Informatik

VDMA

VDMA Studie

Industrial Security 2025

Hinweis
Mit der Erhebung und Weitergabe dieser Daten durch den VDMA ist keine Empfehlung an die Mitgliedsunternehmen verbunden, die (Durchschnitts-)Werte zu übernehmen oder sich daran zu orientieren – eine individuelle Betrachtung ist für jedes Unternehmen absolut unerlässlich.

Wir haben die Angaben der Teilnehmenden mit der gewohnten Diskretion behandelt. In den folgenden Kapiteln finden Sie deshalb die Ergebnisse in anonymisierter und zusammengefasster Form wieder. Sollten Sie für die nächste Studie zu Industrial Security noch weitere Anregungen oder Fragen zur Auswertung haben, dann nehmen Sie bitte mit uns Kontakt auf.

Ansprechpartner zur Studie

Maximilian Moser
VDMA Competence Center Industrial Security
Telefon +49 69 6603-1978
E-Mail maximilian.moser@vdma.org

Dr. Alexander Giehl
Department Product Protection & Industrial Security
Fraunhofer Institute for Applied and Integrated Security AISEC
Telefon +49 89 3229986-189
E-Mail alexander.giehl@aisec.fraunhofer.de

Sebastian Peters
Department Product Protection & Industrial Security
Fraunhofer Institute for Applied and Integrated Security AISEC
Telefon +49 89 3229986-1037
E-Mail sebastian.peters@aisec.fraunhofer.de

VDMA
Lyoner Straße 18
60528 Frankfurt am Main
www.vdma.org

Stand: 01.04.2025

Vorwort

Vorwort

Prof. Claus Oetter

Maximilian Moser

In einer vernetzten, modernen Industrie darf die Security der Produktion nicht außer Acht gelassen werden: Cybercrime verursacht jährlich Schäden in Milliardenhöhe für die europäische Industrie – der Maschinen- und Anlagenbau ist davon nicht ausgenommen. Besonders in der Produktion, wo IT-Systeme mit Steuerungen und Aktorik Einfluss auf die physische Welt und damit auch auf die Beschäftigten und die Umwelt ausüben, kommt der Absicherung dieser Systeme gegenüber Cyberkriminellen und Manipulation eine besondere Bedeutung zu.

Um den aktuellen Stand der Industrial Security im Maschinen- und Anlagenbau zu erfassen und daraus Strategien zur Steigerung der Cyberresilienz der gesamten produktiven Industrie abzuleiten, hat die VDMA Abteilung Informatik in 2025 die Studie „Industrial Security“ erneut durchgeführt.

Das Fraunhofer AISEC, spezifisch die Abteilung „Product Protection & Industrial Security“, hat den VDMA bei der Auswertung und Aufbereitung der Ergebnisse unterstützt.

Die Ergebnisse der Studie zeigen ein überwiegend erfreuliches Bild: Die Cyberresilienz der befragten Unternehmen hat gegenüber der vergangenen Befragung von 2019 eindeutig zugenommen. Obwohl die Unternehmen immer mehr Angriffe und Vorfälle registrieren, haben diese nun weitaus weniger Auswirkungen auf die Produktion und die Unternehmen als 2019.

Besonders kleine und mittelständische Unternehmen (KMU), mit weniger Ressourcen für Industrial Security können vom Erfahrungsaustausch und im Verbandsnetzwerk erarbeiteten Best Practices profitieren. Durch eine zielgerichtete Industrial Security werden die Grundlagen gesichert, die für eine reibungslose Produktion nötig sind. So kann sich der Maschinen- und Anlagenbau auf seine Kernkompetenzen konzentrieren, ohne Produktionsausfälle aufgrund von Ransomware oder ähnlichen Bedrohungen befürchten zu müssen.

Prof. Claus Oetter
Abteilungsleiter
VDMA Informatik

Maximilian Moser
Referent Industrial Security,
Product Security, OT-Security

Inhalt

Management Summary

Nach 2013 und 2019 hat der VDMA mit Unterstützung des Fraunhofer AISEC in 2025 eine erneute Befragung zur Industrial Security des Maschinen- und Anlagenbaus 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 54 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 (32 Prozent) und Produktionsausfälle (29 Prozent). Safety-relevante Auswirkungen (Gefährdung von Mensch oder Umwelt) sind in den vergangen zwei Jahren erfreulicherweise nicht registriert worden. Der Anteil der betroffenen Unternehmen mit Produktionsausfällen unterstreicht die Notwenigkeit von Industrial Security neben der „klassischen“ IT-Security in den Unternehmen.

- Obwohl die Zahl der Cybersecurity-Vorfälle im Vergleich zur VDMA Studie Industrial Security von 2019 gestiegen ist, haben diese weniger Auswirkungen bei den betroffenen Unternehmen gezeigt, als im Jahr 2019. Dies spricht für eine wachsende Cyberresilienz der Unternehmen.

- Zu den Bedrohungen mit der höchsten Risikoeinschätzung gehören erstmalig „Social Engineering und Phishing“ (Platz 1) sowie „Menschliches Fehlverhalten und Sabotage“ (Platz 2). Neu hinzugekommen in die Liste der Top 10 Bedrohungen ist die Thematik „Soft- und Hardwareschwachstellen in der Lieferkette“ auf Platz 3. Dass der Faktor Mensch Platz 1 und 2 belegt, spricht für ein Vertrauen in technische Securitymaßnahmen und unterstreicht den Nutzen von Cybersecurity Awareness Trainings in der Produktion.

- Mittlerweile kennen 93 Prozent der Unternehmen einen der gängigen Security-Standards und knapp die Hälfte (52 Prozent) wendet diese auch an. Insbesondere mangelndes Know-how ist jedoch noch ein Hindernis für den Einsatz, vornehmlich bei kleineren und mittelständischen Unternehmen (bis 250 Mitarbeitende) wird dieser Umstand deutlich. Gerade kleine und mittelständische Unternehmen müssen unterstützt werden, um ihr Security Know-how weiter auszubauen.

- Bei der Etablierung eines Risikomanagements im Produktionsumfeld gibt es noch Handlungsbedarf. Erst 61 Prozent haben ein solches eingeführt. Das Risikomanagement bietet die Grundlage für die effektive wirtschaftliche Implementierung von Cybersecuritymaßnahmen. Eine gezielte Abschätzung von Ausfallkosten bei Security-Vorfällen spielt nach wie vor für rund drei Viertel der Unternehmen keine Rolle.

- Vom Cyber Resilience Act (CRA) und der Netzwerk- und Informationssicherheitsdirektive 2 (NIS2) sind die befragten Unternehmen vielfach direkt betroffen. Rund zwei Drittel (68 Prozent) werden aufgrund der Tätigkeit als Servicedienstleister, Komponentenlieferant oder Integrator davon berührt.

- Nur 8 Prozent der Unternehmen können sich bisher ein Security-Gütesiegel als „generell verpflichtendes Entscheidungskriterium“ für den Produkteinkauf vorstellen. Security ist jedoch ein Lifecycle-Thema: Schwachstellen können auch während der Verwendung eines Produktes identifiziert werden. Ein beim Verkauf angebrachtes Gütesiegel könnte so also gegebenenfalls rasch seine Bedeutung verlieren.

Die nachfolgenden Seiten vermitteln einen detaillierten Einblick in die Ergebnisse der Befragung.

1. Einführung

Der VDMA erstellt regelmäßig Studien zur Ermittlung der Cyberresilienz im Maschinen- und Anlagenbau. In diesem Jahr wurde die Studie „Industrial Security“ erneut durchgeführt, um dem Umstand der gestiegenen digitalen Vernetzung in den Produkten und den verbundenen digitalen Bedrohungen Rechnung zu tragen. Dies bestätigen auch die Umfrageergebnisse: 99 Prozent der befragten Unternehmen setzen Cybersecurity-Maßnahmen zur Absicherung ihrer Betriebsstätte gegen Angriffe ein.

Definition 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 so der Begriff „Security“ als „Schutz der Maschine vor dem Menschen“ beschreiben. Dabei ist dieser klar vom Begriff „Safety“ abzugrenzen: Dabei geht es um die Sicherheit des Menschen, also „Schutz des Menschen vor der Maschine“.

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. 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.

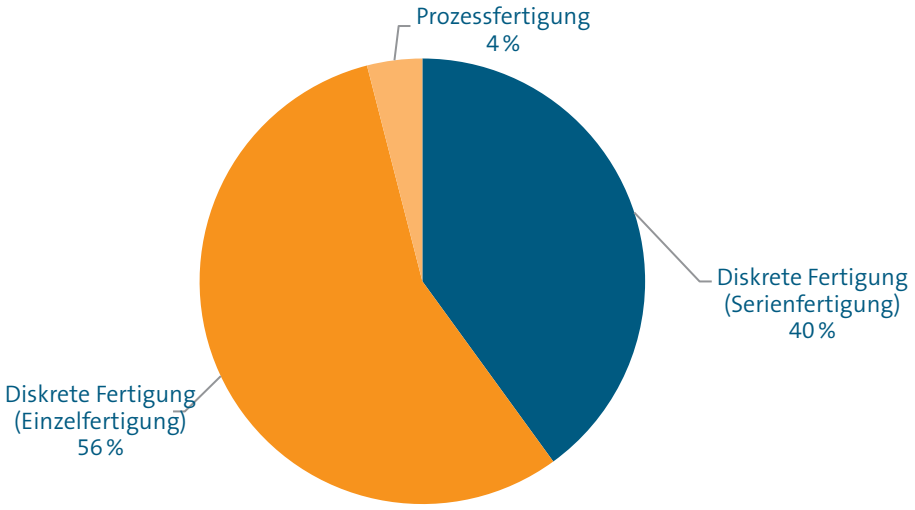
Struktur der teilnehmenden Unternehmen

An der Studie haben insgesamt 79 Unternehmen teilgenommen. Vier davon besitzen keine eigene Produktions- oder Fertigungsumgebung. Deren Antworten werden deshalb in den weiteren Betrachtungen nicht mitberücksichtigt. Von den 75 produzierenden Firmen hat die Mehrheit eine diskrete Fertigung (96 Prozent). Lediglich 4 Prozent sind Unternehmen mit einer Prozessfertigung. Die weitere Verteilung nach Unternehmensumsatz und -größe innerhalb der Studie sind in Abbildung 2 und Abbildung 3 dargestellt.

Abbildung 1

Struktur der teilnehmenden Unternehmen nach Fertigungsart

N = 75

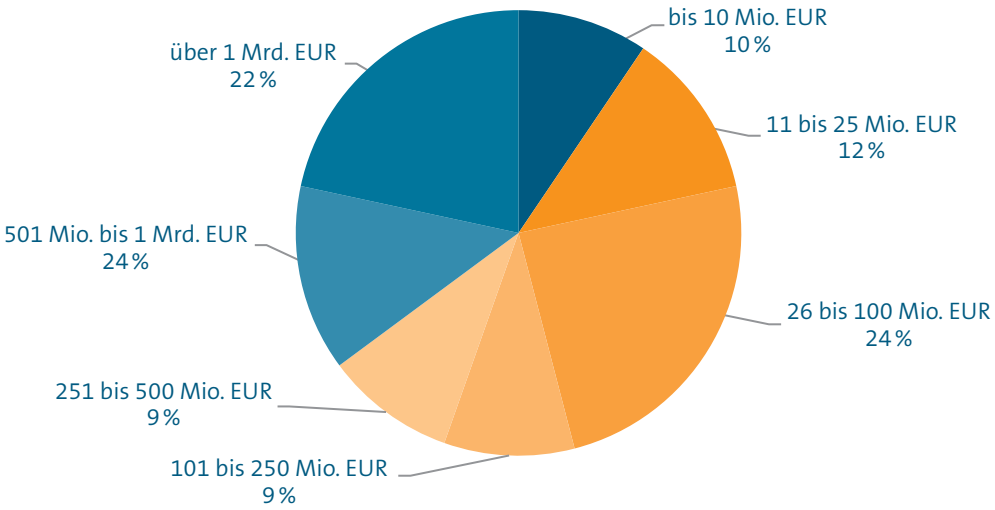


Quelle: VDMA

Abbildung 2

Struktur der teilnehmenden Unternehmen nach Jahresumsatz

N = 74

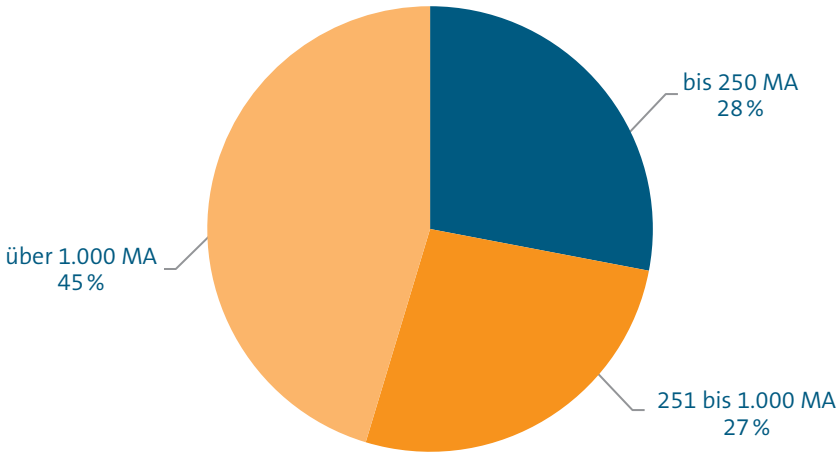


Quelle: VDMA

Abbildung 3

Struktur der teilnehmenden Unternehmen nach Anzahl der Mitarbeitenden

N = 75



Quelle: VDMA

3. Security-Beauftragte in der Produktion

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 einer oder mehrerer qualifizierter Personen durch die Firmenleitung.

Im Vergleich zur Studie von 2019 gibt es mittlerweile bei der Mehrzahl der Unternehmen aus dem Maschinen- und Anlagenbau eine Beauftragte oder einen Beauftragten für die Security in der Produktion (2025: 58 Prozent; 2019: 42 Prozent). Weiterhin planen bis 2027 rund 13 Prozent der Befragten, in diesem Bereich „nachzurüsten“. In Unternehmen mit mehr als 1.000 Mitarbeitenden haben nun 73 Prozent der Unternehmen Personen für die Industrial Security beauftragt (2019: 68 Prozent) und weitere 9 Prozent planen, dies in den kommenden Jahren zu tun.

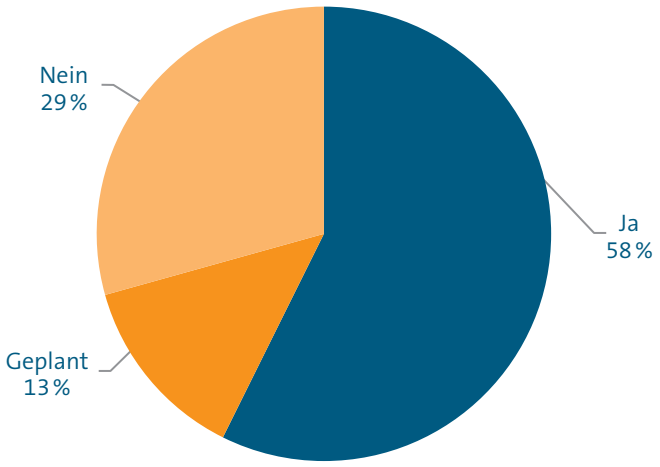
Dabei setzen die Unternehmen weiterhin verstärkt auf die Kompetenz des eigenen Personals. Gegenüber 2019 hat sich dieser Trend weiter verfestigt und die Eigenkompetenz ist vermehrt in den Unternehmen zu finden. Nur noch 12 Prozent der Befragten haben externe Dienstleister dafür beauftragt.

Bei Unternehmen mit weniger als 1.000 Mitarbeitenden ist überwiegend nur eine Person für Industrial Security verantwortlich, niemals aber mehr als fünf Personen. Großunternehmen mit über 1.000 Mitarbeitenden setzen zum Teil deutlich mehr Personen für Industrial Security ein. Zudem haben Großunternehmen im Vergleich zu den kleineren Unternehmen bei den Mitarbeitenden mit dem Aufgabenschwerpunkt Security aufgestockt. 82 Prozent der Unternehmen mit mehr als 1.000 Mitarbeitenden verzeichneten Neueinstellungen. Bei Unternehmen mit weniger als 1.000 Mitarbeitenden waren es dagegen nur 20 Prozent.

Abbildung 4

Gibt es in Ihrem Unternehmen beauftragte Personen für die Security in der Produktion?

N = 75



Quelle: VDMA

Organsatorisch sind Security-Beauftragte über alle Unternehmensgrößen hinweg zumeist (42 Prozent) der IT-Abteilung zugeordnet. Unternehmen mit weniger als 1.000 Mitarbeitenden setzen mit einem Anteil von 47 Prozent sogar noch stärker auf dieses Modell. In den meisten Fällen (64 Prozent) übernimmt der IT-Sicherheitsverantwortliche (ISB/CISO) diese Aufgabe mit und übt damit eine Doppelfunktion aus.

Die Übertragung von „klassischem“ IT-Security-Know-how in das Produktionsumfeld ist also durchaus praktikabel, auch wenn in der Produktion verschiedene Eigenheiten bestehen: Safety kommt als weiteres Schutzziel hinzu, der Gerätepark ist wesentlich heterogener als in der IT und die Standzeiten von Maschinen und Anlagen sind im Allgemeinen wesentlich länger als die Lebenszeit von Clients und Servern in der IT. Diesen Wissenstransfer unterstützt der VDMA stetig, beispielsweise mit der Publikation „OT-Risiko Kochbuch“.

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 93 Prozent der befragten Unternehmen eine Security-Richtlinie ein, die restlichen planen dies bis 2027 umzusetzen.

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.

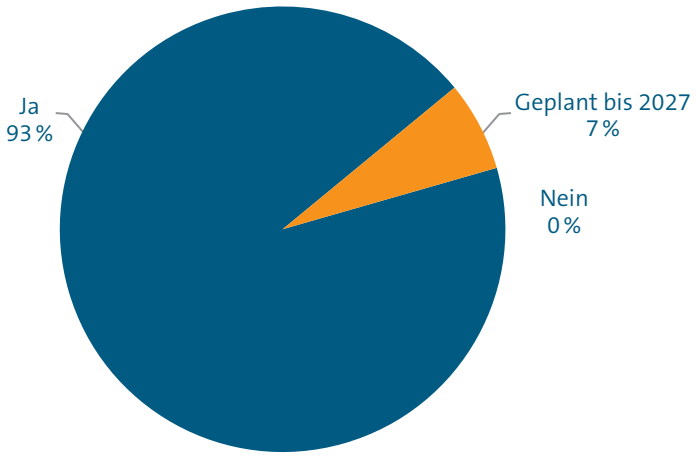
Sind die Security-Richtlinien für Büroumfeld, Produktion und Produktentwicklung identisch, so ist davon auszugehen, dass ein Großteil der Richtlinien ursprünglich aus dem Büroumfeld stammt. In diesen Fällen enthalten die Richtlinien oft nur wenige spezifische Aspekte für die Security in der Produktion. Dies fällt besonders bei Unternehmen bis 1.000 Mitarbeitende auf, die zu mehr als 37 Prozent (2019: 50 Prozent) abgestimmte und identische Richtlinien einsetzen.

Bei rund einem Viertel der Unternehmen sind die Security-Richtlinien immer noch unabgestimmt. Bei Unternehmen bis 1000 Mitarbeiter herrscht

Abbildung 5

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

N = 46



Quelle: VDMA

hier ein gewisser Nachholbedarf, obwohl sich die Gesamtlage seit 2019 verbessert hat. Für eine gut funktionierende Abstimmung ist die Einbindung aller betroffenen Parteien wichtig, sowohl der Beschäftigten aus den verschiedenen Unternehmensbereichen als auch des Datenschutzbeauftragten und des Betriebsrats.

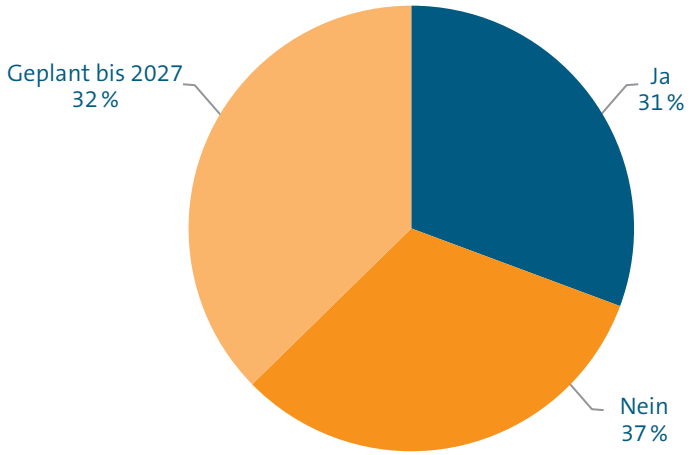
Die befragten Unternehmen (29 bzw. 27 Prozent) verfügen bereits heute über separate Richtlinien und 31, bzw. 42 Prozent der Unternehmen plant bis 2027 die Einführung separater Richtlinien nachzuholen. Insbesondere bei kleinen Unternehmen (unter 250 Mitarbeitende) ist mit zwei Dritteln keine Einführung separater Richtlinien in Planung. Separate Security-Richtlinien sind jedoch sinnvoll, da sie unterschiedliche Risiken und spezifische Anforderungen adressieren. Sie ermöglichen z.B. eine gezielte Berücksichtigung unterschiedlicher gesetzlicher Vorgaben.

Erfreulicherweise zeigt sich bei den Prüfungen zur Einhaltung der Security-Richtlinie für die Produktion ein deutlich positiver Trend. Rund 64 Prozent (2019: 56 Prozent) führen bereits (regelmäßige) Prüfungen durch. Zusätzlich wird dies noch durch schriftliche Verpflichtungen und unangekündigte, stichprobenartige Prüfungen unterstützt.

Abbildung 6

Gibt es in Ihrem Unternehmen eine Security-Richtlinie für die eigene Produktion?

N = 75

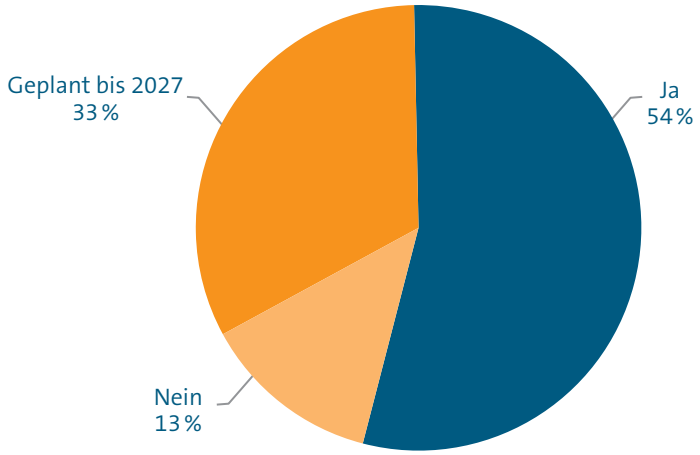


Quelle: VDMA

Abbildung 7

Gibt es in Ihrem Unternehmen eine Security-Richtlinie für die eigene Produktentwicklung?

N = 46

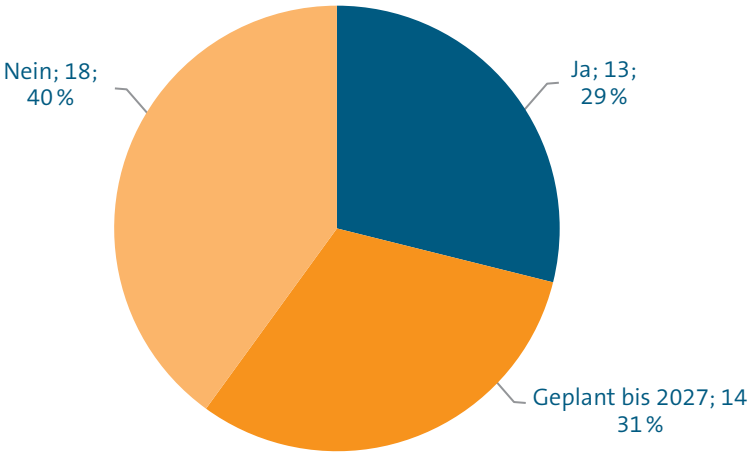


Quelle: VDMA

Abbildung 8

Existieren separate Security-Richtlinien für Einkauf/Beschaffung von Komponenten, Maschinen oder Anlagen?

N = 45

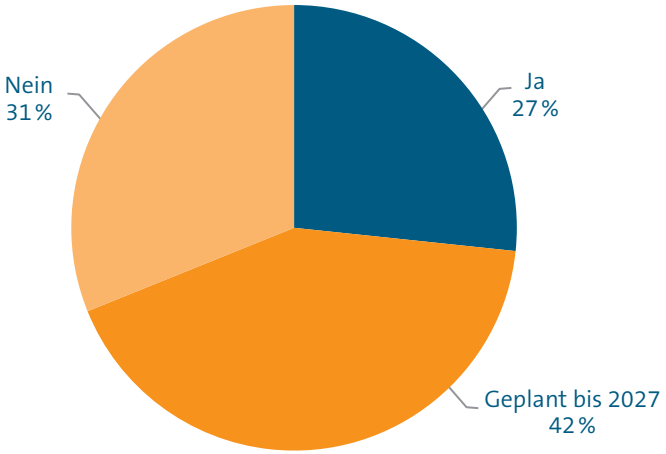


Quelle: VDMA

Abbildung 9

Existieren separate Security-Richtlinien für externe Dienstleister (Anlagenhersteller, Servicetechniker etc.)?

N = 46



Quelle: VDMA

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.).

Auch im Hinblick auf Cybersecurity Regularien wie der NIS2 und CRA ist das Risikomanagement unabdingbar, um effektiv Produkte und Produktionsumgebungen abzusichern. Nur über eine Risikobewertung kann in Abhängigkeit der identifizierten Bedrohungen und Angriffsvektoren festgestellt werden, welche Cybersecuritymaßnahmen geeignet bzw. wirtschaftlich für Unternehmen und Produkte sind.

Bisher haben im Durchschnitt 61 Prozent der befragten Unternehmen im Produktionsumfeld ein Risikomanagement eingeführt (2019: 41 Prozent). Vorreiter sind in diesem Fall die mittelgroßen Unternehmen (251 bis 1.000 Mitarbeitende) mit 70 Prozent. Einen deutlichen Nachholbedarf zeigen dagegen noch die kleinen Unternehmen (bis 250 Mitarbeitende). Der heutige Anteil von 45 Prozent (2019: 26 Prozent) soll sich nach Planung der Unternehmen bis 2027 aber auf 60 Prozent erhöhen.

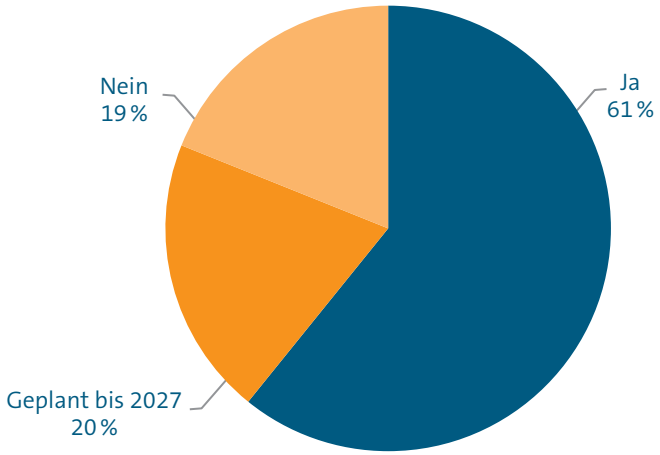
Auch wenn noch kein vollständiges Risikomanagement etabliert wurde, ist mit einer Risikoanalyse bereits der Anfang gemacht, um die Bedrohungslage besser einschätzen zu können. Mehr als die Hälfte der befragten Unternehmen (60 Prozent) hat eine entsprechende Analyse schon durchgeführt und verfügt in neun von zehn Fällen über einen vollständigen oder zumindest teilweisen Einblick in die Bedrohungslage für die eigene Produktionsumgebung.

Mehr als ein Drittel (39 Prozent) der befragten Unternehmen führt keine regelmäßigen Security-Audits im Produktionsumfeld durch. Genauso viele führen immerhin Security-Audits in unregelmäßigen Abständen durch. Nur eine Minderheit der Unternehmen führt dies regelmäßig durch (22 Prozent). Rund die Hälfte der Unternehmen (53 Prozent) verfügen darüber hinaus über keine Abschätzung zu Ausfallkosten bei Security-Vorfällen (z.B. Kosten pro Ausfallstunde). Insbesondere Unternehmen mit weniger als 1.000 Mitarbeitenden tun sich hier mit zwei Dritteln hervor. Dem Management von rund der Hälfte der Unternehmen (53 Prozent) sind diese Berechnungen, falls sie durchgeführt werden, auch nicht bekannt.

Abbildung 10

Ist im Produktionsumfeld des Unternehmens ein Risiko-management etabliert?

N = 74

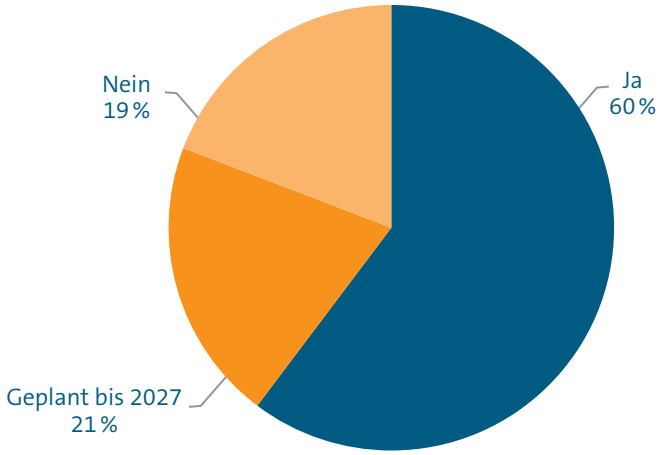


Quelle: VDMA

Abbildung 11

Wurde eine Risikoanalyse durchgeführt?

N = 73

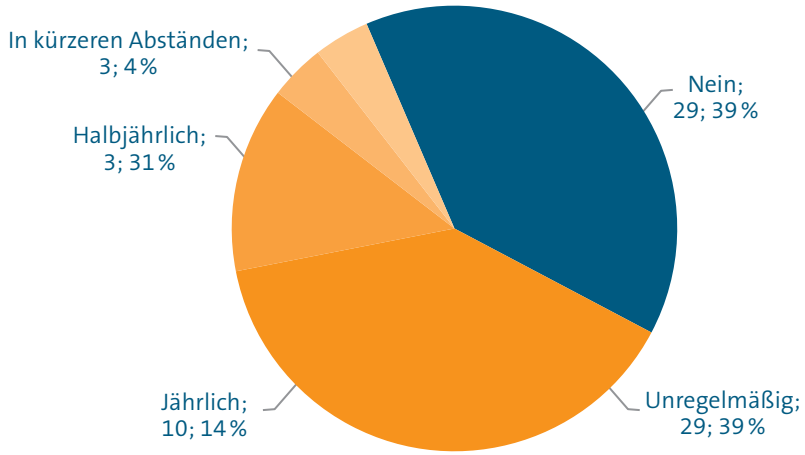


Quelle: VDMA

Abbildung 12

Werden regelmäßige Security-Audits im Produktionsumfeld durchgeführt?

N = 74

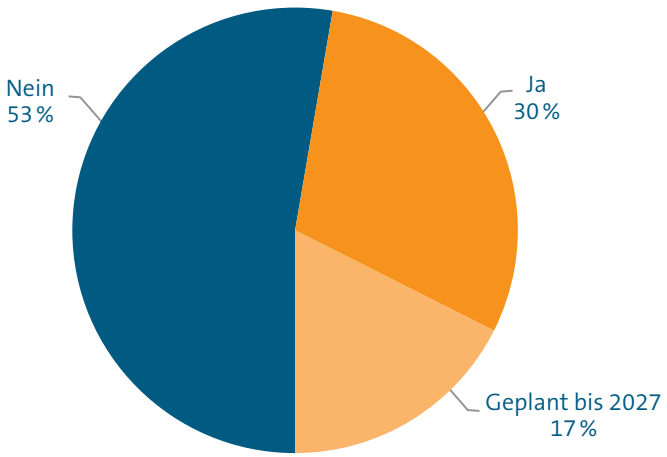


Quelle: VDMA

Abbildung 13

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

N = 74



Quelle: VDMA

6. TOP 10 Bedrohungen

Ausgehend von dem im Jahr 2022 veröffentlichten Dokument des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum Thema „Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen“[1] wurden die Teilnehmerinnen und 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):

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten
- Social Engineering und Phishing

Die befragten Unternehmen schätzen die Bedrohungslage im Durchschnitt eher als „mittel“ ein. Den höchsten Wert mit rund 3,4 erreicht dabei „Social Engineering und Phishing“. 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.

Dass die Eintrittswahrscheinlichkeiten von „Social Engineering und Phishing“ sowie „Menschliches Fehlverhalten und Sabotage“ die obersten Plätze belegen, zeigt, dass zumindest subjektiv in den Unternehmen verstärkt der Mensch in den Fokus der Betrachtung gerät. Hieraus ergibt sich auch die Notwendigkeit für organisatorische Maßnahmen wie beispielsweise Security Policies und Security Awareness Trainings spezifisch für Produktionsmitarbeiter, um über Bedrohungen aufzuklären und für das richtige Verhalten zu sensibilisieren.

1 https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html

Abbildung 14

Wie schätzen Sie die Eintrittswahrscheinlichkeit für folgende Bedrohungen in Ihrem Unternehmen ein?

N= zwischen 74 und 75

Quelle: VDMA

7. Security-Vorfälle

Dass die Anzahl der Security-Vorfälle in Zukunft zurückgeht, ist für die Mehrheit der befragten Unternehmen unwahrscheinlich. 89 Prozent (2019: 90 Prozent) der Unternehmen erwarten ein gleichbleibendes oder ansteigendes Niveau. Trotz dieser gleichbleibenden Betroffenheit von Vorfällen gehen die negativen Auswirkungen zurück: Nur noch 55 Prozent der Maschinen- und Anlagenbauunternehmen verzeichnen solche. Im Jahr 2019 galt dies noch in mehr als zwei Dritteln aller Fälle. Damit ergibt sich ein positives Bild, was die Steigerung der Cyberresilienz unter den VDMA-Mitgliedsfirmen angeht.

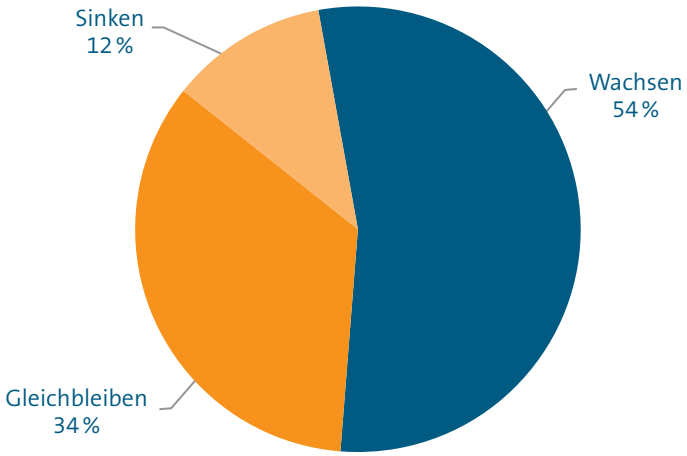
Die aktuell von den Unternehmen angegebenen Vorfälle spiegeln mit hoher Wahrscheinlichkeit jedoch nicht die tatsächliche Anzahl an Vorkommnissen wider. Auch wenn derzeit 68 Prozent (2019: 57 Prozent) der Unternehmen Maßnahmen ergriffen haben, um Security-Vorfälle zu erkennen, bleiben die restlichen Unternehmen noch im Unklaren. Neben der Tatsache, dass aus Compliance-Gründen oder der Angst vor einem 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 2019 zeigt sich eine deutlich gemischtere Bedrohungslandschaft für die Unternehmen. Zufällige externe Einflüsse (z.B. durch ungerichtete E-Mails mit Viren) mit 36 Prozent (2019: 47 Prozent) sind immer noch vorrangig zu nennen. Auf den weiteren Plätzen folgen als Ursachen die „Innentäter“ mit 31 Prozent (2019: 38 Prozent) und die gezielten externen Einflüsse mit 33 Prozent (2019: 26 Prozent). Letztere konnten teilweise (49 Prozent) durch die Unternehmen zurückverfolgt werden. Ein Grund mag darin liegen, dass bei knapp zwei Dritteln (65 Prozent) der betroffenen Unternehmen, die gezielt „attackiert“ wurden, externe Beratungsstellen wie Ver-

Abbildung 15

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

N = 61



Quelle: VDMA

fassungsschutz, spezialisierte Sicherheitsdienstleister oder Polizeibehörden hinzugezogen wurden.

Weiterhin unterstreicht die heterogene Bedrohungslandschaft die Notwendigkeit von ganzheitlichen Securitykonzepten, welche beispielsweise interne und externe Bedrohungen gleichermaßen beachten.

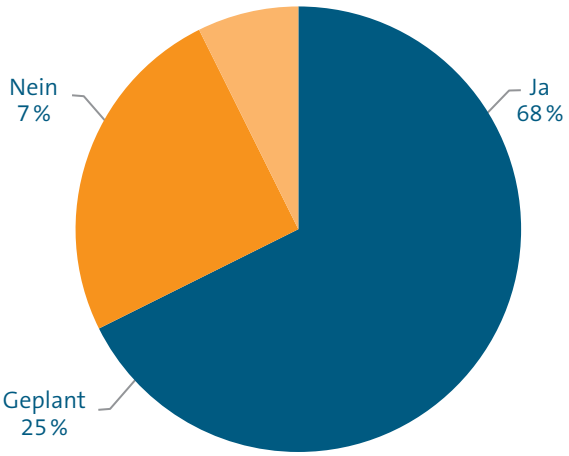
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat 2012 unter anderem für den Austausch von Meldungen zu Security-Vorfällen die „Allianz für Cybersicherheit“ gegründet. Auch wenn diese zentrale Meldestelle deutlich bekannter geworden ist (2019: 70 Prozent, 2025: 85 Prozent), hat dort bisher nur ein kleiner Anteil der Unternehmen (12 Prozent) entsprechende Vorfälle gemeldet. Immerhin würde die große Mehrheit der befragten Unternehmen (91 Prozent) dort weiter Security-Vorfälle melden.

Treten Security-Vorfälle ein, dann sind die Auswirkungen oft weitreichend. So werden bei jedem dritten Unternehmen (32 Prozent) bereits heute entsprechende Kapitalschäden verursacht. An zweiter und dritter Stelle folgen mit 29 Prozent Produktionsausfall und mit 16 Prozent Imageschäden. Auch eine Gefährdung von Maschinen und Anlagen 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. Auch Umweltschäden wurden nicht verzeichnet.

Abbildung 16

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

N = 68

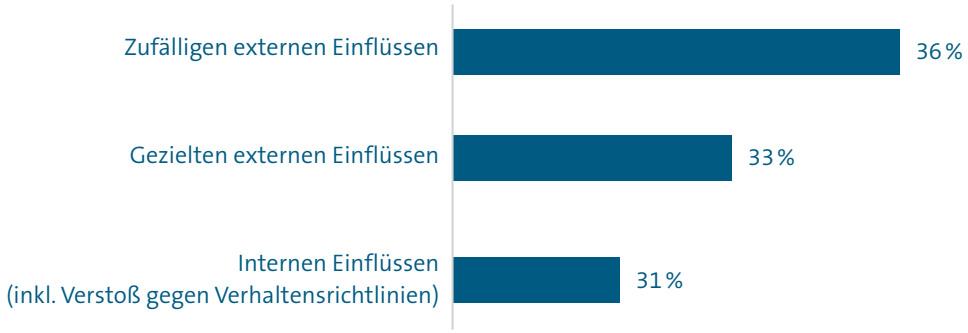


Quelle: VDMA

Abbildung 17

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

N = 33



Quelle: VDMA

Abbildung 18

Wie haben sich die Security-Vorfälle ausgewirkt?

N = 67, Mehrfachantworten möglich

Quelle: VDMA

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.

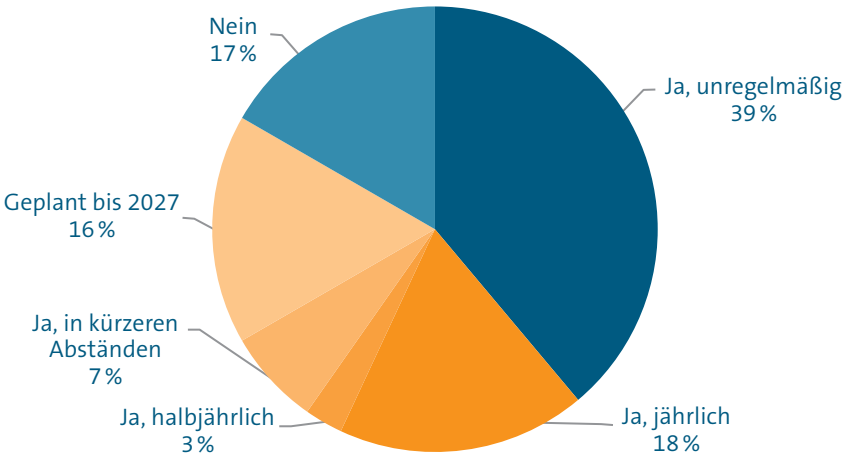
Trotz einer vorhandenen Security-Richtlinie für die Produktion überprüfen erst rund drei von zehn Unternehmen die Security im Maschinen- und Anlagennetzwerk regelmäßig (2025: 28 Prozent, 2019: 23 Prozent). Unregelmäßige Prüfungen stellen mit 39 Prozent immer noch die Mehrheit dar (2019: 35 Prozent), was eher auf Reaktion statt Aktion hindeutet. 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. Wird eine Prüfung durchgeführt, verlassen sich rund zwei Drittel (65 Prozent) aller befragten Unternehmen auf eigenes Personal statt auf externe Prüferinnen oder Prüfer.

Ebenfalls haben über zwei Drittel der Unternehmen (69 Prozent) bereits ein Notfallmanagement eingerichtet, um im Krisenfall auf Security-Bedro-

Abbildung 19

Wird die Einhaltung der in Ihrem Unternehmen ergriffenen Security-Maßnahmen überprüft?

N = 72

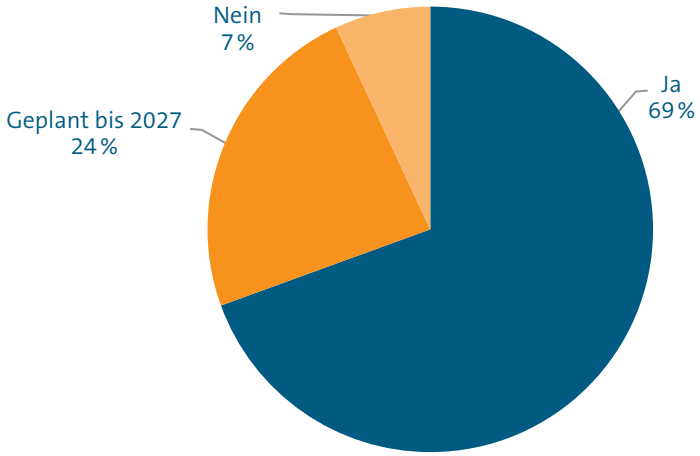


Quelle: VDMA

Abbildung 20

Ist in Ihrem Unternehmen ein Notfallmanagement eingerichtet?

N = 72

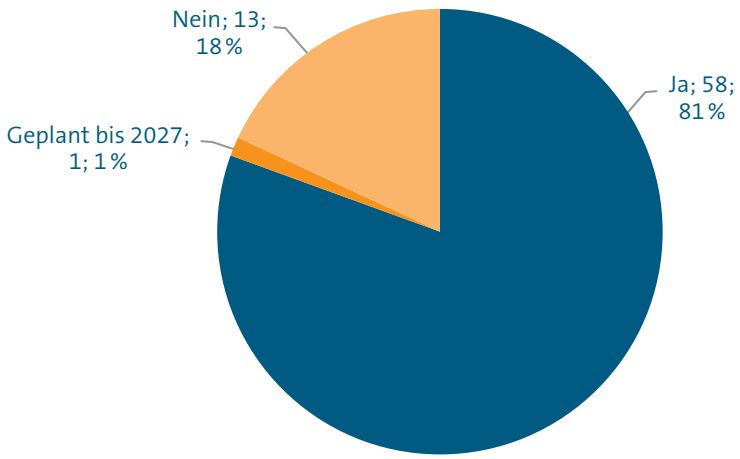


Quelle: VDMA

Abbildung 21

Gibt es in Ihrem Unternehmen ein Budget für die Security der Office-IT?

N = 72



Quelle: VDMA

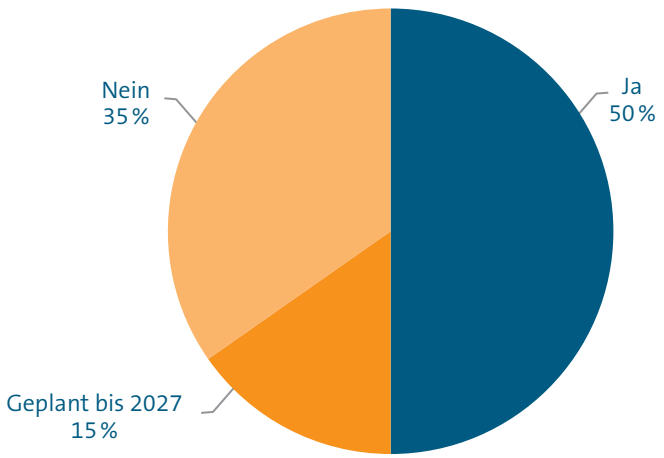
hungen reagieren zu können. Es zeigt sich aber auch, dass insbesondere bei kleinen Unternehmen (bis zu 250 Mitarbeitende) nur 42 Prozent über solch ein Notfallmanagement verfügen. Ein Fünftel der kleinen Unternehmen (21 Prozent) plant auch nicht, ein solches einzuführen. Dies schränkt im Notfall den Handlungsspielraum für kleine Unternehmen weiter ein. Ist ein solches Notfallmanagement eingerichtet, werden die Maßnahmen aber nicht unweigerlich getestet. Weniger als die Hälfte (42 Prozent) der befragten Unternehmen hat die eigenen Notfallmaßnahmen bereits getestet. Immerhin plant noch ein Viertel (26 Prozent) dies in den nächsten beiden Jahren zu tun. Auch eine Dokumentation von Security-relevanten Vorfällen wird nur bei rund der Hälfte der Unternehmen (54 Prozent) gepflegt.

Bei den verfügbaren Mitteln für Security in der Produktion zeigen sich ebenfalls Unterschiede bei den befragten Unternehmen. So haben 81 Prozent ein dediziertes Budget für die Office IT, aber lediglich 50 Prozent verfügen auch über eigene Geldmittel für die Security in der Produktions-IT. Bei kleinen Unternehmen (bis 250 Mitarbeitende) sind dies sogar nur 16 Prozent. Immerhin plant etwas mehr als die Hälfte aller befragten Unternehmen (53 Prozent) mit einem insgesamt wachsenden Budget für Security. Nur sehr wenige (3 Prozent) rechnen dagegen mit einem sinkenden Security-Budget.

Abbildung 22

Gibt es in Ihrem Unternehmen ein Budget für die Security der Produktions-IT?

N = 72



Quelle: VDMA

9. Organisatorische Schutzmaßnahmen

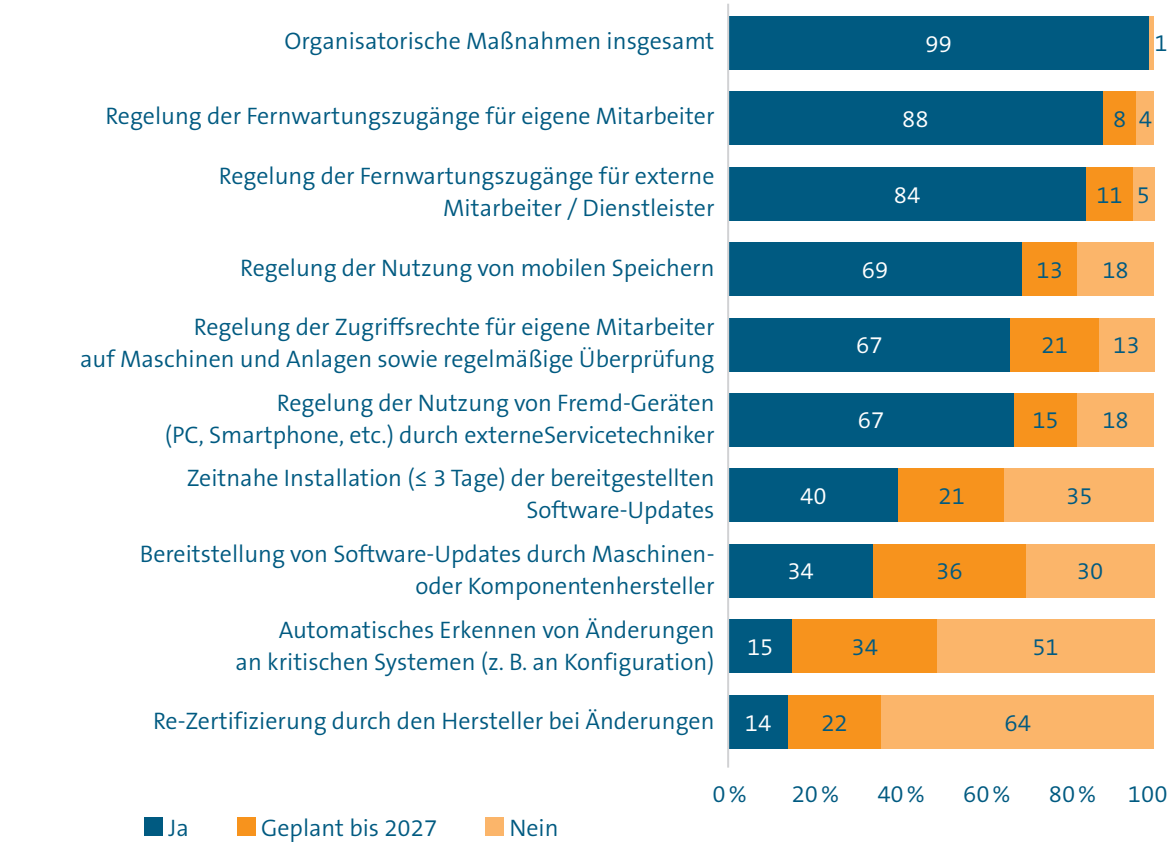
Organisatorische Maßnahmen sind die Grundvoraussetzung, um menschliches Fehlverhalten im gesamten Lebenszyklus einer Anlage zu minimieren und somit Fehler zu vermeiden. Für spezielle Bereiche, in denen konkrete Regelungen notwendig sind, müssen gegebenenfalls gesonderte Richtlinien und Maßnahmen genutzt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

Bereits 99 Prozent der Unternehmen wenden organisatorische Maßnahmen an. Dabei ist ein breites Spektrum an Sicherheitsmaßnahmen in Gebrauch. Die jeweiligen Aktivitäten sollten dabei in Relation zur unternehmensspezifischen Bedrohungslage stehen.

Abbildung 23

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

N = 71 bis 75



Quelle: VDMA

10. Technische Schutzmaßnahmen

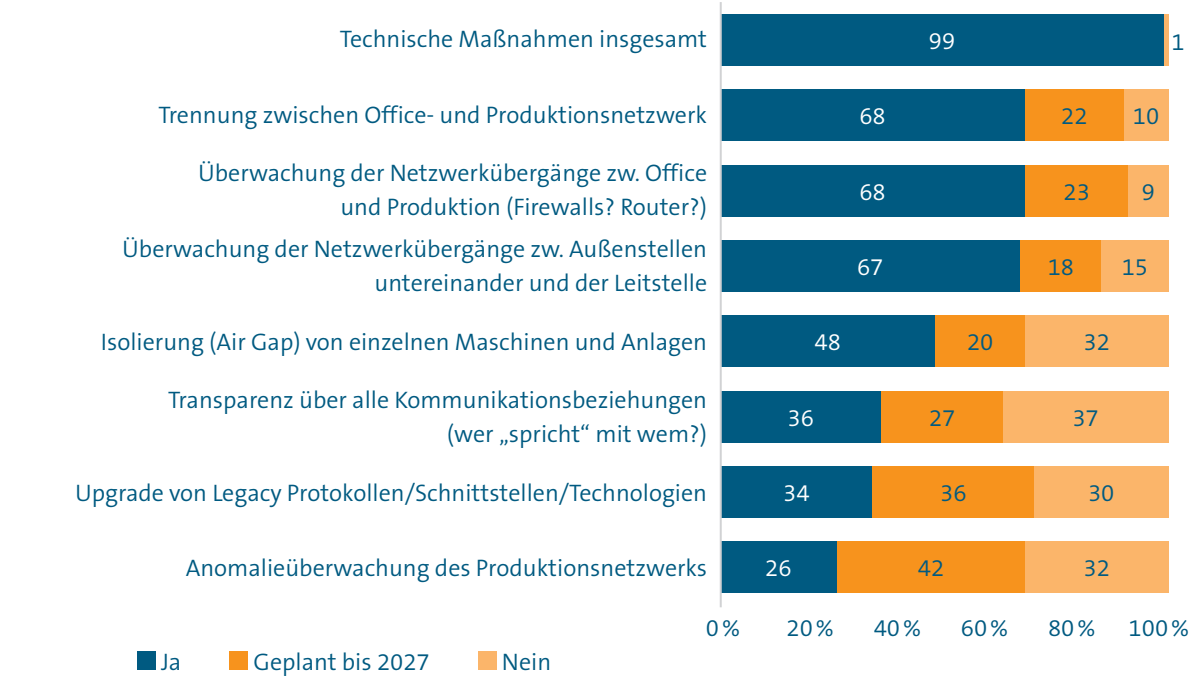
Technische Maßnahmen zum Schutz von Produktion, Maschinen und Anlagen dienen der Unterstützung von organisatorischen Maßnahmen, können diese jedoch nicht ersetzen. Schwierig ist zudem, dass gängige Maßnahmen der IT-Sicherheit in der Produktionsumgebung oft nicht direkt angewendet werden können.

Beim Einsatz der technischen Maßnahmen zeigt sich ein etwas diffuses Bild. 99 Prozent der Unternehmen nutzen bereits technische Maßnahmen, aber typische Maßnahmen, wie die Trennung zwischen Office- und Produktionsnetzwerk, werden erst bei 68 Prozent (2019: 60 Prozent) der befragten Unternehmen 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.

Abbildung 24

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

N = 71 bis 75



Quelle: VDMA

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 zu schützender 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 2022 überarbeitet.[2]

BSI Grundschutz
Der IT-Grundschutz des BSI 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 von 2022 als „IT-Grundschutz-Kompendium“ sind spezifische Bausteine für industrielle Komponenten (IND) enthalten. [3]

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. [4]

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. [5] Die IEC Standardreihe wird als Grundlage für Security im Bereich Industrie 4.0/IoT angesehen und ist in Teilen bereits zertifizierbar (Produkte, Prozesse). [6]

Dieses Jahr wurden darüber hinaus noch folgende Standards neu abgefragt:

2 https://www.iso.org/standard/27001
3 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
4 https://www.vdi.de/richtlinien/
5 https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/vdma-security-automation.html
6 https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung

TISAX
Der Trusted Information Security Assessment Exchange ist ein Standard für die Informationssicherheit in der Automobilindustrie. Er ermöglicht Unternehmen, Sicherheitsbewertungen auszutauschen und zu vergleichen. Der Schwerpunkt liegt auf dem Schutz sensibler Daten und der Einhaltung von Datenschutzanforderungen. TISAX stellt sicher, dass die Informationssicherheit in der gesamten Lieferkette eingehalten wird, was auch für Unternehmen des Maschinen- und Anlagenbaus relevant ist, insbesondere wenn sie in der Automobilindustrie tätig sind oder mit Unternehmen aus diesem Sektor zusammenarbeiten. [7]

DIN SPEC 27076
Die DIN SPEC 27076 bietet Richtlinien für die Informationssicherheit in der Automatisierungstechnik. Sie richtet sich speziell an kleine und mittelständische Unternehmen mit dem Ziel, das IT-Schutzniveau dieser Unternehmen anzuheben. Unternehmen werden bei der Implementierung geeigneter Sicherheitsmaßnahmen unter anderem mit einem „CyberRisikoCheck“ unterstützt. [8]

TRBS 1115-1
Die Norm für „Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ beschreibt die sicherheitstechnischen Anforderungen an Maschinen und Anlagen. Der Fokus liegt auf der Identifikation von Gefährdungen und der Umsetzung geeigneter Schutzmaßnahmen zur Gewährleistung der Sicherheit im Betrieb. [9]

EN 18031-1/2/3
Die EN 18031 behandelt die Sicherheitsanforderungen für Funkanlagen und kann auch für Maschinen und Anlagen in verschiedenen Anwendungsbereichen angewendet werden. [10]

Gegenüber 2019 ist es erfreulich, dass die Bekanntheit von Security-Standards (2025: 93 Prozent, 2019: 83 Prozent) deutlich zugenommen hat. Nachholbedarf zeigt sich nach wie vor bei der Anwendung der meisten Standards. Die meisten der Unternehmen, denen ein Standard bekannt ist, nutzen diesen nur zu 58 Prozent (2019: 40 Prozent). Es 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.

Die höchste durchschnittliche Durchdringung in der Anwendung verbuchen nach wie vor mit 52 Prozent (2019: 30 Prozent) der BSI IT-Grundschutz und mit 39 Prozent (2019: 26 Prozent) die ISO/ IEC-27000er-Reihe. Bei Unternehmen mit weniger als 250 Mitarbeitenden wenden bisher nur 10 Prozent (2019: 6 Prozent) der Befragten einen der beiden Standards an. Vor allem die mangelnde Kenntnis über Standards verhindert in kleineren Unternehmen oft noch eine entsprechend höhere Nutzung.

7 https://portal.enx.com/de-de/TISAX/
8 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/KMU/CyberRisikoCheck/CyberRisikoCheck_node.html
9 https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1
10 https://www.dinmedia.de/de/norm/sn-en-18031-1/384588571

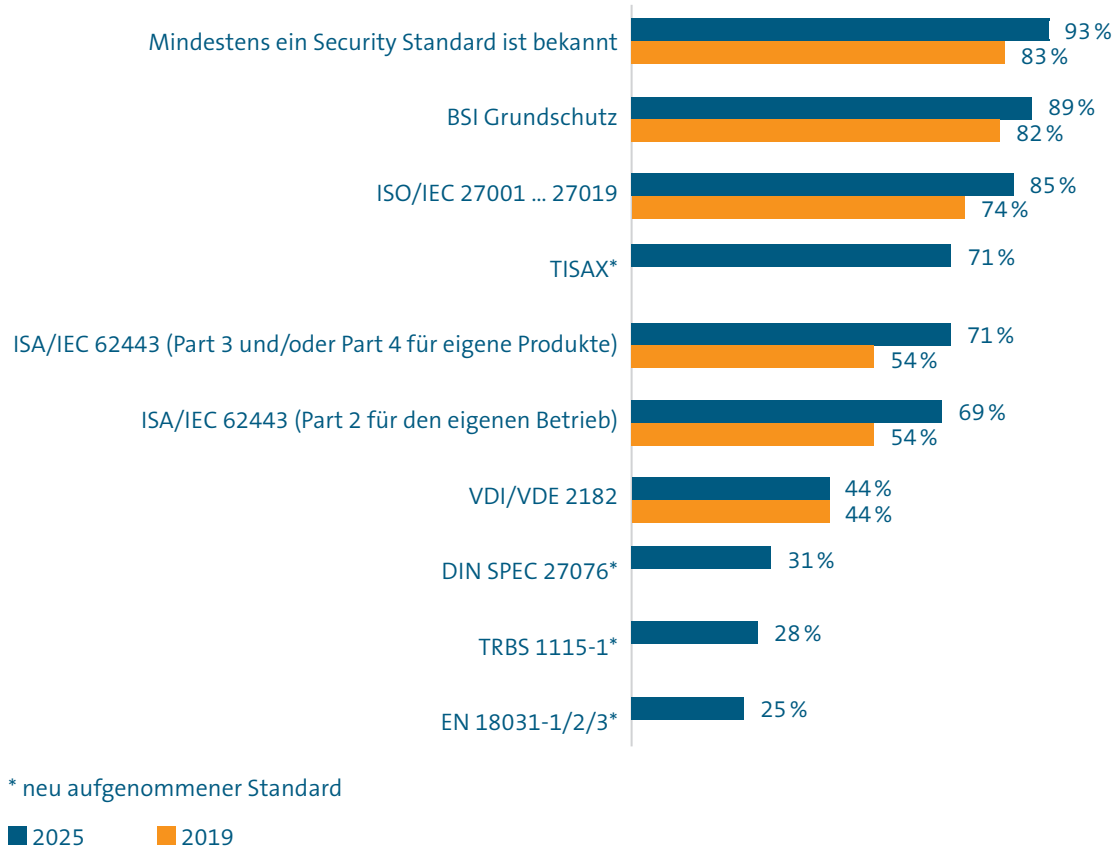
Der IT-Security-basierte Standard BSI IT-Grundschutz hat den Vorteil einer bereits integrierten allgemeinen Risikobetrachtung und verfügt über spezielle Bausteine für Maschinen und Anlagen. Die ISO 27000er-Reihe ist international weit verbreitet und wird häufig von Großkunden verpflichtend eingefordert. 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 Grundlage für die Absicherung der Produktion und von Produkten im Maschinen- und Anlagenbau dar. Unternehmen ist es daher angeraten, sich intensiv mit diesem Standard zu befassen. Den geeigneten Einstieg liefert der IEC 62443 Leitfaden des VDMAs – Im VDMA Verlag für Mitglieder (kostenfrei) und Nicht-Mitglieder (gegen Gebühr) verfügbar.

Abbildung 25

Welche IT-Security Standards sind Ihnen bekannt?

N = 71 bis 75

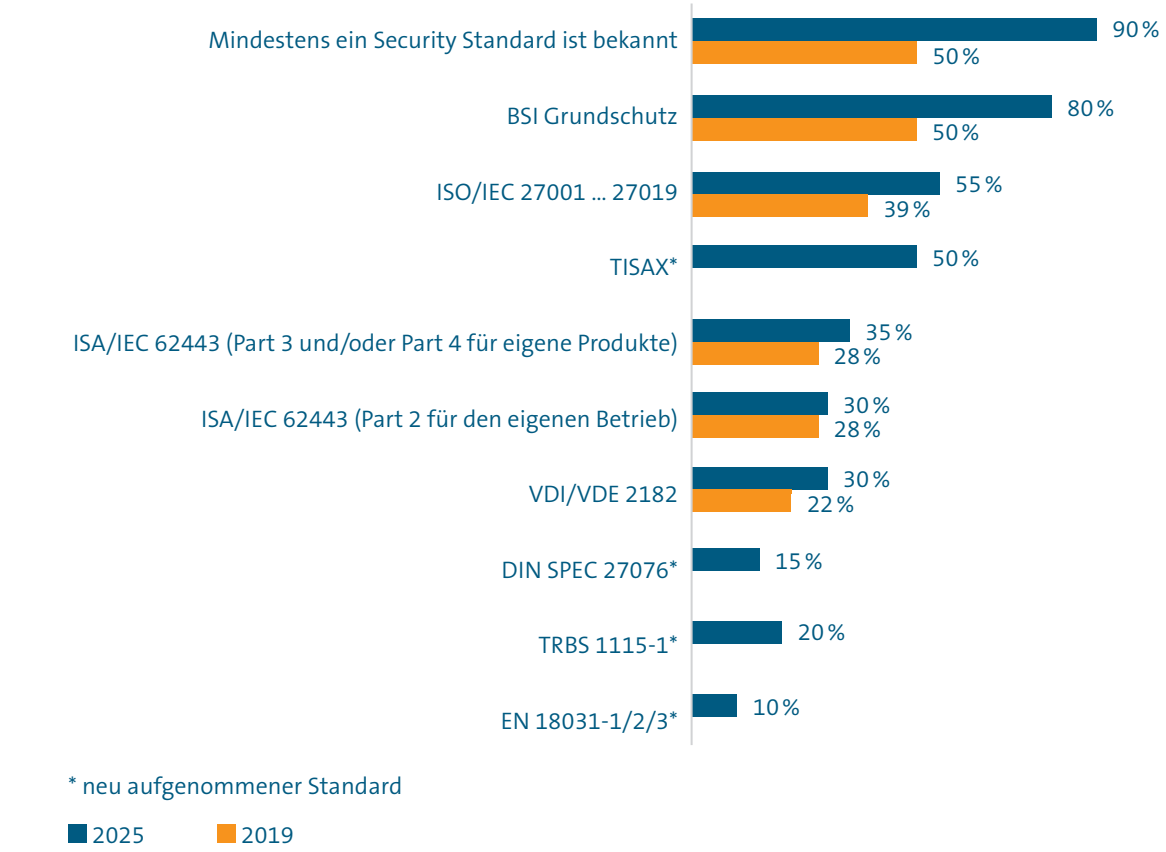


Quelle: VDMA

Abbildung 26

Welche IT-Security Standards sind Ihnen bekannt?

Bei Unternehmen bis 250 Mitarbeitende
N = 20 bis 21

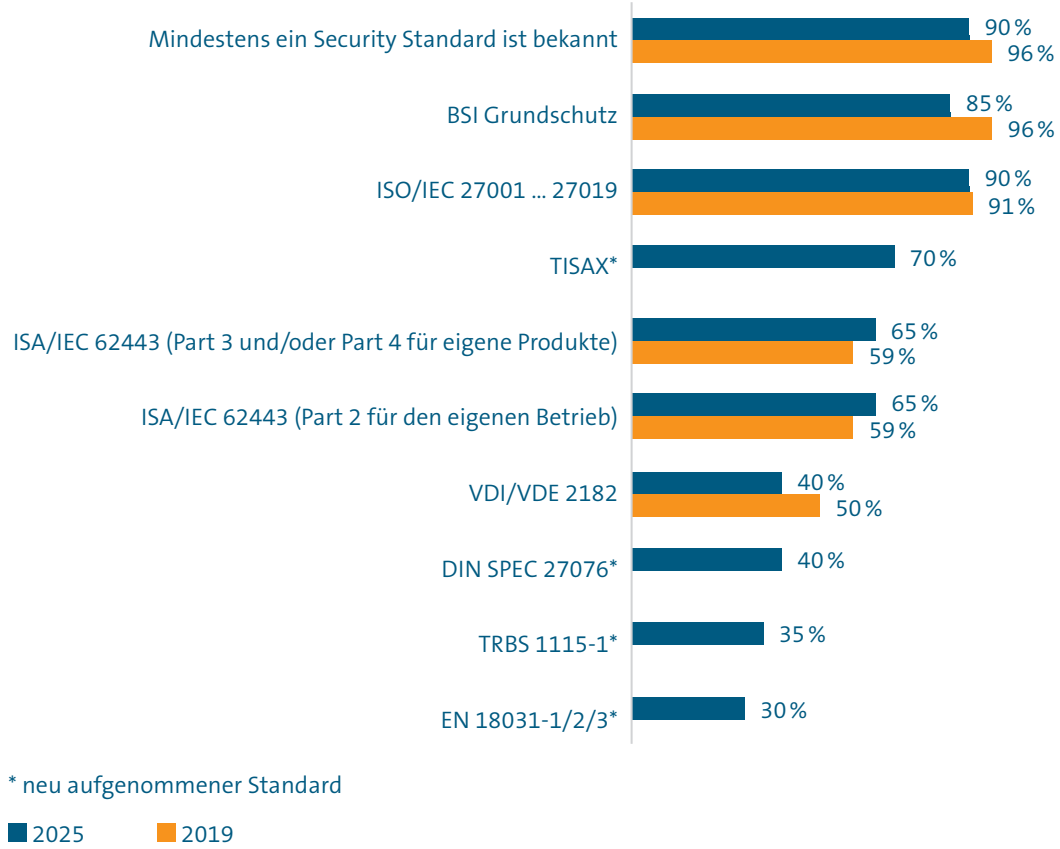


Quelle: VDMA

Abbildung 27

Welche IT-Security Standards sind Ihnen bekannt?

Bei Unternehmen mit 251 bis 1.000 Mitarbeitenden
N = 20

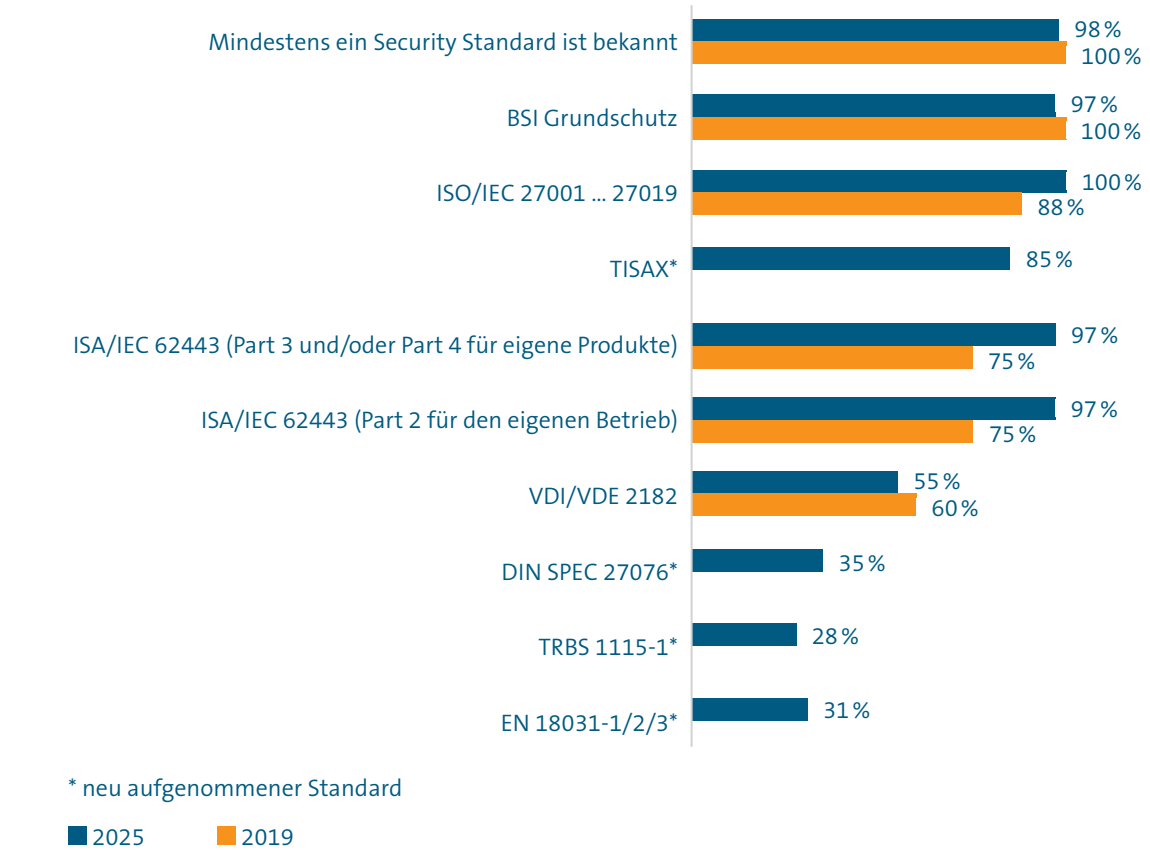


Quelle: VDMA

Abbildung 28

Welche IT-Security Standards sind Ihnen bekannt?

Bei Unternehmen mit über 1.000 Mitarbeitenden
N = 41 bis 31



Quelle: VDMA

12. Zukunft der Industrial Security

Cyber Resilience Act (CRA)

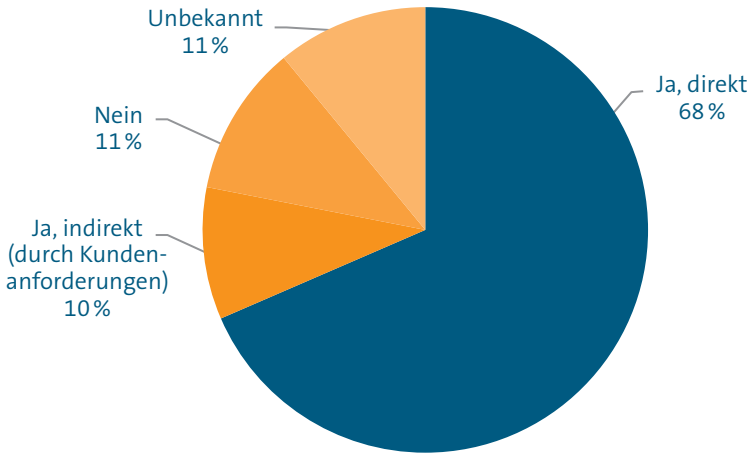
Aktuell sind bis zu zwei Drittel (68 Prozent) der befragten Unternehmen nach derzeitiger Definition direkt vom Cyber Resilience Act der EU betroffen. Weitere 10 Prozent der Studienteilnehmer sehen sich aufgrund Ihrer Funktion als Zulieferer, Integrator oder Servicedienstleister indirekt mit den Anforderungen von Kundenseite konfrontiert. Allerdings zeigt die Befragung auch, dass besonders bei kleinen Unternehmen (bis 250 Mitarbeitende) häufig noch Unkenntnis herrscht, ob sie direkt oder indirekt davon berührt sind. So kann rund ein Drittel (30 Prozent) der kleinen Unternehmen aktuell noch keine Aussage zur eigenen Betroffenheit machen.

Sind Unternehmen aber entweder direkt oder indirekt vom Cyber Resilience Act betroffen, so haben sie in den meisten Fällen bereits entsprechende Maßnahmen (79 Prozent organisatorische, 72 Prozent technische Maßnahmen) durchgeführt.

Abbildung 29

Ist Ihr Unternehmen vom Cyber Resilience Act betroffen?

N = 73



Quelle: VDMA

Netzwerk- und Informations-sicherheitsdirektive 2 (NIS2)

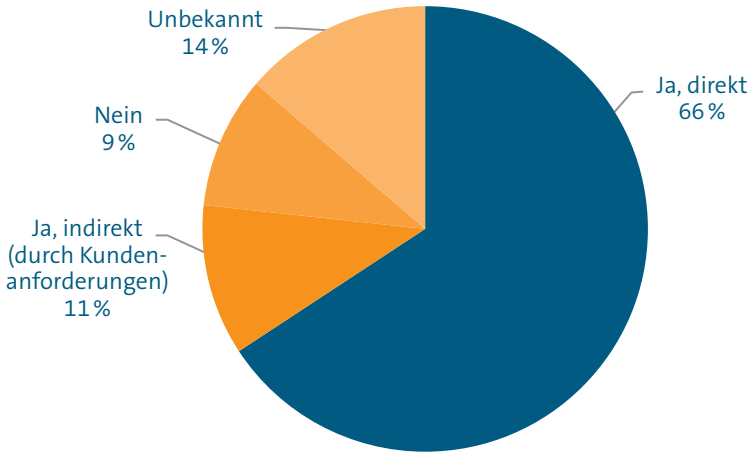
Weiterhin sind ebenfalls zwei Drittel (68 Prozent) der befragten Unternehmen nach derzeitigem Kenntnisstand direkt von der Netzwerk- und Informationssicherheitsdirektive 2 betroffen. Ebenso sehen sich weitere 11 Prozent der Unternehmen durch Kundenanforderungen indirekt mit den Anforderungen konfrontiert. Erneut sind sich wiederum 30 Prozent der kleinen Unternehmen (bis 250 Mitarbeitende) darüber unsicher, ob sie direkt oder indirekt davon betroffen sind.

Unternehmen, die von NIS-2 betroffen sind, haben ebenfalls oft schon entsprechende Maßnahmen (89 Prozent organisatorische, 80 Prozent technische Maßnahmen) umgesetzt.

Abbildung 30

Ist Ihr Unternehmen von der Netzwerk- und Informations-sicherheitsdirektive 2 (NIS2) betroffen?

N = 73



Quelle: VDMA

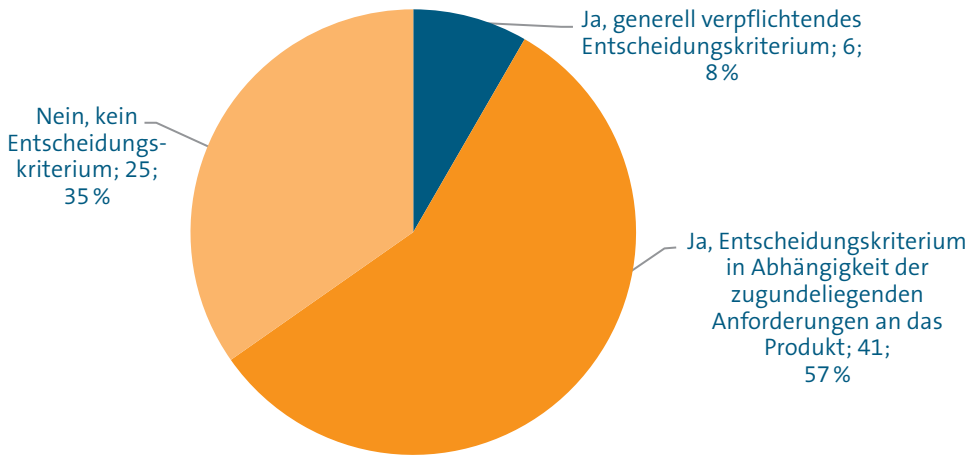
Security Gütesiegel

Ein Gütesiegel für die „geprüfte“ Security-Qualität von industriellen IT-Systemen sowie vernetzten Komponenten und Maschinen kann für die Einkäufer von Integratoren und Betreibern unter Umständen ein Entscheidungskriterium darstellen. Rund zwei Drittel der befragten Unternehmen (65 Prozent) können sich vorstellen, dies beim Produkteinkauf zu berücksichtigen – entweder als verpflichtendes Kriterium oder in Abhängigkeit der Anforderungen an das jeweilige Produkt. Für ein Drittel der Unternehmen (35 Prozent) stellt dies aber kein relevantes Entscheidungskriterium dar.

Abbildung 31

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

N = 72



Quelle: VDMA

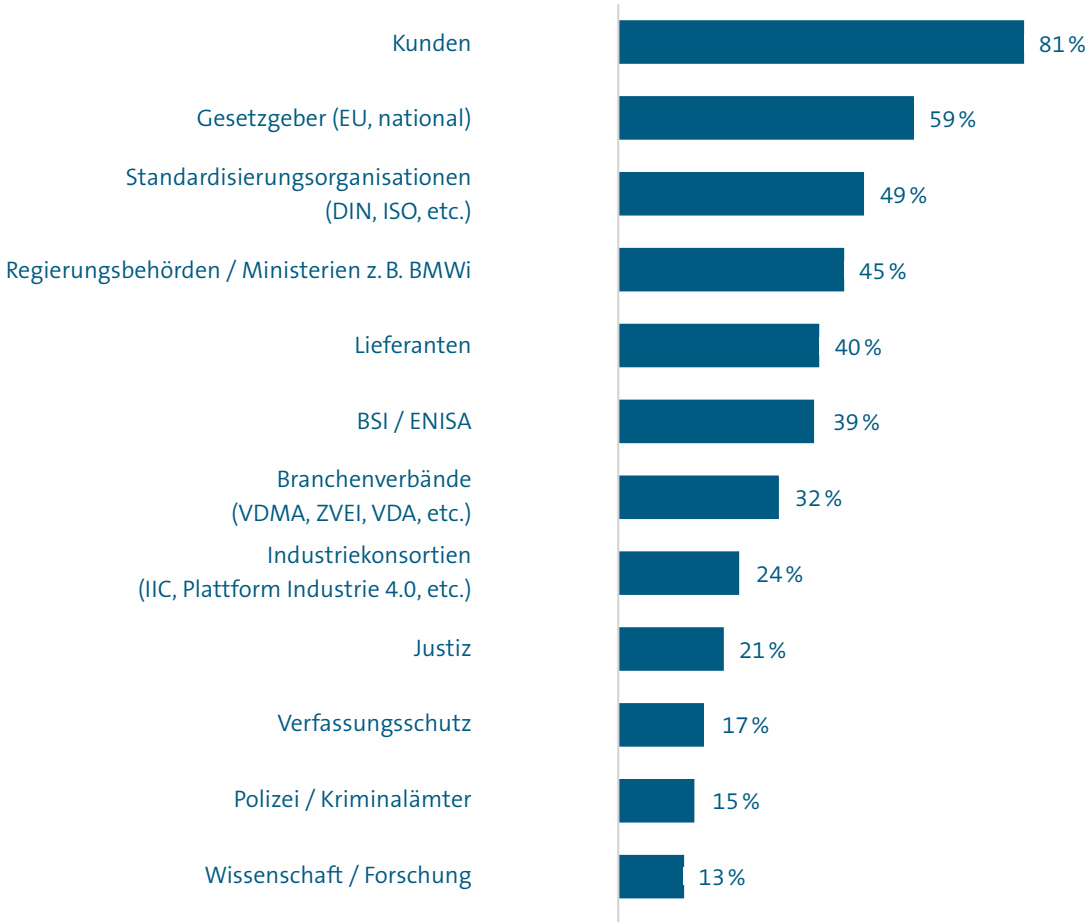
Anforderungen und Unterstützung zur Industrial Security

Die meisten befragten Unternehmen 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.

Abbildung 32

Von wem erwarten Sie zukünftig Anforderungen zur Industrial Security?

N = 70 bis 74

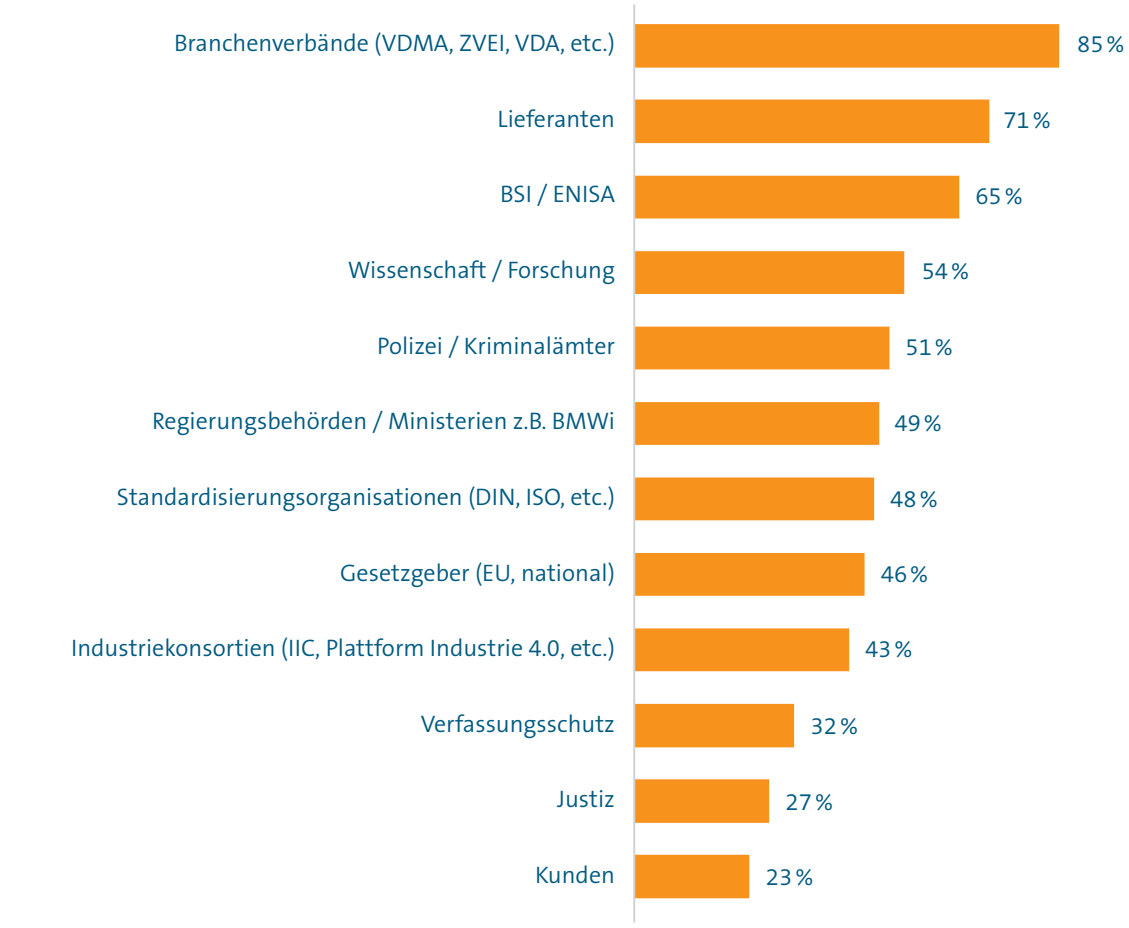


Quelle: VDMA

Abbildung 33

Von wem erwarten Sie zukünftig Unterstützung zur Industrial Security?

N = 70 bis 74



Quelle: VDMA

13. Unterstützung durch den VDMA

Dem Wunsch der Unternehmen, weiterhin vorrangig Unterstützung durch Branchenverbände zu erhalten, nimmt sich der VDMA nach wie vor an. Die Auswertung der gesamten Befragung bestätigt das Bild, was sich auch in der Gremienarbeit und dem Verbandsnetzwerk allgemein abzeichnet: Besonders kleine und mittelständische Unternehmen sind auf Unterstützung in Sachen Industrial Security angewiesen.

Gleichzeitig ist die Cyberresilienz der VDMA-Mitglieder auch bei einer stetig evolvierenden Bedrohungslandschaft gestiegen. Die Teilnahme am Veranstaltungsangebot, die Nutzung von Guidelines und Gremien versetzt unsere Mitglieder in die Lage, Best-Practices zu Industrial Security gemeinsam zu erarbeiten und von der gesamten Expertise der VDMA-Securitycommunity zu profitieren.

Spezifisch der VDMA Arbeitskreis „Industrial Security“ erarbeitet praxisnahe Arbeitshilfen für den gesamten Maschinen- und Anlagenbau. Dafür werden gleichermaßen die unterschiedlichen Perspektiven der Branche berücksichtigt: Komponentenhersteller, Maschinen- und Anlagenbauunternehmen, Integratoren und Betreiber, von großen Konzernen mit hunderten Katalogteilen bis zu kleinen Sondermaschinenbauunternehmen mit Losgröße 1 kommen hier zum Erfahrungsaustausch zusammen – nun mit immer mehr Schlagkraft – die Teilnehmerzahl dieses Gremiums hat sich in den vergangenen 12 Monaten auf derzeit rund 150 Teilnehmende verdoppelt (Stand 03/2025).

Die Mission des Arbeitskreises „die Produktsicherheit und Cyberresilienz der produktiven Industriebranchen zu steigern“ wird zumindest durch die Ergebnisse der Studie als bisher erfolgreich bestätigt – obwohl die Zahl der Cybervorfälle unter den befragten Unternehmen in den vergangenen Jahren gestiegen ist, werden die dadurch verursachten Auswirkungen immer geringer. Dennoch besteht weiterhin Handlungsbedarf: Die Umfrageergebnisse bestätigen, dass besonders kleine und mittelständische Unternehmen praktische Unterstützung zur Security benötigen, spezifisch wenn es in den kommenden Jahren zunehmend um die Bewältigung von Anforderungen aus Cybersecurity-Regulatorik, wie NIS2 oder CRA, geht. Mit den vom Gremium als zentral identifizierten Themen Risikomanagement, Supply Chain Security und Schwachstellenmanagement werden diese Anforderungen und weitere Herausforderungen so aufbereitet, dass auch Unternehmen mit Kernkompetenzen abseits von Security möglichst reibungslos ihre Cyberresilienz stärken und gleichzeitig Compliance mit der Securityregulatorik herstellen können.

Weiterhin wird von uns angegliedert an den Arbeitskreis „Industrial Security“ parallel der Expertenkreis „Security Solutions for Industry“ für VDMA Mitglieder veranstaltet. Auch hier stehen die Themen Industrial Security und Product Security im Fokus, jedoch wird in diesem Gremium die Expertise von Firmen mit Security im Kern ihres Portfolios gebündelt. Mit beiden Gremien wird so der Status Quo der modernen, vernetzten Industrie abgebildet: Produktion findet heutzutage in enger Interaktion zwischen Betreibern und deren Lösungsanbietern, Dienstleistern und Zulieferern statt – vom Austausch und einem gemeinsamen Verständnis von Industrial Security profitieren sämtliche Stakeholder. Nur so kann die Grundlage für eine cyberresiliente europäische Industrie geschaffen und die durch Cybercrime verursachten Schäden weiter reduziert werden.

Auch für Ihre Firma sollte damit das passende, praxis-orientierte Securitygremium im VDMA-Verbandsnetzwerk existieren. Wenn also auch Sie, bzw. Ihre Firma, sich in Sachen Industrial Security abholen lassen, oder gar wegweisend an Best-Practices und VDMA-Guidelines mitwirken möchten, kontaktieren Sie gerne maximilian.moser@vdma.org für Gremienbeteiligung oder Beratungstermine. Einzig die VDMA-Mitgliedschaft ist hierfür Voraussetzung. Weiterhin können Sie sich im folgenden Kapitel über unser aktuelles Angebot zu Industrial Security informieren.

14. Publikationen und Angebot des VDMA zu Industrial Security

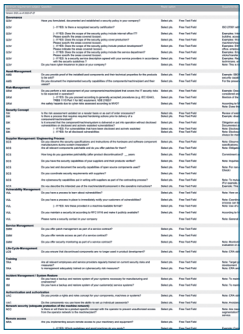
Publikationen

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. Teil der Supply Chain Security Dokumentenreihe.

https://www.vdma.org/viewer/-/v2article/render/92030451

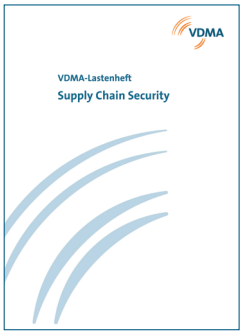


VDMA Lieferantenselbstauskunft (Excel)

Sprache: Deutsch, Englisch
Preis: kostenfrei

Allgemein gültiger Fragebogen an Lieferanten ohne konkreten Beschaffungsbezug. Referenz auf Maschinenverordnung und Cyber Resilience Act. Mit dem BSI gemeinsam erarbeitet. Teil der Supply Chain Security Dokumentenreihe.

https://www.vdma.org/viewer/-/v2article/render/92030451

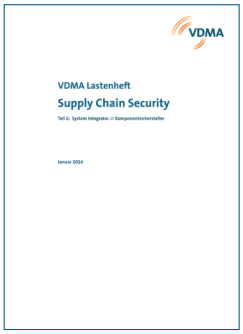


VDMA Lastenheft „Lastenheft Betreiber<>Integrator“

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. Teil der Supply Chain Security Dokumentenreihe.

https://www.vdma.org/viewer/-/v2article/render/92030451

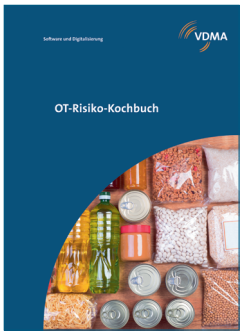


VDMA Lastenheft „Lastenheft Integrator<>Komponentenhersteller“

Sprache: Deutsch, Englisch
Preis: kostenfrei

Lastenheft mit Cybersecurity-Anforderungen auf Basis der IEC 62443. Zielgruppe sind Einkäufer der Integratoren, die allgemein anerkannte Anforderungen an die Security ihrer Komponentenlieferanten stellen möchten, vom Design bis hin zum cybersicheren Betrieb. Teil der Supply Chain Security Dokumentenreihe.

https://www.vdma.org/viewer/-/v2article/render/92030451



VDMA OT-Risiko Kochbuch

Sprache: Deutsch
Preis: kostenfrei

Praktische Anleitung zur Durchführung von OT-Risikobewertungen mit Fokus auf Prozesse und Methoden. Ermöglicht gezielten Transfer von IT-Security-Expertise ins OT-Umfeld. Richtet sich an Führungskräfte aus Produktion und Security/IT.

https://www.vdma.org/viewer/-/v2article/render/93887232

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.

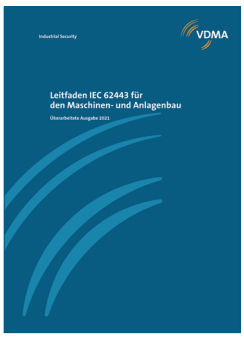
https://www.vdma.org/viewer/-/v2article/render/55742079

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

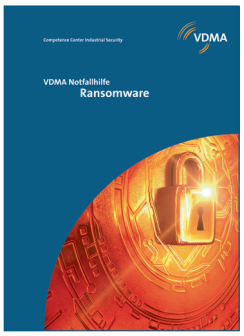


VDMA Leitfaden IEC 62443 für den Maschinen- und Anlagenbau

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.

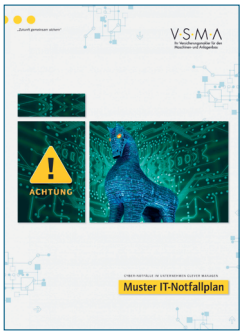
https://www.vdma.org/viewer/-/v2article/render/1295961

VDMA 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.

https://www.vdma.org/viewer/-/v2article/render/1141526

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/unternehmensfueh-rung/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/executive-briefings/informatik-und-tech-nik/711/leitfaden-zur-informationssicherheit-teil-2-isms-dokumente-und-vorlagen

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-informa-tionsaustausch-mit-externen-und

Gremien & Weiterbildung

VDMA Arbeitskreis „Industrial Security“
Aufgaben: Erarbeitet Leitlinien und Praxishilfen für die Industrial Security
Teilnehmer: Maschinen- und Anlagenbau, Betreiber, Automatisierer, Dienstleister, Security-Spezialisten, Bundesamt für Sicherheit in der IT (BSI)
VDMA-Kontakt: Maximilian Moser, Competence Center Industrial Security
Vorsitzender: Bernd Gehring, Voith GmbH, Heidenheim

VDMA Expertenkreis „Security Solutions for Industry“
Aufgaben: Erarbeitet Leitlinien und Praxishilfen für die Industrial Security
Teilnehmer: Lösungsanbieter, speziell Softwarehäuser und VDMA-Mitglieder mit Security im Kern ihres Portfolios.
VDMA-Kontakt: Maximilian Moser, Competence Center Industrial Security
Vorsitzender: Dr. Rodrigo Do Carmo, secunet secure Networks AG, Essen

VDW Arbeitskreis „Product Security“
Aufgaben: Praxisorientierter Arbeitskreis für Austausch zwischen Werkzeugmaschinen und Steuerungskomponentenhersteller. Erarbeitung von Strategien zur Steigerung der IT-Sicherheit von Werkzeugmaschinen und assoziierten Produkten.
Teilnehmer: Steuerungshersteller, Werkzeugmaschinenhersteller, VDW-Mitglieder
VDMA-Kontakt: Götz Görisch, VDW
Vorsitzende: Alexandra Gleich, Trumpf SE + Co. KG

MBI Schulungen zur IEC 62443:

Betreiber, Hersteller, Integratoren und Dienstleister müssen sich alle mit der Normenreihe IEC 62443 beschäftigen, um sowohl die OT-Security als 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.

Grundlage bildet der Kurs IC32, der im MBI in Kombination mit dem Kur IC46 für Systemintegratoren angeboten wird.
IC32 und IC46 – Grundlagen & Security für Systemintegratoren
https://www.maschinenbau-institut.de/seminar/cybersecurity-nach-iec-62443-grundlagen/

Für Fortgeschrittene gibt es den 5-tägigen Kompaktkurs direkt zum „Cybersecurity Expert“.
IC-33, IC-34 und IC-37 – Kompaktkurs für Fortgeschrittene
https://www.maschinenbau-institut.de/seminar/cybersecurity-nach-iec-62443-kompaktkurs-fuer-fortgeschrittene/

Security by Design für Maschinen und Anlagen

Cybersicherheit muss gemäß Cyber Resilience Act (CRA) bereits im Entwicklungsprozess verankert werden: „Security by Design“ ist eine grundlegend zu erfüllende Anforderung im Rahmen der Regulierung. Das Seminar wurde in Zusammenarbeit mit dem **Fraunhofer IEM** und **Fraunhofer IOSB** speziell für den Maschinenbau entwickelt und erläutert, wie die Prinzipien für „Security by Design“ konkret angewendet werden müssen. Basis bilden die IEC 62443, die Anforderungen aus dem Cyber Resilience Act und das VDMA Lastenheft zu Supply Chain Security.

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

Über uns

Die Abteilung Informatik vertritt die Interessen der IT- und Digitalisierungsbereiche des Maschinenbaus und deren technologischen Herausforderungen. Die Abteilung Informatik und der VDMA Software und Digitalisierung arbeiten sehr eng zusammen und werden als eine Einheit im VDMA geführt.

Ziel der beiden Gruppierungen ist es, die Zusammenarbeit von Softwareindustrie und Maschinenbau zu fördern und damit die digitale Transformation voranzutreiben.

vdma.org/software-digitalisierung
vdma.org/digitalisierung-industrie-40

Cybersecurity

Beim Thema Security im VDMA dreht sich alles um den Schutz von Maschinen und Anlagen in Produktion, Fertigung oder Intralogistik vor Angriffen und Störungen. Ziel der organisatorischen und technischen Schutzmaßnahmen ist es, cyberresiliente Maschinen- und Anlagen und vertrauenswürdige Dienste zu entwickeln und den dauerhaften Betrieb zuverlässig aufrecht zu erhalten.

Mit dieser Expertenseite bieten wir eine Übersicht über die verschiedenen Aspekte, Aufgaben und Anforderungen an Cybersecurity und Industrial Security. Dabei verweisen wir sowohl auf VDMA-Empfehlungen und Positionen als auch auf konkrete Hilfestellungen unserer Mitglieder und Partner.

https://www.vdma.org/cybersecurity

Weitere Publikationen

Unsere Publikationen beschäftigen sich mit verschiedenen Aspekten der Digitalisierung in Maschinenbauunternehmen sowie Cybersecurity und Informationssicherheit und dienen als Handlungsempfehlungen.

https://www.vdma.org/viewer/-/v2article/render/77810045

VDMA-Industrie Podcast

Der Audio-Blog für den Maschinen- und Anlagenbau beleuchtet auch digitale Trendthemen wie Plattformökonomie, Digitale Souveränität, Künstliche Intelligenz, Smart Factory, Security und Blockchain.

https://derindustriepodcast.podigee.io

Impressum

Herausgeber
VDMA
Lyoner Straße 18
60528 Frankfurt
Telefon +49 69 6603-1360
E-Mail biljana.gabric@vdma.org
Internet www.vdma.org/cybersecurity

Design
VDMA DesignStudio

Produktion
Druck- und Verlagshaus
Zarbock GmbH & Co. KG
Frankfurt am Main

Erscheinungsjahr
2025

Bildnachweis
VDMA

VDMA

Lyoner Straße 18
60528 Frankfurt am Main
Telefon +49 69 6603-1360
E-Mail biljana.gabric@vdma.org
Internet www.vdma.org/cybersecurity

www.vdma.org/cybersecurity

VDMA DesignStudio