf allen Ebenen zu rechnen.

Bei der außereuropäischen Regulierung konzentriert sich der VDMA auf die Unterstützung in China. Hierzu wurden bereit mehrere Unterlagen veröffentlicht (siehe Publikationsliste).

4. Gremien und Arbeitskreise

Folgende Arbeitskreise pflegen den Gedankenaustausch und Wissensaufbau zu Industrial Security 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
Vorsitzender: Bernd Gehring, Voith GmbH, Heidenheim

VDMA Arbeitskreis "Informationssicherheit"

Aufgaben: Erfahrungsaustausch zur 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 "IT-Sicherheit in der Gebäudeautomation"

Aufgaben: Erfahrungsaustausch, Verantwortung für VDMA Einheitsblatt 24774
Teilnehmer: VDMA-Mitglieder des Fachverbands Automation + Management für Haus + Gebäude, Bundesamt für Sicherheit in der IT (BSI)
VDMA-Kontakt: Thomas Müller, Fachverband Automation + Mgmt. 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

VDMA Arbeitskreis "NIS2" i.Gr. (ab Herbst 2023)

Aufgaben: Erfahrungsaustausch von kleinen und mittelständischen Mitgliedern zur NIS2 und dem NIS2UmsuCG. Feststellung der Angemessenheit von Maßnahmen zur Erfüllung der Anforderungen.
Teilnehmer: NIS2-Verantwortliche von VDMA-Mitgliedern < 500 MA
VDMA-Kontakt: Steffen Zimmermann, Competence Center Industrial Security

5. Weiterbildungsangebote

Das Maschinenbau-Institut als Weiterbildungsakademie des VDMA bietet zum Thema Industrial Security ein breitgefächertes Weiterbildungsangebot. Zudem wurden in Kooperation mit University4Industry (U4I) digitale Selbstlern-Module erarbeitet.

5.1. Weiterbildungen zur IEC 62443

Betreiber, Hersteller, Integratoren und Dienstleister müssen sich alle mit der Normenreihe IEC 62443 beschäftigen, um sowohl die OT-Security wie auch die Product Security sicherzustellen. Kurz: Die IT-Sicherheit von vernetzen Maschinen, Anlagen und Systemen muss über den gesamten Lebenszyklus gewährleistet werden. Dies beginnt beim Entwicklungsprozess und endet bei der Außerbetriebnahme.

Hierfür bietet das Maschinenbau-Institut die folgenden Seminare an:

ISA-Qualifizierungsprogramm zum IEC 62443 Cybersecurity Expert

Die Quantität an Sicherheitsvorfällen nimmt auch im Maschinenbau stetig zu. Deshalb bietet das MBI in Kooperation mit der **ISA Europe** und in Zusammenarbeit mit dem **Fraunhofer IOSB** ein Qualifizierungsprogramm zur Ausbildung von "**Cybersecurity Experts**" an. In vier aufeinander aufbauenden Seminaren werden die unterschiedlichen Aspekte zur IT-Sicherheit von vernetzten Maschinen und Anlagen eingehend behandelt.
Für Fortgeschrittene gibt es den 5-tägigen Kompaktkurs direkt zum „Cybersecurity Expert“.

Weitere Informationen unter:
https://www.maschinenbau-institut.de/isa-qualifizierungsprogramm

Security by Design für Maschinen und Anlagen

Cybersicherheit bereits im Entwicklungsprozess mitdenken – das ist der Ansatzpunkt von Security by Design. Das Seminar wurde in Zusammenarbeit mit dem **Fraunhofer IEM** und **Fraunhofer IOSB** speziell für den Maschinenbau entwickelt und erläutert, wie die Prinzipien konkret angewendet werden müssen. Basis bilden die IEC 62443 und das VDMA Lastenheft zu Supply Chain Security.

Weitere Informationen unter: https://www.maschinenbau-institut.de/seminar/security-by-design-fuer-maschinen-und-anlagen/

Produktionsanlagen gegen Cyber-Bedrohungen schützen

In diesem Seminar werden Betreiber von industriellen Produktionssystemen in die Lage versetzt, diese vor Cyberangriffen und anderen Bedrohungen zu schützen. Es wird vermittelt, welche Maßnahmen gemäß der Normenreihe IEC 62443 ergriffen werden sollten.

Weitere Informationen unter: https://www.maschinenbau-institut.de/seminar/produktionsanlagen-gegen-cyber-bedrohungen-schuetzen/

5.2. VDMA Campus bei University4Industry – Lernmodule “Industrial Security”

U4I bietet VDMA-Mitgliedern kostenfreie digitale Lernmodule zu Industrial Security, welche gemeinsam mit Experten des VDMA Arbeitskreises „Industrial Security“ entwickelt wurden.

Die Lernmodule sind für ein besseres Lernerlebnis in die zwei Sichtweise der Industrial Security unterteilt. Zum einen die des Maschinenbauers als Betreiber und zum anderen die als Hersteller bzw. Integrator.

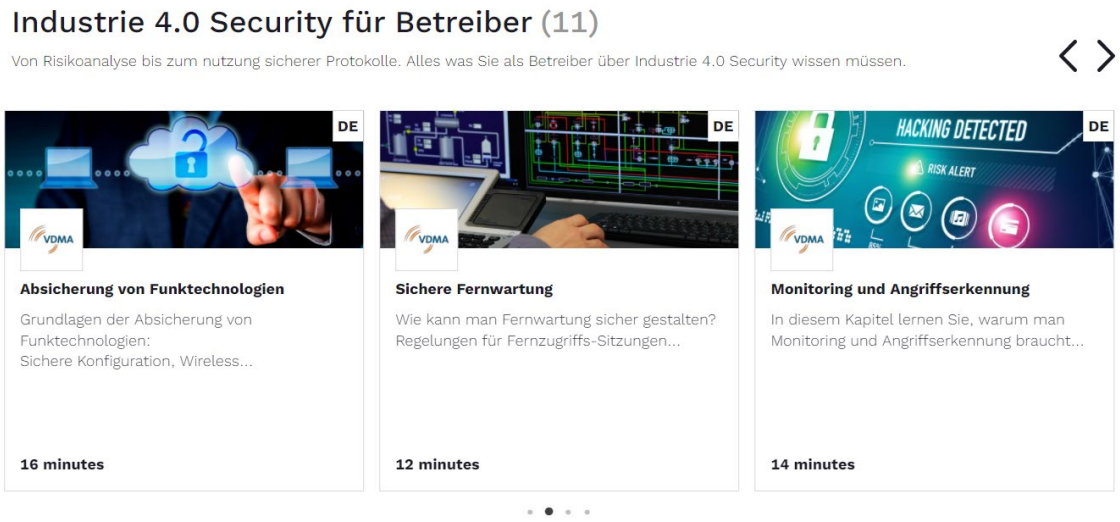


Abbildung 2: Lernmodule für Betreiber

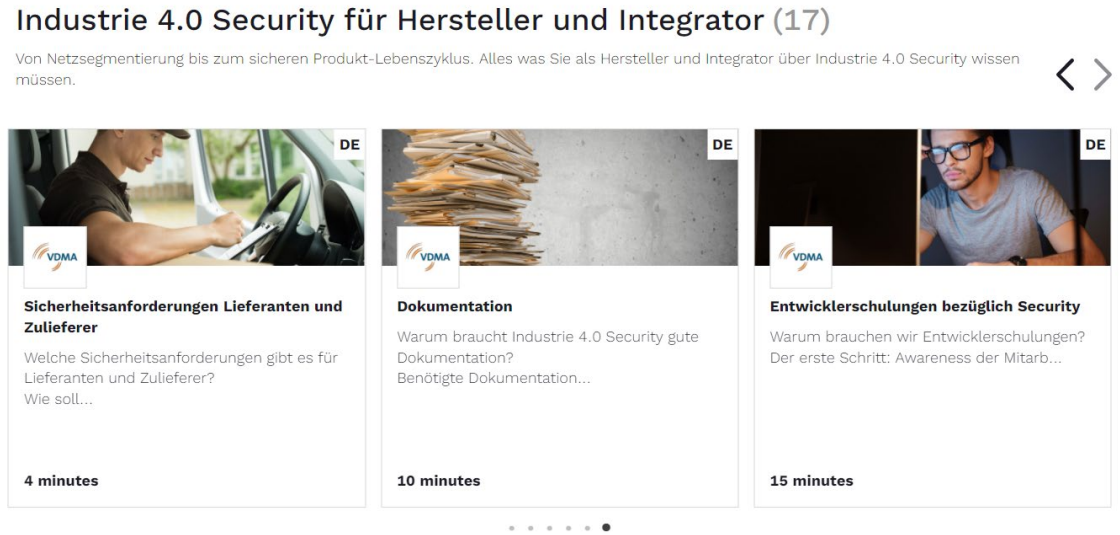


Abbildung 3: Lernmodule für Hersteller und Integratoren

Die Module bietet über acht Stunden Know-how für unterschiedliche Lernstufen. Weitere Themenbereiche bei University4Industry sind Industrial IoT & Connectivity, Software-Engineering, Machine Learning und Additive Manufacturing.

Weitere Informationen unter https://www.university4industry.com/vdma

6. Cyberversicherung: Die VDMA Cyber Police (VCP)

Ansprechpartner Nr. 1 für Versicherungen im industriellen Umfeld ist die VSMA, der Versicherungsmakler des VDMA. Die VSMA berät bereits seit über 90 Jahren die Mitglieder des VDMA. Gemeinsam mit dem Competence Center Industrial Security hat die VSMA eine Cyber Police für den Maschinen- und Anlagenbau erarbeitet. Die VSMA betreibt zudem das Informationsportal "**Unternehmen Cybersicherheit**", auf dem Mitglieder neben aktuellen Informationen auch Zugang zu Arbeitshilfen erhalten.

Abbildung 4: Angebots-Webseite der VSMA zur Cyber Police

Die „VDMA Cyber Police" ist ein auf die Bedürfnisse von Maschinen- und Anlagenbauern zugeschnittenes Versicherungsangebot. Die Cyber Police kommt für alle maßgeblichen Dritt- und Eigenschäden auf. Sie bietet Hilfe bei Ransomware-Vorfällen oder wenn Fernwartungszugänge bei Kunden durch Hacker missbraucht wurden. Inklusive sind auch wichtige Assistance-Leistungen für den Schadenfall, z. B. eine Notfallhotline und ein erfahrenes Team von Forensikern, das betroffene Unternehmen bei der Bewältigung des Vorfalls sofort unterstützt.

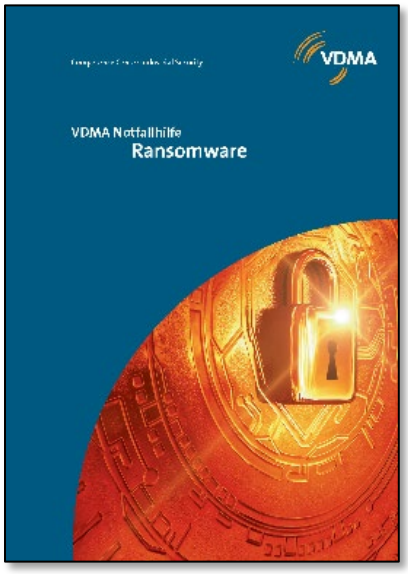
Weitere Informationen erhalten Sie von Thomas Völker oder unter:
https://unternehmen-cybersicherheit.de/cyber-versicherung-vdma-cyber-police

Thomas Völker

VSMA GmbH
Lyoner Str. 18
60528 Frankfurt am Main

Telefon: +49 69 66 03 – 15 20
E-Mail: tvoelker@vsma.org
Web: www.vsma.de

7. Sonderthema Ransomware



Die Vorfälle mit Ransomware im Maschinen- und Anlagenbau haben seit 2019 stark zugenommen. So waren in den letzten zwei Jahren über 50 Mitglieder von Ransomware direkt betroffen.

Die Erfahrungen zeigen, dass es nicht ausreicht, sich allein auf die präventive Abwehr von Ransomware-Angriffen zu fokussieren. Jeder Maschinen- und Anlagenbauer muss davon ausgehen, dass früher oder später ein Angriff erfolgreich sein kann. Was dann zählt ist die schnelle Wiederherstellung eines sicheren Arbeitsmodus.

Besonders bedroht von kritischen Ransomware-Angriffen sind kleine und mittelständische Unternehmen, fehlen hier doch oft die notwendigen Notfallvorsorgekonzepte und Krisenpläne, um bei einem Ransomware-Angriff sofort zu wissen, welche Schritte zu tun sind.

Mit der Notfallhilfe Ransomware hat der VDMA Arbeitskreis „Informationssicherheit“ die Antworten auf grundlegende Fragen bei einer Ransomware-Infektion zusammengeführt.

- Woran erkenne ich einen Angriff?
- Wann rufe ich einen Ransomware-Notfall aus?
- Wie gehe ich im Ransomware-Notfall vor?
- Was sollte ich vermeiden?
- Wen kann ich im Notfall um Unterstützung bitten?
- Welche Maßnahmen kann ich vornehmen, damit es nicht (nochmal) passiert?

Angriffsschritte	Risiken	Pflicht?	Maßnahmen	Kommentare zu Maßnahmen	Einrichtung	Pflege	Nutzen
					1=geringer Aufwand		5=hoch
Empfang einer Email	R: Faken des Absenders		M: DNS & IP-Tools: Nutzung von SPF, DKIM, DMARC, E-Mail-Blacklists, Spamcop, etc.	Blacklists müssen regelmäßig gepflegt werden, für Kunden sollten Ausnahmen definiert werden können	4	2	5
			M: DNAE Domain Named Authenticated Entities	Zertifikatsprüfung durch den Absender	4	2	3
			M: Einschränken der "Spam-Authentizität" (wie echt können gefälschte Emails aussehen)	Mailserver so konfigurieren, dass SPAM für Nutzer einfach erkennbar wird	2	2	3
		ja	M: Awarenesstraining: Nicht auf einfach fälschbaren "Display Namen" verlassen	Nachhaltig nur durch Wiederholung, auch für neue Mitarbeiter	5	3	4
		ja	Markierung einer externen Mail als „Extern"	Ablehnende Haltung von Vertriebsmitarbeitern	1	1	3
	R: E-Mail mit ausführbarer Datei im Anhang	ja	M: gefährliche Dateitypen blocken, mind. ausführbare Dateien	https://www.govcert.ch/downloads/blocked-filetypes.txt	1	1	3
	R: E-Mail mit aktivem Inhalt im Anhang (Office z.B.)		M: Einschränkung der Empfangsrechte auf spezifische Gruppen	Gefahr des Dauerzustands für alle Mitarbeiter	3	2	2
			M: Makros in Officedateien beim Empfang automatisiert entfernen	schwierig umzusetzen, fehlerhafte Dateien möglich	5	1	2
			M: BSI-Empfehlung zu Gruppenrichtlinien für Microsoft Office umsetzen	sehr umfangreich	4	3	4
			M: Nur signierte Makros oder weniger in Office zulassen	Standardeinstellung in Office	1	1	3
Öffnen einer E-Mail	R: Öffnen einer privaten Mail über Webmailer		M: Sensibilisierung der User: organisatorische Richtlinie	Evtl. auch automatisiert via Webfilter einschränken	2	2	2
	R: Der Anhang enthält eine ausführbare Datei		M: Empfang von ausführbaren Dateien einschränken		1	1	3
Ausführen einer geskripteten Datei durch den User	R: funktioniert auf voll gepatchten Systemen, da die User die Datei ausführen		M: Heuristik / "KI" des Antivirus-Programms nutzen	Statistik: 10% der User klicken auf eine Phishing-Mail	2	2	3
			M: Verhaltensbasierte Analyse/Abwehr	Ist meist bei Next Generation AV integriert	2	2	3
			M: Sandboxing (Gateway)	Angreifer können Sandboxing erkennen	3	3	3
		ja	M: Deaktivieren von Office Makros per Gruppenrichtlinie, Aktivierung nur für ausgewählte User	Ablehnende Haltung der Mitarbeiter da viel selbst gestricktes im Umlauf	1	3	3
Starten von Aktionen auf dem Client	R: User hat umfassende Rechte	ja	M: Kein angemeldeter Benutzer hat Adminrechte	Ausbreitung auf Systeme mit Schreibrechten begrenzt	2	1	4

Ergänzend dazu bietet ein Excel-Datenblatt eine Übersicht von Maßnahmen (Ransomware Kill Chain, Indikatoren, Kontaktdaten und frei zugänglichen Informationen Dritter.

Die Notfallhilfe ist auf Deutsch und Englisch kostenfrei verfügbar.

https://www.vdma.org/viewer/-/v2article/render/1295961

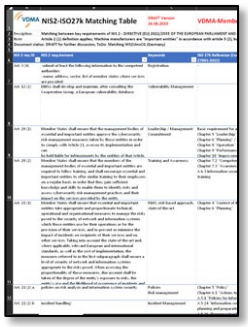
8. Publikationen zu Industrial Security

VDMA Lieferantenselbstauskunft (Excel)

Sprache: Deutsch, Englisch
Preis: kostenfrei

allgemein gültiger Fragebogen für Lieferanten ohne konkreten Beschaffungsbezug. Referenz auf Maschinenverordnung und Cyber Resilience Act. Mit dem BSI gemeinsam erarbeitet.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org

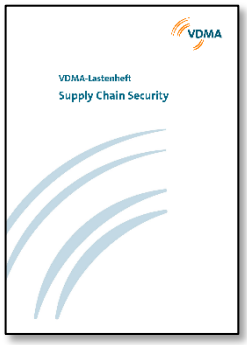


VDMA Mapping NIS2-27001:2002 (Excel)

Sprache: Englisch
Preis: kostenfrei, nur für VDMA-Mitglieder

Mapping der ISO/IEC 27001:2022 auf die Anforderungen aus der NIS2-Richtlinie.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org

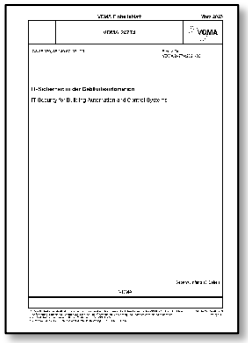


VDMA Lastenheft "Supply Chain Security"

Sprache: Deutsch
Preis: kostenfrei

Lastenheft mit Cybersecurity-Anforderungen auf Basis der IEC 62443. Zielgruppe sind Einkäufer, die allgemein anerkannte Anforderungen an die Cybersecurity von Maschinen und Anlagen stellen möchten, vom Design bis hin zum cybersicheren Betrieb.

https://www.vdma.org/viewer/-/v2article/render/73448513



VDMA Einheitsblatt 24774:2023-03
"IT-Sicherheit in der Gebäudeautomation"

Sprache: Deutsch
Preis: kostenfrei für VDMA-Mitglieder

Überarbeitete Ausgabe von März 2023, welche die Anforderungen der Grundschutzbausteine Infrastruktur für Technisches Gebäudemanagement (INF.13) und Gebäudeautomation (INF.14) des BSI IT-Grundschutz-Kompendiums abbildet.

https://www.vdma.org/viewer/-/v2article/render/55742079

VDMA Publikation "Sichere Fernwartung im Maschinen- und Anlagenbau"

Sprache: Deutsch
Preis: kostenfrei, nur für Mitglieder

Beispiele von Fernwartungsarchitekturen zeigen auf, wie der Maschinen- und Anlagenbau einen sicheren Service aus der Ferne gewährleisten kann.

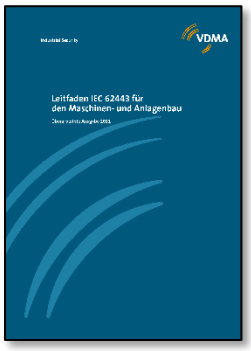
https://www.vdma.org/viewer/-/v2article/render/45231112

VDMA Mindestempfehlungen zu Security in der Supply Chain

Sprache: Deutsch
Preis: kostenfrei

Mindestempfehlungen für Maschinen- und Anlagenbauer zu technischen, organisatorischen und prozessualen Anforderungen bei der Umsetzung von Security für Produkte und Prozesse.

https://www.vdma.org/viewer/-/v2article/render/51129051

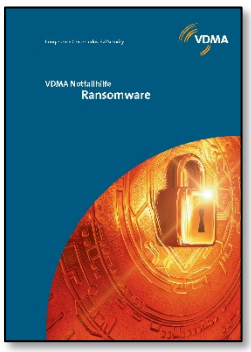


VDMA Leitfaden IEC 62443 für den Maschinen- und Anlagenbau

Sprache: Deutsch, Englisch
Preis: 50 Euro für Nicht-Mitglieder, kostenfrei für Mitglieder

Beschreibung eines Weges durch die IEC 62443, als Integrator einer Maschine nach Security-Level 2, inkl. Beispielen nach 62443-3-3.

https://www.vdmashop.de/executive-briefings/informatik-und-technik/482/leitfaden-iec-62443-fuer-den-maschinen-und-anlagenbau?number=&c=23

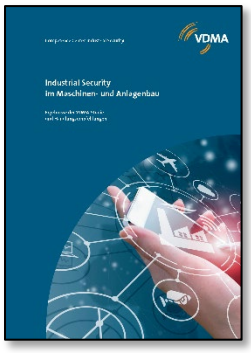


VDMA Notfallhilfe Ransomware

Sprache: Deutsch, Englisch
Preis: kostenfrei

Unterstützung, Handlungsempfehlung bei einer Infektion mit Ransomware, Kontaktstellen bei Behörden und Dienstleistern. Liste von Indikatoren für eine Infektion und Maßnahmen.

https://www.vdma.org/viewer/-/v2article/render/1295961



VDMA Studie „Industrial Security“

Sprache: Deutsch, Englisch
Preis: kostenfrei

Status Quo der Industrial Security im Maschinen- und Anlagenbau, Ergebnisse der Umfrage, Maßnahmen und Handlungsempfehlungen.

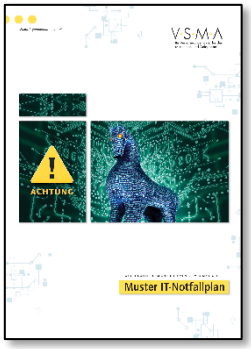
https://www.vdma.org/viewer/-/v2article/render/11923532

VDMA Positionspapier „Cybersecurity: Betreiber- und Arbeitgeberpflichten im Sinne gemeinsamer Anstrengungen“

Sprache: Deutsch
Preis: kostenfrei

Formulierung der VDMA Position zu Cybersecurity-Pflichten im täglichen Anlagenbetrieb.

https://vdma.org/viewer/-/v2article/render/4769363



VSMA Muster IT-Notfallplan

Sprache: Deutsch
Preis: kostenfrei auf Anfrage bei VSMA

Der Muster IT-Notfallplan dient der Unterstützung, nach einer massiven Beeinträchtigung des betrieblichen Ablaufs aufgrund von nicht funktionierender IT-Infrastruktur, schnellstmöglich wieder in einen geordneten IT-Betrieb zurückzufinden.

https://unternehmen-cybersicherheit.de

VDMA Leitfaden „Industrie 4.0 Security“

Sprache: Deutsch, Englisch
Preis: kostenfrei

83 Handlungsempfehlungen in 17 Bereichen für die sichere und dauerhaft zuverlässige Vernetzung von Maschinen und Anlagen.

DE: https://www.vdma.org/documents/34570/1052572/
EN: https://www.vdma.org/documents/34570/4887363/

VDMA Fragenkatalog „Industrial Security – Einfach anfangen."

Sprache: Deutsch
Preis: kostenfrei, nur für Mitglieder

Einstiegshilfe in die Auswahl und Bewertung von Security-Maßnahmen für Produktionsumgebungen. Ersteinschätzung mit Hilfe von 33 Fragen.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org

VDMA Leitfaden „Informationssicherheit, Teil 1: Mitarbeitersensibilisierung"

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

https://www.vdmashop.de/executive-briefings/unternehmensfuehrung/132/leitfaden-zur-informationssicherheit/teil-1-sensibilisierung

VDMA Leitfaden „Informationssicherheit, Teil 2: ISMS, Dokumente und Vorlagen"

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

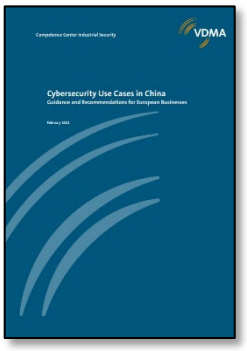
https://www.vdmashop.de/Informatik-und-Technik/Leitfaden-zur-Informationssicherheit-Teil-2---download.html

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

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

https://www.vdmashop.de/executive-briefings/unternehmensfuehrung/138/leitfaden-zur-informationssicherheit/teil-3-elektronischer-informationsaustausch-mit-externen-und

9. Publikationen zu Cybersecurity in China



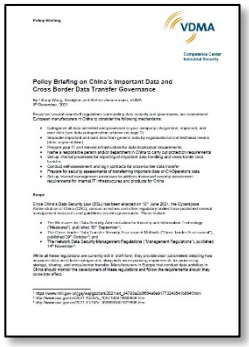
Cybersecurity Use Cases in China – Guidance and Recommendations

Sprache: Englisch
Preis: kostenfrei, nur für Mitglieder

Kleine und mittlere Unternehmen benötigen eine praktische Anleitung für Cybersecurity in China.

In fünf industrienahen Use Cases werden Fragen beantwortet und Empfehlungen ausgesprochen, mit Unterstützung von Sinolytics.

https://www.vdma.org/viewer/-/v2article/render/48588138

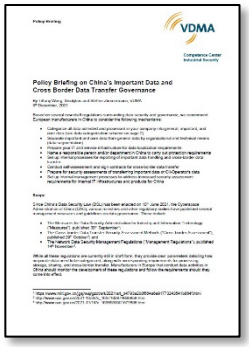


Policy Briefing on the Chinese Cross-Border Data Transfer Measures

Sprache: Englisch
Preis: kostenfrei, nur für Mitglieder

Information und Empfehlung von VDMA und Sinolytics zu den Vorgaben für den grenzüberschreitenden Datentransfer von „Important Data“ und „Personal Information“, Stand 03/2023

https://www.vdma.org/viewer/-/v2article/render/69389762

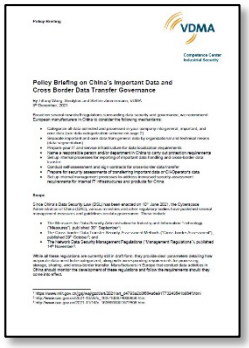


Datenschutz: Chinesische Standardvertragsklauseln (C-SCC)

Sprache: Deutsch/Englisch (Artikel)
Preis: kostenfrei, nur für Mitglieder

Die Cyberspace Administration of China (CAC) hat die C-SCC und die entsprechende Verordnung am 24. Februar 2023 veröffentlicht. Diese treten am 1. Juni 2023 in Kraft.

https://www.vdma.org/viewer/-/v2article/render/76106748

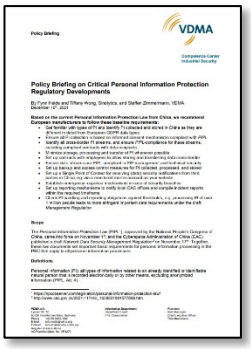


China’s Important Data and Cross Border Data Transfer Governance

Sprache: Englisch
Preis: kostenfrei, nur für Mitglieder

Informationen und Empfehlung von VDMA und Sinolytics zu Vorgaben für den Umgang mit "Important Data" und dem grenzüberschreitenden Datentransfer.

https://www.vdma.org/viewer/-/v2article/render/39322581

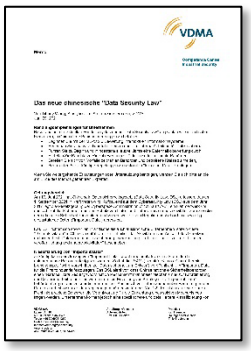


China's Personal Information Processing (PIP) Law

Sprache: Englisch
Preis: kostenfrei, nur für Mitglieder

Informationen und Empfehlung von VDMA und Sinolytics zum Ende 2021 in Kraft getretenen Gesetz zum Umgang und Schutz von personenbezogenen Daten (PIP Law).

https://www.vdma.org/viewer/-/v2article/render/39322985

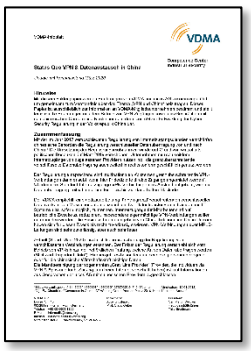


Das chinesische Data Security Law

Sprache: Deutsch, Englisch
Preis: kostenfrei, nur für Mitglieder

Das Policy Briefing von VDMA und Sinolytics nimmt die für den Maschinen- und Anlagenbau wichtigen Teile des chinesischen Datensicherheitsgesetzes genauer unter die Lupe und gibt Empfehlungen für in China operierende Mitgliedsunternehmen.

https://www.vdma.org/viewer/-/v2article/render/17569547



Status Quo VPN & Datenaustausch in China

Sprache: Deutsch, Englisch
Preis: kostenfrei, nur für Mitglieder

Mit diesem Papier werden Erfahrungen und konkrete Empfehlungen von VDMA und nicos AG zusammengeführt. Das Papier benennt zugelassene Business-Internetdienste und empfiehlt technisch/organisatorische Maßnahmen.

https://vdma.org/viewer/-/v2article/render/1301985

10. Publikationen zu Produktpiraterie

VDMA Studie „Produktpiraterie 2022“

Sprache: Deutsch/Englisch
Preis: kostenfrei

Aktuelle Studie zur Entwicklung der Produktpiraterie im Maschinen- und Anlagenbau.

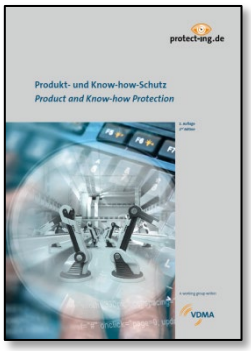
https://www.vdma.org/viewer/-/v2article/render/52232441

Leitfaden „Produkt- und Know-how-Schutz“

Sprache: Deutsch oder Englisch
Preis: kostenfrei nach Registrierung als PDF

Anleitung zum erfolgreichen Einsatz von Schutzmaßnahmen inkl. praxisnaher Beispiele.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org



Branchenführer „Produkt- und Know-how-Schutz“

Sprache: Deutsch und Englisch
Preis: kostenfrei

Beiträge zu Produktpiraterie, Security und Know-how-Schutz. Übersicht von Technologien, Schutzmaßnahmen und Lösungen in der (aufgelösten) Arbeitsgemeinschaft inkl. Matrix.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org

INS-Studie „Integratives System zur einheitlichen Kennzeichnung und Identifizierung von Maschinenbauprodukten“

Sprache: Deutsch
Preis: kostenfrei als PDF

Übersicht über Kennzeichnungstechnologien und deren Eignung für verschiedene Einsatzzwecke.

Auf Anfrage bei Biljana Gabric erhältlich: biljana.gabric@vdma.org

Piraterierobuste Gestaltung von Produkten und Prozessen

ISBN 978-3-8163-0601-6
Band 1 der Reihe „Innovationen gegen Produktpiraterie“ mit Ergebnissen aus den Projekten:

- PiratPro
- Protactive
- ProProtect

https://www.vdmashop.de/executive-briefings/unternehmensfuehrung/44/piraterierobuste-gestaltung-von-produkten-und-prozessen

Kennzeichnungstechnologien zum wirksamen Schutz gegen Produktpiraterie

ISBN 978-3-8163-0602-3
Band 2 der Reihe „Innovationen gegen Produktpiraterie“ mit Ergebnissen aus den Projekten:

- O-Pur
- EZ-Pharm
- Mobil Authent

https://www.vdmashop.de/executive-briefings/unternehmensfuehrung/45/kennzeichnungstechnologien-zum-wirksamen-schutz-gegen-produktpiraterie

Wirksamer Schutz gegen Produktpiraterie im Unternehmen

ISBN 978-3-8163-0603-0
Band 3 der Reihe Innovationen gegen Produktpiraterie mit Ergebnissen aus den Projekten:

- ProOriginal
- KoPira
- KoPiKomp
- ProAuthent

https://www.vdmashop.de/executive-briefings/unternehmensfuehrung/46/wirksamer-schutz-gegen-produktpiraterie-im-unternehmen

11. Das VDMA Competence Center Industrial Security

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 Centers ist erster Ansprechpartner für Mitglieder, Behörden und Politik. Es leistet zudem die fachliche Beratung und Unterstützung der VDMA Fachverbände und Querschnittsabteilungen.

Aktuell im VDMA in Erarbeitung befindliche Themen sind:

- Austausch mit dem Bundeskriminalamt (BKA)
- Cyber Resilience Act, NIS2
- Cybersecurity in China – Use Cases
- OT Risk Management
- Supply-Chain-Security, Software Bill of Material (SBOM)

12. Kontakt – Ihre Ansprechpartner im VDMA

Steffen Zimmermann,
Leiter Competence Center Industrial Security

Telefon: +49 69 66 03 - 19 78
Mobil: +49 170 3 38 54 40
E-Mail: steffen.zimmermann@vdma.org

Biljana Gabric
Assistentin der Geschäftsführung

Tel.: +49 69 66 03 - 13 60
E- Mail: biljana.gabric@vdma.org

Kai Kalusa,
Referent, Bundespolitische Interessenvertretung

Telefon: +49 30 30 69-4624
E-Mail: kai.kalusa@vdma.org

VDMA
Competence Center Industrial Security
Lyoner Str. 18

60528 Frankfurt am Main

Hinweis

Stand

31. Juli 2023

vdma.org/cybersecurity