Industrial Security

PILZ
THE SPIRIT OF SAFETY

Ein Leitfaden für Hersteller und Betreiber von Maschinen
zum Umgang mit der aktuellen EU-Gesetzgebung

Whitepaper
Version: April 2025

Haftungsausschluss

Wir haben unser Whitepaper sehr sorgfältig zusammengestellt. Es enthält Informationen über die aktuelle Pilz Interpretation der neuen EU-Maschinenverordnung, zur NIS-2-Richtlinie sowie zum Cyber Resilience Act. Alle Angaben haben wir nach dem heutigen Wissens- und Interpretationsstand und bestem Wissen und Gewissen gemacht. Dennoch können wir für die Richtigkeit und Vollständigkeit der Angaben, sofern uns nicht der Vorwurf grober Fahrlässigkeit trifft, keine Haftung übernehmen, da sich trotz aller Sorgfalt Fehler nicht vollständig vermeiden lassen. Insbesondere haben die Angaben nicht die rechtliche Qualität von Zusicherungen oder zugesicherten Eigenschaften. Für Hinweise auf Unstimmigkeiten sind wir dankbar.

Urheberrecht

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern

2. überarbeitete Auflage

Auf einen Blick

Der Begriff Industrial Security hat viele Facetten, in diesem Leitfaden sind die wichtigsten Eckpunkte für Maschinenhersteller und -betreiber beschrieben. Sowohl den Herstellern als auch den Betreibern soll der Einstieg in das Thema erleichtert werden, um die neuen Anforderungen verstehen und bewältigen zu können.

Der Leitfaden beschreibt die gesetzliche Lage in Europa, gibt einen Überblick über die technischen Grundlagen, beschreibt die wichtigsten Punkte für Maschinenhersteller sowie für Maschinenbetreiber und verweist auf weiterführende Angebote für unsere Kundinnen und Kunden.

In Europa sind in den letzten Monaten zahlreiche umfangreiche Gesetzestexte erschienen, die unmittelbar Einfluss auf den Maschinenbau haben:

- Die **Maschinenverordnung** (EU) 2023/1230 stellt neue Anforderungen an Maschinen, wie unter anderem den Schutz gegen Korrumpierung.
- die **EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau** in der Union (NIS 2) 2022/2555 fordert für sehr viele Unternehmen ein Information Security Management System.
- Der **Cyber Resilience Act** (EU) 2024/2847, definiert Anforderungen an Produkte mit digitalen Elementen, darunter fallen in der Regel auch Maschinen.

Bei der Umsetzung der Gesetzgebung sind einige Normen und Begriffe von großer Bedeutung:

- Zum Thema Informationssicherheit im industriellen Umfeld hat sich die Normenfamilie **IEC 62443** etabliert.
- Der **Security Level** von 0 bis 4 beschreibt die Fähigkeiten des Angreifers.
- Industrial Security ist eine fortlaufende Aufgabe, weshalb neben den technischen Maßnahmen auch organisatorische Maßnahmen unabdingbar sind. Ein **Information Security Management System** (ISMS) hilft hierbei und wird für viele Unternehmen obligatorisch.

Maschinenhersteller sind von verschiedenen gesetzlichen Anforderungen betroffen und bewegen sich zwischen den Vorgaben von Betreibern und dem Angebot von Komponentenherstellern. Hier wird der Maschinenhersteller eine Vermittlungsrolle einnehmen müssen, um weiterhin konforme und qualitativ hochwertige Produkte anbieten zu können.

Auch die Betreiber von Maschinen müssen sich in Zukunft über die Sicherung ihrer Maschinen Gedanken machen. Um sich einen Überblick zu verschaffen, bietet es sich an, eine systematische Risikoanalyse durchzuführen und die Schwachstellen effizient zu schließen.

Die Pilz GmbH & Co. KG bietet zu diesem Thema weiterführende Schulungen und Dienstleistungen an.

Der Autor

Matthias Kuczera hat sich nach seinem Maschinenbaustudium in verschiedenen Industriebereichen ein umfassendes Wissen über Maschinensicherheit angeeignet.

Als Entwicklungsingenieur für Sensoren erlangte er tiefgreifendes Wissen über die Umsetzungsmöglichkeiten funktionaler Sicherheitsanforderungen.

Während der Tätigkeit als Sachverständiger im Bereich der Fördertechnik war er für die Durchführung von Baumusterprüfungen von Sicherheitsbauteilen bei einer benannten Stelle zuständig.

In seiner jetzigen Tätigkeit als Fachexperte für „Funktionale Sicherheit - Normen“ bei Pilz ist er in Normengremien aktiv und betreut das Normenmanagement.

Zu seinen Aufgaben zählen:

- die Mitarbeit in Normengremien für Maschinensicherheit
- die Bewertung neuer gesetzlicher Anforderungen
- die Durchführung interner Schulungen

Pilz – the Spirit of Safety in Digital Automation

Mit allem, was wir tun, machen wir die Welt sicherer. Als globaler Anbieter von Produkten, Systemen und Dienstleistungen für die Automatisierungstechnik blickt Pilz auf eine über 75-jährige Erfolgsgeschichte zurück: Gegründet 1948, beschäftigt die Pilz Gruppe heute rund 2 500 Mitarbeiter in 42 Tochtergesellschaften und Niederlassungen. Der Experte für Maschinensicherheit mit Stammsitz in Ostfildern schafft weltweit mit seinen kompletten Automatisierungslösungen Sicherheit für Mensch, Maschine und Umwelt. Das Portfolio des Technologieführers umfasst die Sensorik, Steuerungs- und Antriebstechnik genauso wie Systeme für die industrielle Kommunikation, Diagnose und Visualisierung. Ein internationales Dienstleistungsangebot mit Beratung, Engineering und Schulungen rundet das Spektrum ab. Die Lösungen für Safety und Security kommen über den Maschinen- und Anlagenbau hinaus in zahlreichen Branchen wie etwa der Intralogistik, der Bahntechnik oder im Bereich Robotik zum Einsatz.

Inhalt

1. Die gesetzliche Lage in Europa

Neue Technologien bringen Chancen und Risiken mit sich. Die wohl wichtigsten Neuerungen unserer Branche zurzeit sind die hochgradige Vernetzung von Maschinen über das Internet der Dinge, Künstliche Intelligenz und Robotik.

Mit der Vernetzung von Unternehmen und Maschinen steigt das Risiko, dass Schwachstellen in den Informationssystemen ausgenutzt werden und wirtschaftliche und körperliche Schäden entstehen. Beispielsweise haben sich in den letzten Jahren die Fälle von erfolgreichen Cyberangriffen auf Unternehmen gehäuft, wodurch Schäden in Milliardenhöhe entstanden. Statista.com schätzt, dass im Jahr 2023 weltweit rund 8,15 Billionen Dollar Schaden durch Cyberangriffe verursacht wurden. Allein in Deutschland waren es 2023 knapp 206 Milliarden Euro, das entspricht etwa 5 Prozent des Bruttoinlandprodukts.

Um die Gefährdungen zu reduzieren, hat der europäische Gesetzgeber neue Regelwerke geschaffen. Für den Maschinenbau sind das im Wesentlichen die Maschinenverordnung, die NIS-2-Richtlinie (NIS 2) und der Cyber Resilience Act (CRA). Sie machen Industrial Security zur Pflicht. Der Umgang mit bestehenden Maschinen und Anlagen wird in der Richtlinie 2009/104/EG für Sicherheit und Gesundheitsschutz bei Benutzung von Arbeitsmitteln beschrieben.

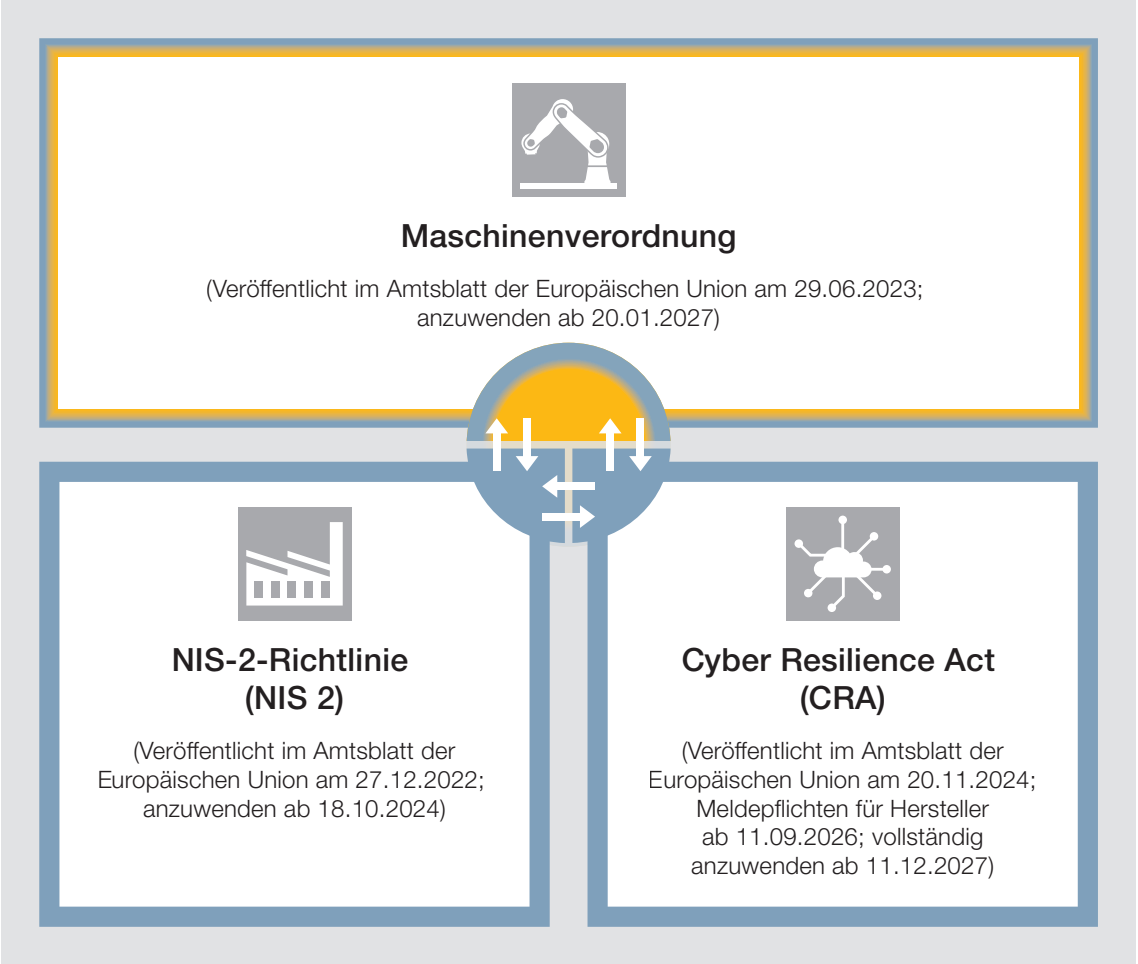

Abbildung 1: Darstellung eines Auszuges neuer grundlegender Rechtsvorlagen, die Anforderungen an Industrial Security beschreiben

	Maschinenverordnung (EU) 2023/1230	NIS-2-Richtlinie (EU) 2022/2555	Cyber Resilience Act (EU) 2024/2847
Richtet sich an	Maschinen	Unternehmen	Komponenten
Verabschiedet am	29.06.2023	27.12.2022	20.11.2024
Verbindlich ab	20.01.2027	18.10.2024	11.12.2027
Pflichten	▸ Schutz vor Korrumpierung (mit Fokus auf Funktionen der funktionalen Sicherheit ▸ Beachtung böswilliger Versuche Dritter	▸ Maßnahmen zum Management von Cybersicherheitsrisiken ▸ Einhaltung von technischen und organisatorischen Maßnahmen ▸ Meldung erheblicher Sicherheitsvorfälle	▸ Meldepflichten der Hersteller ab 11.09.2026 ▸ Secure Development Lifecycle Process ▸ EU-Baumusterprüfung für kritische Produkte ▸ Meldungen von Schwachstellen ▸ Bereitstellung von Sicherheitsaktualisierungen

Tabelle 1: Überblick Maschinenverordnung, NIS-2-Richtlinie und Cyber Resilience Act im Vergleich

1.1. Maschinenverordnung (EU) 2023/1230

Abbildung 2: Die Maschinenverordnung im Überblick

Die Maschinenverordnung (EU) 2023/1230 wurde im Juni 2023 verabschiedet, ist nach einer Übergangsfrist von 42 Monaten für alle EU-Staaten verbindlich und löst die Maschinenrichtlinie 2006/42/EG zum Stichtag am 20. Januar 2027 ab.

Die Maschinenverordnung betrifft Hersteller, Importeure, Händler und Bevollmächtigte von Maschinen oder dazugehöriger Produkte. Sie müssen zukünftig bestätigen, dass die Maschinen der Maschinenverordnung entsprechen, das beinhaltet auch Security-Anforderungen. Dazu gehört unter anderem der Schutz sicherheitsrelevanter Steuerungsfunktionen gegen Korrumpierung. Hersteller von Maschinen müssen Vorkehrungen gegen Risiken treffen, die sich aus böswilligen Handlungen Dritter ergeben können und die Maschinensicherheit betreffen. Das Einhalten der Maschinenverordnung wird formal in der Konformitätserklärung bestätigt und mit dem CE-Zeichen an der Maschine gekennzeichnet. Maschinen, die die Anforderungen der neuen Maschinenverordnung nicht erfüllen, dürfen in der EU nicht mehr in Verkehr gebracht werden.

Praxistipp:
Im Vergleich zur Maschinenrichtlinie ist das Thema Security nicht die einzige Neuerung in der Maschinenverordnung. Weitere Anforderungen, wie etwa der Umgang mit Künstlicher Intelligenz, sind hinzugekommen. Pilz bietet einen Leitfaden zur Maschinenverordnung zum Download an:
www.pilz.com/mr

1.2. Die NIS-2-Richtlinie (EU) 2022/2555

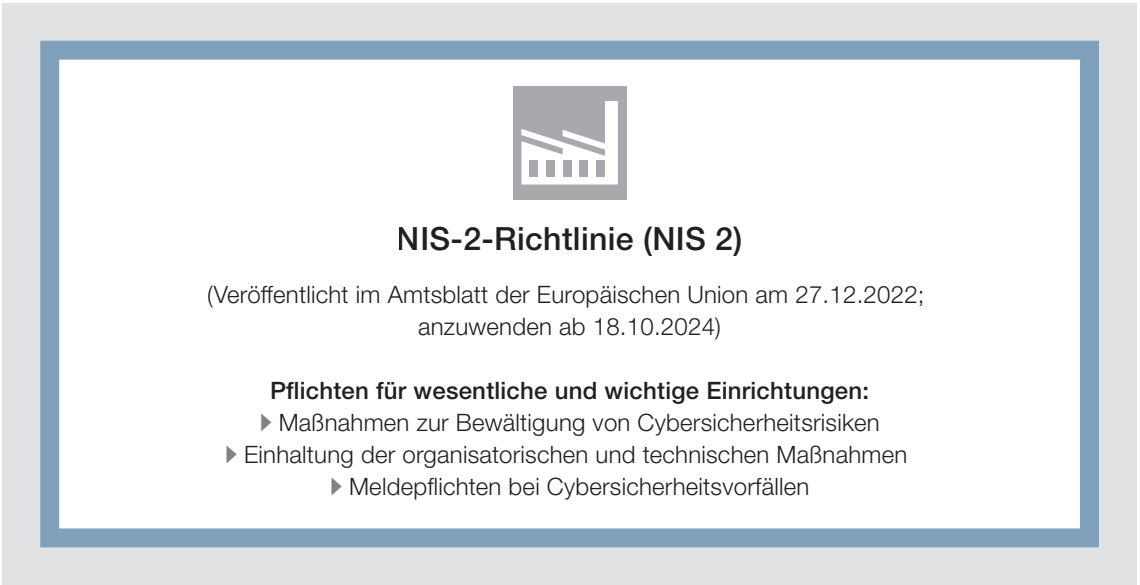

Abbildung 3: Die NIS-2-Richtlinie im Überblick

Die NIS-2-Richtinlie findet man im Amtsblatt der EU unter dem Namen „Richtlinie (EU) 2022/2555 … über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union … (NIS-2-Richtlinie)“. Die Abkürzung „NIS“ ist historisch bedingt und steht im Sprachgebrauch für „Netz- und Informationssicherheit“. Die NIS-1-Richtlinie galt vorwiegend für kritische Infrastrukturen und Anbieter relevanter digitaler Dienste. Die NIS-2-Richtlinie erweitert die Sektoren unter anderem um das produzierende Gewerbe: Maschinenbau, Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, elektrischen Ausrüstungen, Kraftwagen und Kraftwagenteilen sowie sonstiger Fahrzeugbau. **Innerhalb dieser Branchen sind Unternehmen mit mehr als 50 Beschäftigten oder einem Jahresumsatz bzw. einer Jahresbilanz von über 10 Millionen Euro betroffen.**

Diese Unternehmen sind künftig verpflichtet, Risikomanagementmaßnahmen für die Cybersicherheit zu ergreifen. Dazu gehören:

- **Risikoanalysen und Sicherheitskonzepte** für Informationssysteme, den Schutz der Lieferkette und die Sicherheit des Personals
- Konzepte für die **Zugriffskontrolle** und das Management von Anlagen
- **verpflichtende Schulungen** für das Management
- bei erheblichen Security-Sicherheitsvorfällen eine **Frühwarnung** binnen 24 Stunden und binnen 72 Stunden eine **Meldung an die zuständige Behörde**

Die NIS 2 wurde Ende 2022 durch das Europäische Parlament und den Rat der EU verabschiedet. Bis zum 18. Oktober 2024 müssen die EU-Mitgliedsstaaten die Richtlinie in nationales Recht überführen.

Praxistipp:
Die Agentur der Europäischen Union für Cybersicherheit (ENISA) bietet viele nützliche Informationen zum Thema Cybersicherheit, unter anderem ein Tool zur Selbstbewertung, mit dem Unternehmen ihre Cybersicherheitsstrategie überprüfen können: **www.enisa.europa.eu**

Praxistipp:
Software-Tools wie z. B. OpenVAS können Unternehmen helfen, Schwachstellen zu finden und Gegenmaßnahmen zu überprüfen.

1.3. Cyber Resilience Act (EU) 2024/2847

Abbildung 4: Der Cyber Resilience Act im Überblick

Die Europäische Kommission wertet Cyberangriffe als eine Angelegenheit von öffentlichem Interesse, da diese nicht nur auf die Wirtschaft der Union, sondern auch auf die Demokratie, die Sicherheit der Verbraucher und die Gesundheit kritische Auswirkungen haben können.

Darum hat die Europäische Kommission im September 2022 einen Entwurf für eine Verordnung vorgelegt, die die Cybersicherheit von Produkten erhöhen soll.

Dieser Cyber Resilience Act (CRA) richtet sich an **Hersteller von Produkten mit digitalen Elementen (Hard- und Software),** die in der Lage sind, mit anderen Produkten zu kommunizieren.

Betroffen sind also Produkte sowohl aus dem B2C-Bereich, wie etwa Smartphones oder Staubsaugerroboter, als auch aus dem B2B-Bereich, wie **Steuerungen und Sensoren,** aber auch reine Softwareprodukte wie Betriebssysteme.

Gemäß CRA dürfen künftig nur noch Produkte auf dem Markt bereitgestellt werden, die ein angemessenes Cybersicherheitsniveau gewährleisten – und zwar über den gesamten Lebenszyklus eines Produkts. Die Verordnung wurde am 20.11.2024 im Amtsblatt der Europäischen Union veröffentlicht. Die Meldepflichten von ausgenutzten Schwachstellen für Hersteller gelten ab dem 11.09.2026. Produkte mit digitalen Elementen müssen ab dem 11.12.2027 die Anforderungen aus dem CRA erfüllen, um in der EU auf dem Markt bereitgestellt werden zu dürfen. Der CRA ist eine EU-Verordnung und wird somit in den EU-Mitgliedsstaaten unmittelbar gültig sein.

Der CRA ist parallel zur Maschinenverordnung anzuwenden. Das heißt, auch eine Maschine wird als Produkt mit digitalen Elementen gesehen. Dies wiederum führt dazu, dass es neben den Anforderungen aus der Maschinenverordnung zusätzliche aus dem CRA geben wird.

Das ist notwendig, da die Maschinenverordnung auf den Schutz der Personen im unmittelbaren Umfeld der Maschine zielt, während der CRA zusätzlich die natürlichen oder juristischen Personen vor wirtschaftlichen Schäden schützt.

In der praktischen Umsetzung wird es unter Umständen Synergieeffekte geben, dass beispielsweise eine Cybersicherheits-Maßnahme Anforderungen aus dem CRA und aus der Maschinenverordnung erfüllt. Diese Synergieeffekte, müssen beispielsweise durch die Anwendung harmonisierter Normen durch den Hersteller nachgewiesen werden.

Praxistipp:
Abonnieren Sie Newsletter und RSS-Feeds auf **https://eur-lex.europa.eu**, um stets über Gesetzesänderungen auf EU-Ebene informiert zu werden.

1.4. Richtlinie für Sicherheit und Gesundheitsschutz bei Benutzung von Arbeitsmitteln 2009/104/EG

Auch für die Betreiber von Maschinen und Anlagen stellt sich die Frage, welchen Verpflichtungen sie nachkommen müssen. Die Richtlinie über Mindestvorschriften für Sicherheit und Gesundheitsschutz bei Benutzung von Arbeitsmitteln durch Angestellte bei der Arbeit macht hierzu Vorgaben. Die Richtlinie ist am 3. Oktober 2009 im Amtsblatt der Europäischen Union veröffentlicht worden und wurde anschließend von allen Mitgliedsstaaten in nationales Recht umgesetzt. Sie definiert „Arbeitsmittel“ als Maschinen, Apparate, Werkzeuge oder Anlagen, die bei der Arbeit benutzt werden.

Nach dieser Richtlinie ist es unter anderem die allgemeine Pflicht des Arbeitgebers, den Arbeitnehmern geeignete Arbeitsmittel zur Verfügung zu stellen, sodass bei deren Benutzung die Sicherheit und der Gesundheitsschutz der Arbeitnehmer gewährleistet ist.

Die Arbeitsmittel müssen während der gesamten Zeitdauer der Benutzung z. B. durch entsprechende Wartung auf einem Stand gehalten werden, der gewährleistet, dass sie den Bestimmungen aller geltenden einschlägigen EU-Gemeinschaftsrichtlinien entsprechen.

Auch wenn es sich bei der Maschinenverordnung formal um eine Verordnung – und nicht um eine Richtlinie – handelt, ist davon auszugehen, dass sie aus juristischer Sicht als einschlägige Gemeinschaftsrichtlinie anerkannt werden wird. Somit gelten die neuen Anforderungen aus der Maschinenverordnung auch für Bestandsmaschinen ab dem Zeitpunkt, an dem die Maschinenverordnung gültig ist.

Abbildung 5: Gesetzliche Anforderungen zur Maschinensicherheit müssen berücksichtigt und eingehalten werden

2. Security für Maschinenhersteller

Die Security-Anforderungen an Maschinen steigen aus zwei Gründen: Zum einen stellen anspruchsvolle Kunden bereits heute Fragen zu den Security-Eigenschaften der Maschinen, zum anderen setzt der Gesetzgeber ab 2027 grundlegende Eigenschaften voraus, damit Maschinen in Europa in Verkehr gebracht bzw. bereitgestellt werden dürfen.

Nicht zu vergessen ist, dass die meisten Maschinenhersteller vom Gesetzgeber als wichtige Einrichtung gesehen werden und somit unter die NIS-2-Richtlinie fallen. Das bedeutet, dass sie gut beraten sind, über die Einführung eines **Information Security Management System (ISMS)** nachzudenken.

Kurz gefasst:
Maschinen, die die Security-Anforderungen der Maschinenverordnung nicht erfüllen, dürfen ab dem 20.01.2027 in der EU nicht mehr in Verkehr gebracht werden. Ob und welche Maßnahmen getroffen werden müssen, lässt sich durch eine strukturierte Risikoanalyse ermitteln.

Darüber hinaus wird der Cyber Resilience Act (CRA) weitergehende Informations- und Dokumentationspflichten fordern. Die Meldepflichten für Hersteller gelten ab dem 11.09.2026; vollständig anzuwenden ist der CRA ab dem 11.12.2027.

2.1. Security in der Maschinenverordnung

Die Maschinenverordnung fordert unter den grundlegenden Sicherheits- und Gesundheitsanforderungen in Abschnitt 1.1.9 den Schutz gegen Korrumpierung. Dieser wird wie folgt beschrieben:

> „[…] Die Maschine bzw. das dazugehörige Produkt muss so konstruiert und gebaut sein, **dass der Anschluss von einer anderen Einrichtung an die Maschine** oder das dazugehörige Produkt **durch jede Funktion der angeschlossenen Einrichtung** selbst oder über eine mit der Maschine bzw. dem dazugehörigen Produkt kommunizierende entfernte Fernzugriffseinrichtung **nicht zu einer gefährlichen Situation führt.**
>
> **Ein Hardware-Bauteil, das Signale oder Daten überträgt,** die für den Anschluss oder den Zugriff auf die Software relevant sind, die für die Übereinstimmung einer Maschine oder eines dazugehörigen Produkts mit den einschlägigen Sicherheits- und Gesundheitsschutzanforderungen von entscheidender Bedeutung ist, **muss so konstruiert sein, dass es angemessen gegen unbeabsichtigte oder vorsätzliche Korrumpierung geschützt ist. Maschinen** bzw. dazugehörige Produkte **müssen Beweise für ein rechtmäßiges oder unrechtmäßiges Eingreifen in das genannte Hardware-Bauteil sammeln,** soweit es für den Anschluss oder den Zugriff auf die Software relevant ist, die für die Konformität der Maschinen bzw. dazugehörigen Produkte **von entscheidender Bedeutung ist.**
>
> **Software und Daten,** die für die Übereinstimmung der Maschine oder des dazugehörigen Produkts mit den einschlägigen Sicherheits- und Gesundheitsschutzanforderungen von entscheidender Bedeutung sind, **sind als solche zu benennen und angemessen gegen unbeabsichtigte oder vorsätzliche Korrumpierung zu schützen.**

> Die Maschine bzw. das dazugehörige Produkt muss die installierte Software, die für den sicheren Betrieb erforderlich ist, kenntlich machen und diese Informationen jederzeit in leicht zugänglicher Form bereitstellen können.
>
> Maschinen bzw. dazugehörige Produkte müssen Nachweise für ein rechtmäßiges oder unrechtmäßiges Eingreifen in die Software oder eine Veränderung der in Maschinen bzw. dazugehörigen Produkte installierten Software oder ihrer Konfiguration sammeln. […]“

Daneben gibt es in Abschnitt 1.2.1 Sicherheit und Zuverlässigkeit von Steuerungen die Anforderung:

> „[…] Steuerungen müssen so ausgelegt und beschaffen sein, dass
>
> a) sie, wenn den Umständen und Risiken angemessen, den zu erwartenden Betriebsbeanspruchungen sowie beabsichtigten und unbeabsichtigten Fremdeinflüssen, **einschließlich vernünftigerweise vorhersehbare böswillige Versuche Dritter, die zu einer Gefährdungssituation führen, standhalten können;** […]“

Eine genauere Spezifizierung des Schutzziels „Schutz gegen Korrumpierung“ und dessen technische Realisierung soll eine neue europäische Norm, EN 50742, geben. Diese wird momentan erarbeitet. Da noch nicht abzusehen ist, ob diese Norm rechtzeitig zum Ende der Übergangsfrist der Maschinenverordnung veröffentlicht und harmonisiert wird, empfiehlt es sich, sich bereits heute über den Stand der Technik zu informieren. Hierbei hilft z. B. IEC TS 63074. Diese Spezifikation beschreibt die Sicherheitsaspekte im Zusammenhang mit der funktionalen Sicherheit von sicherheitsbezogenen Steuerungssystemen. Daneben erläutert IEC 62443-3-3 die Security-Anforderungen an industrielle Automatisierungssysteme. Im Anhang dieses Leitfadens werden einige grundlegende Informationen zu der Normenfamilie dargestellt.

Einige Anforderungen aus der Maschinenverordnung können durch die Wahl von passenden Komponenten erfüllt werden, andere erfordern eine zusätzliche Dokumentation. Um einen pragmatischen Weg zu finden, empfiehlt es sich, eine systematische Risikoanalyse bereits während der konzeptionellen Phase der Maschinenentwicklung vorzusehen. Diese kann auch zu einem späteren Zeitpunkt durchgeführt werden, doch steigt erfahrungsgemäß der Aufwand, je fortgeschrittener die Entwicklung ist.

Abbildung 6: Die EU-Maschinenverordnung macht Industrial Security zur Pflicht im Konformitätsbewertungsprozess

2.2. Zwischen Komponentenherstellern und Kunden

Ein sicherer und rechtskonformer Betrieb der Maschine ist der Anspruch von Maschinenbetreibern. Bei der Umsetzung bewegen sich Maschinenhersteller bzw. Integratoren zwischen den Anforderungen der Kunden und dem Angebot der Komponentenhersteller.

Hilfestellung geben die Typ-C-Normen. Sie beschreiben den Stand der Technik für bestimmte Anwendungsbereiche und legen das Mindestmaß an Sicherheit fest, über die eine Maschine verfügen muss. Da es Stand heute noch keine harmonisierten C-Normen gibt, die den Security-Aspekt berücksichtigen, bleibt nichts anderes übrig, als nach bestem Wissen und Gewissen eine Risikoanalyse unter Anwendung etablierter internationaler Normen durchzuführen und daraus Maßnahmen zur Risikominderung abzuleiten.

Um die Risikoanalyse korrekt durchführen zu können, ist es wichtig, die Umgebungsbedingungen und Security-Anforderungen an die Maschine zu kennen. Hierbei spielen zwei Dinge eine Rolle: zum einen das mögliche Ausmaß des Schadens, das heißt, wie hoch ist die Motivation des Angreifers, Schaden anzurichten, und zum anderen die Wahrscheinlichkeit eines Angriffs. Man kann davon ausgehen, dass eine frei zugängliche Maschine eher angegriffen wird als eine Maschine, zu der nur eine eingeschränkte Personengruppe Zugang hat.

Jeder kennt Sicherheitsupdates von Alltagsprodukten wie Smartphones und Computer. Auch Maschinensteuerungen oder andere Maschinenkomponenten benötigen nach einer bekanntgewordenen Sicherheitslücke ein Update. Stand heute führen die meisten Komponenten keine automatischen Updates durch und die Komponentenhersteller stehen in der Regel nicht direkt mit den Betreibern in Verbindung. Das führt zu der Frage, wie der Betreiber sicherstellen kann, dass seine Maschine rechtzeitig die notwendigen Updates erhält.

Hier spielt der Integrator, also der Maschinenhersteller bzw. der Systemintegrator, eine Schlüsselrolle und kann durch seine Position zwischen Betreiber und Komponentenhersteller vermitteln. Zum einen kann er mit den Security-Anforderungen des Betreibers auf die Komponentenhersteller zugehen und die richtigen Komponenten auswählen. Zum anderen kann er die Informationen zu den Komponenten, z. B. zu neuen Sicherheitsupdates, mit dem Betreiber teilen.

Praxistipp:
Um ein einheitliches Vorgehen zu fördern, hat der Verband Deutscher Maschinen- und Anlagenbau e. V. (VMDA) in der Arbeitsgruppe Industrial Security die Dokumentenreihe „Supply Chain Security“ erstellt, die die Kommunikation zwischen Betreiber, Integratoren und Komponentenhersteller erleichtern soll: **www.vdma.org**

Die folgende Abbildung veranschaulicht die Schnittstellen zwischen Betreibern, Integratoren und Komponentenherstellern.

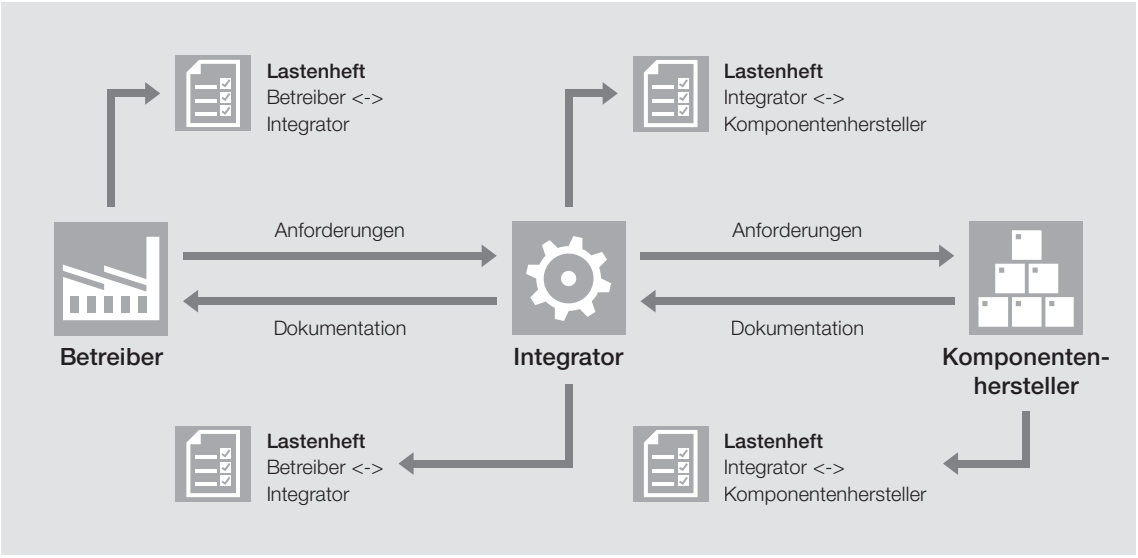

Abbildung 7: Empfehlung zur Lieferkette von VDMA (Quelle: https://www.vdma.org/cybersecurity)

2.3. Cyber Resilience Act für Maschinenhersteller

Der Cyber Resilience Act (CRA) ist eine Verordnung, die am 20.11.2024 im Amtsblatt der Europäischen Union veröffentlicht wurde. Sie bezieht sich auf Produkte mit digitalen Elementen. Alle Produkte mit digitalen Elementen müssen ab dem 11.12.2027 die Anforderungen des CRA erfüllen. Hersteller von Produkten mit digitalen Elementen, müssen bereits ab dem 11.09.2026 den Meldepflichten nachkommen. Es ist davon auszugehen, dass, sobald eine Maschine unter den CRA fällt, der Hersteller auch die Konformität mit dem CRA bescheinigen muss. Das bedeutet, dass verschiedene Anforderungen erfüllt sein müssen.

Erwähnenswert an dieser Stelle sind unter anderem folgende Anforderungen:

- **Meldepflicht** für Hersteller von ausgenutzten Schwachstellen an die Behörde innerhalb 24 Stunden
- Produkte mit digitalen Elementen werden so entworfen, entwickelt und hergestellt, dass sie ein **angemessenes Maß an Cybersicherheit gewährleisten,** das dem ermittelten Risiko entspricht
- auf Basis der Risikoanalyse dürfen die Produkte **nur ohne bekannte ausnutzbare Schwachstellen** auf dem Markt verfügbar gemacht werden
- Sicherstellung, dass Schwachstellen durch **Sicherheitsaktualisierungen** behoben werden können
- **Schutz der Verfügbarkeit wesentlicher und grundlegender Funktionen,** auch nach einem Zwischenfall, u. a. durch Ausfallsicherheit und Abhilfemaßnahmen gegen Denial-of-Service-Angriffe
- Identifizierung und Dokumentation von **Schwachstellen und Komponenten durch Hersteller von Produkten mit digitalen Elementen,** u. a. durch die Erstellung einer Software-Stückliste in einem maschinenlesbaren Format, die zumindest die wichtigsten Abhängigkeiten der Produkte abdeckt
- zusätzliche **Dokumentation über den Umgang mit Sicherheitslücken,** wie z. B. dem Zeitraum, in dem der Hersteller Sicherheitsupdates für sein Produkt zur Verfügung stellt
- Erstellung einer EU-Konformitätserklärung

Diese (unvollständige) Liste der Anforderungen aus dem CRA macht deutlich, dass für alle beteiligten Wirtschaftsakteure ein erheblicher Aufwand entstehen wird. Wie sich diese Vorgaben auf die Produktvielfalt auswirken und ob die veranschlagte Übergangsfrist von drei Jahren ausreichend ist, wird sich zeigen.

Pilz empfiehlt allen Maschinenherstellern, sich zeitnah mit diesem Thema zu befassen und zusammen mit den Komponentenherstellern und den Betreibern Konzepte zu entwickeln, um den Anforderungen des CRA gerecht zu werden.

Praxistipp:
Das Common Security Advisory Framework (CSAF) ist ein standardisiertes und quelloffenes Framework zur Kommunikation und automatisierbaren Verteilung von maschinenverarbeitbaren Schwachstellen- und Mitigationsinformationen, so genannten Security Advisories:
https://oasis-open.github.io/csaf-documentation

Praxistipp:
Durch die Einführung einer Software Bill of Materials (SBOM) ist es möglich, den Überblick über alle verwendeten Softwareversionen zu behalten.

3. Security für Maschinenbetreiber

Betreiber von Maschinen sind ebenfalls von den neuen Rechtsakten betroffen: sei es bei der Beschaffung von neuen Maschinen, Änderungen an bestehenden Maschinen oder der wiederkehrenden Überprüfung, ob der Stand der Technik weiterhin eingehalten wird.

Da typischerweise Maschinen im produzierenden Gewerbe eingesetzt werden, müssen auch Maschinenbetreiber die NIS-2-Richtlinie erfüllen.

Kurz gefasst:
Betreiber von Bestandsanlagen sind von der neuen Maschinenverordnung ebenfalls betroffen. Durch Netzwerksegmentierung und die Beschränkung von Zugriffsmöglichkeiten lässt sich der geforderte Schutz in der Regel auch nachträglich erreichen. Mit einer zuvor durchgeführten strukturierten Risikoanalyse werden Handlungsbedarfe ermittelt.

Die NIS-2-Richtlinie verlangt von einem großen Kreis von produzierenden Unternehmen umfassende Security-Konzepte. Vernetzte Maschinen müssen in diese Betrachtungen einbezogen werden.

3.1. Umgang mit Bestandsanlagen

Betreiber von Maschinen, die typischerweise als Arbeitsmittel eingesetzt werden, müssen sicherstellen, dass die Arbeitnehmer einen ausreichenden Arbeitsschutz genießen und niemand zu Schaden kommt. Dies wird beschrieben in der oben vorgestellten **EU-Richtlinie für Sicherheit und Gesundheitsschutz bei Benutzung von Arbeitsmitteln** aus dem Jahr 2009, die von allen Mitgliedsstaaten in nationales Recht umgesetzt wurde.

In dieser Richtlinie wird gefordert, dass der Betreiber durch wiederkehrende Prüfungen sicherstellt, dass seine Arbeitsmittel während der gesamten Zeit der Benutzung durch entsprechende Wartung auf einem Niveau gehalten werden, welches den Bestimmungen aller geltenden einschlägigen Gemeinschaftsrichtlinien entspricht.

Im Umkehrschluss bedeutet das: Ab dem Tag, ab dem die Maschinenverordnung gilt, also dem 20. Januar 2027, müssen alle aktiven Maschinen dahingehend überprüft sein, ob sie dem Niveau der Maschinenverordnung entsprechen. Es wird Fälle geben, in denen der Arbeitgeber den Anforderungen nicht vollumfänglich nachkommen kann. Auch in diesen Fällen ist er dennoch verpflichtet, geeignete Maßnahmen zu treffen, um die Gefahren weitgehend zu verringern.

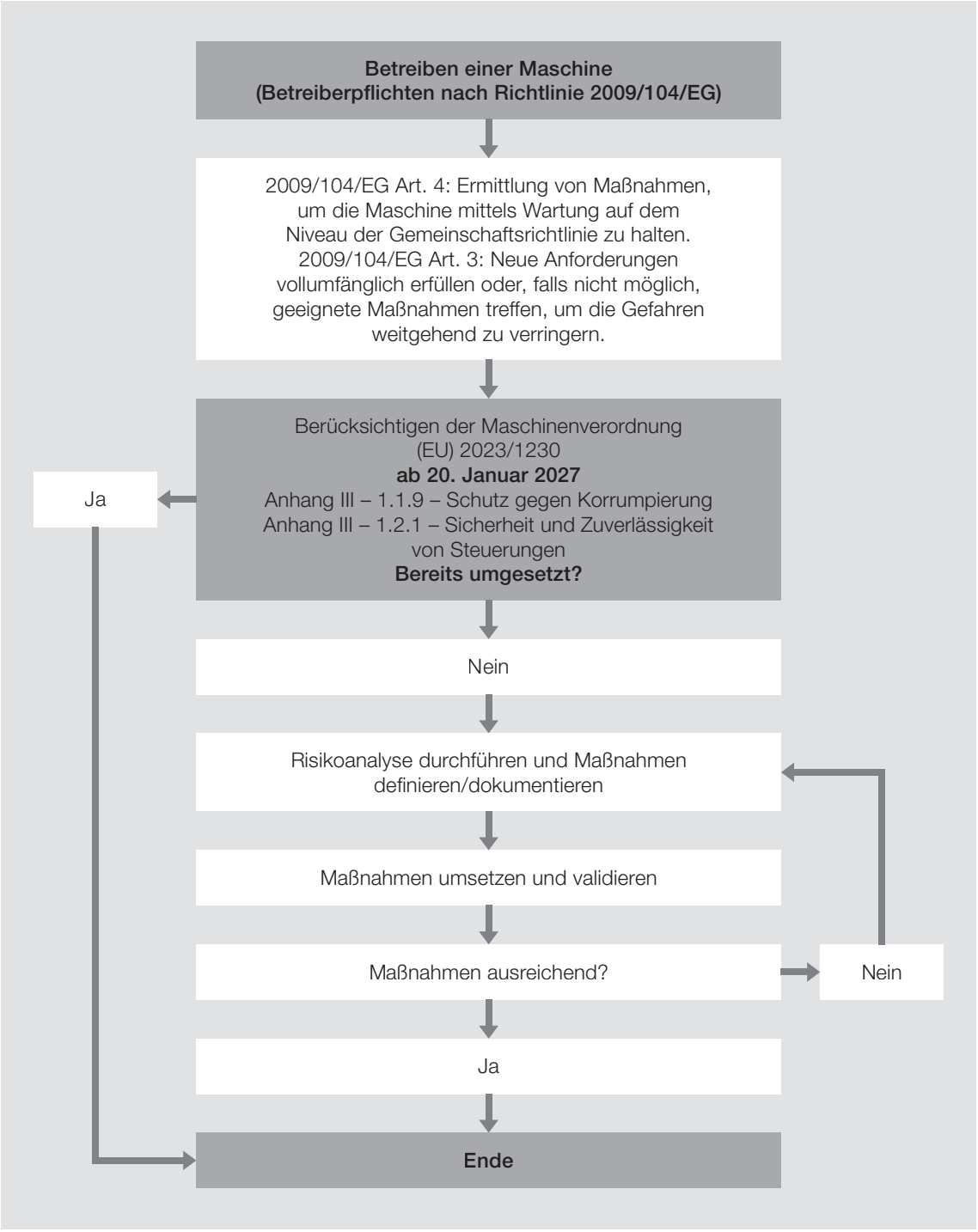

Abbildung 8: Prozessablauf – Umgang mit Bestandsanlagen

Betreiber, die sich noch nicht mit dem Thema auseinandergesetzt haben, müssen Maßnahmen ergreifen, um den neuen Anforderungen in Bezug auf die Cybersicherheit nachzukommen.

Der erste Schritt ist eine Security-Risikoanalyse. Aus dieser Risikoanalyse ergeben sich die umzusetzenden Maßnahmen. In den meisten Fällen beinhaltet das eine Segmentierung des Netzwerks und die Einschränkung von Zugriffsmöglichkeiten.

3.2. Von IT-Security zur unternehmensweiten Security

In aller Regel ist die IT-Abteilung (Informationstechnologie) für die Informations- und Kommunikationstechnologie in Unternehmen zuständig, inklusive IT-Security.

In Unternehmen ist das Thema Security z. B. in Form einer Stabstelle angesiedelt. Diese Security-Experten oder -Beauftragte, z. B. in der Rolle des Chief Information Security Officer (CISO), sollten mit den Anforderungen der NIS-2-Richtlinie vertraut sein und ein Konzept haben, wie diese im gesamten Unternehmen umgesetzt werden können.

Erfahrungsgemäß verlässt sich der Produktionsbereich des Unternehmens bei Fragen rund um die IT-Security auf die IT-Abteilung und beschäftigt sich mit dem Thema eher am Rande.

Hier ist zwingend ein Umdenken erforderlich, da die im Produktionsbereich stehenden Maschinen Teil des Security-Konzeptes des Unternehmens sind. Um das Gesamtkonzept korrekt umzusetzen, muss das Unternehmen in Sicherheitszonen unterteilt und die Schnittstellen und Anforderungen der einzelnen Zonen bis auf die Maschinenebene im Unternehmen definiert und umgesetzt werden.

Abbildung 9: Industrial Security betrifft auch den Zusammenhang zwischen IT-Sicherheit und OT-Sicherheit

Praxistipp:
Über die Suchmaschine **https://www.shodan.io/** können vernetzte Geräte gefunden werden, häufig auch solche, die eigentlich durch eine Netzwerksegmentierung nicht mehr gefunden werden dürften. Sind Ihre Geräte auch dabei?

Praxistipp:
Eine der häufigsten Angriffsarten ist der Weg über Mitarbeiterinnen und Mitarbeiter eines Unternehmens, z. B. über Phishing-Mails. Regelmäßige Schulungen für die Belegschaft vermindern dieses Risiko.

4. Der Weg zur sicheren Maschine – Safe und Secure

Kurz gefasst:
Mit einer strukturierten Risikoanalyse lassen sich die Kosten für Gegenmaßnahmen und auch für die Analyse selbst drastisch reduzieren. Dabei wird die Betrachtung der Vielzahl möglicher Angriffswege reduziert auf diejenigen, die definierte Schutzziele tatsächlich gefährden. Die Bewertung der möglichen Schadenshöhe und der Eintrittswahrscheinlichkeit gibt zusätzlich Hinweise auf den sinnvollen Aufwand zur Risikominimierung.

Gefährdungen der Security von Maschinen können auf vielerlei Wegen entstehen, sowohl über Datennetzwerke als auch physisch durch direkten Zugang zur Maschine. Um eine Maschine möglichst kosteneffizient zu schützen, empfiehlt sich eine strukturierte Vorgehensweise, die im Folgenden beschrieben ist.

- **Assets identifizieren**
  Im ersten Schritt werden die zu schützenden Assets definiert und gegeneinander abgegrenzt. Das Ergebnis liefert ein vollständiges und widerspruchsfreies Bild der zu schützenden Anlagen und Anlagenteile. Diese Maßnahme stellt sicher, dass keine Teile vergessen werden, aber auch, dass Angriffsvektoren nicht unnötigerweise mehrfach betrachtet werden.
- **Bedrohungen analysieren**
  Im nächsten Schritt gilt es, die Höhe des möglichen Schadens bei einer Kompromittierung zu ermitteln. Diese Frage lässt sich leichter beantworten, wenn man die drei Schutzziele der Informationssicherheit separat betrachtet. Diese sind: Vertraulichkeit, Integrität und Verfügbarkeit – die englischen Begriffe lauten Confidentiality, Integrity und Availability, häufig abgekürzt als CIA.
  - **Confidentiality (Vertraulichkeit)**
    Enthält die Maschine Informationen, deren Offenlegung dem Unternehmen schaden? Dies könnten z. B. Hinweise zu Fertigungsverfahren, Rezepturen oder anderen Geschäftsgeheimnissen sein, die Unternehmen einen Wettbewerbsvorteil sichern. Wie hoch ist der potenzielle Schaden?
  - **Integrity (Integrität)**
    Welche Auswirkungen kann die unerwünschte Veränderung von Daten haben? Kann die Veränderung von Daten zu wirtschaftlichen Schäden führen, z. B. durch Beschädigung der Maschine, oder Menschen in Gefahr bringen, z. B. durch die Beeinflussung von Sicherheitsfunktionen? Wie hoch ist der potenzielle Schaden?
  - **Availability (Verfügbarkeit)**
    Welche wirtschaftlichen Schäden entstehen durch den Ausfall einer Maschine, z. B. durch Produktionsunterbrechungen?
- **Schutzziele ermitteln**
  Nach diesen Vorarbeiten können die Schutzziele formuliert werden. Je konkreter die Ziele definiert sind, desto spezifischer lassen sich Angriffsvektoren ermitteln. Dies vermeidet unnötige Maßnahmen, die vielleicht die Security der Maschinen steigern, aber nicht der Erreichung der definierten Schutzziele dienen.
- **Risiken bewerten**
  Nachdem die Schutzziele ermittelt wurden, wird die Wahrscheinlichkeit abgeschätzt, mit der die ermittelten Risiken tatsächlich auftreten können. Das Ergebnis gibt einen Hinweis auf den sinnvollen Umfang der weiteren Maßnahmen.

- **Angriffsvektoren analysieren**
  In diesem Schritt wird systematisch ermittelt, auf welchen Wegen ein Angriff tatsächlich stattfinden kann und welche Schutzmaßnahmen bereits existieren, z. B. durch intrinsische Schutzmaßnahmen in verwendeten Maschinenkomponenten. Daraus ergibt sich eine Liste der verbleibenden Gefährdungsursachen.
- **Security-Konzept erstellen und umsetzen**
  Das Security-Konzept beschreibt konkret alle Maßnahmen, die notwendig sind, um die definierten Schutzziele für die betrachtete Maschine zu erreichen. Diese können sowohl konstruktive Maßnahmen an der Maschine als auch organisatorische Anpassungen der Abläufe umfassen.
- **Umsetzung überprüfen**
  Die tatsächliche Wirksamkeit der durchgeführten Maßnahmen lässt sich nur durch sehr aufwendige Penetrationstests prüfen, bei denen Hackerangriffe von spezialisierten Dienstleistern simuliert werden. Ersatzweise sollte die korrekte Umsetzung des Security-Konzeptes geprüft werden.
- **Regelmäßige Neubewertungen durchführen**
  Im Gegensatz zur Safety sind Schutzmaßnahmen für die Security keine einmalige Sache. Da in komplexen Systemen ständig neue Schwachstellen auftreten, sollte die Analyse in regelmäßigen Zeitabständen oder bei Bekanntwerden von Bedrohungen wiederholt werden. Neue Schwachstellen können auf allen Ebenen der Beschaffungspyramide auftreten, z. B. bei Hardwarekomponenten, Open-Source-Code in Geräten oder spezifischer Geräte-Firmware. Sobald eine Schwachstelle erkannt wird, veröffentlichen die verantwortlichen Hersteller entsprechende Security Advisories mit Informationen über die Gefährdung und Hinweisen zu geeigneten Gegenmaßnahmen. Es empfiehlt sich, sich regelmäßig über neue Security Advisories von Lieferanten zu informieren.

Abbildung 10: Nur durch eine Security-Betrachtung sind Maschinen, Komponenten und Anlagen wirklich sicher und vor Korrumpierung geschützt

Praxistipp:
Die Pilz Security Advisories erhalten Sie auf **www.pilz.com/advisories**

5. Safety und Security aus einer Hand

Mit den neuen gesetzlichen Vorgaben beim Thema Security kommen neue Herausforderungen auf Maschinenhersteller und -betreiber zu. Die Prozesse zur Risikoverminderung von Angriffen auf Maschinen (Security) ähneln dabei sehr stark den Abläufen zur Reduzierung von Risiken, die von Maschinen ausgehen können (Safety). Pilz als Experte für Maschinensicherheit verhilft Schritt für Schritt zu passgenauen Lösungen und sicheren Maschinen – Safe und Secure.

Abbildung 11: Safety und Security gehören in der Maschinensicherheit als ganzheitliches Konzept zusammen

- Fachwissen und Know-how durch Mitarbeit in Normengremien
- Recherche und Verfolgung der aktuellen Gesetzes- und Normenlage
- Basis- und Expertenschulungen für maschinenorientierte Industrial Security
- Dienstleistungen im Rahmen maschinenorientierter Industrial Security
  - Schutzbedarfsanalysen
  - Risikoanalysen
  - ganzheitliche Sicherheitskonzepte
  - Validierungen/Verifizierungen
  - Prozessoptimierungen
- Produkte und Lösungen für physische Zugangskontrolle und Cybersecurity an der Maschine

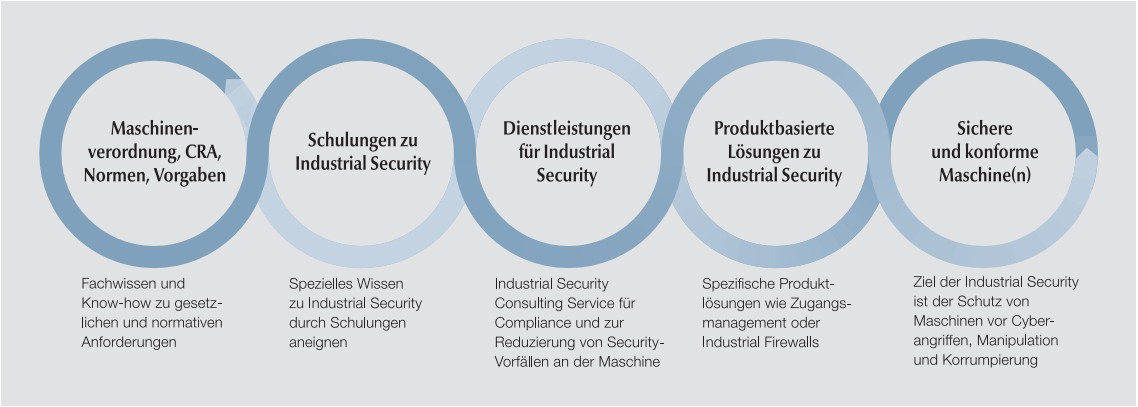

Abbildung 12: Schritt für Schritt zur sicheren Maschine mit Industrial-Security-Lösungen

Praxistipp:
Mehr zu Industrial-Security-Lösungen bei Pilz finden Sie unter **www.pilz.com/security**

6. Zusammenfassung und Ausblick

Die Zunahme an Bedrohungen durch Cyberangriffe und Korrumpierung hat eine unmittelbare Auswirkung auf die gesetzliche Lage in Europa und mündet in einen klaren Kurs seitens des Gesetzgebers in Richtung Industrial Security: Künftig werden speziell durch die Maschinenverordnung, die NIS-2-Richtlinie und den CRA neue Anforderungen zu Industrial Security durch den Gesetzgeber gestellt. Für Maschinenhersteller und -betreiber bedeutet dies ein aktives Handeln durch die Ausarbeitung und Umsetzung von organisatorischen und technischen Maßnahmen zur Erfüllung der neuen Anforderungen an Unternehmen, Maschinen und Komponenten. Der vorliegende Leitfaden hat diese Aufgaben und den Umgang damit erläutert.

Die NIS-2-Richtlinie ist bereits für einen Großteil der Maschinenhersteller und -betreiber verbindlich, im Jahr 2027 werden die neue Maschinenverordnung und der CRA folgen. Durch vorausschauendes Handeln lassen sich die notwendigen Projekte rechtzeitig planen und umsetzen.

Normengremien geben Maschinenherstellern Orientierung an die Hand, wie die neuen Anforderungen umzusetzen sind. Wichtig ist eine strukturierte Vorgehensweise, wie sie in der Normenreihe IEC 62443 beschrieben ist.

Erfahrene und qualifizierte Dienstleister helfen, Schritt für Schritt notwendige Maßnahmen zu analysieren, um die neuen Zielvorgaben mit in der Regel überschaubarem Aufwand zu erfüllen.

Maschinensicherheit bedeutet künftig Safety und Security – zum Schutz der Menschen und zum Schutz der Maschinen. Mit einem ganzheitlichen und abgestimmten Konzept können komplexe Problemstellungen in der Maschinensicherheit effizient und sauber segmentiert werden. Eine Risikoanalyse stellt auch für Industrial Security den initialen Schritt dar und bietet eine strukturierte Orientierung und Methodik, um Anforderungen auf das eigene Unternehmen herunterzubrechen.

Mit dieser Vorgehensweise sind Unternehmen gut gerüstet, um den wachsenden Herausforderungen im Bereich Industrial Security zu begegnen.


Weitere Informationen
von Pilz zu Industrial Security –
jetzt entdecken
PILZ
Erfahren Sie mehr unter:
www.pilz.com/security

7. Anhang

7.1. Begriffe aus dem Bereich Industrial Security

Cybersicherheit, im Sinne der EU Kommission, bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

Cyberbedrohung bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

Industrial Security verfolgt das Ziel, die Verfügbarkeit von Maschinen und Anlagen sowie die Integrität und Vertraulichkeit von maschinellen Daten und Prozessen zu gewährleisten.

IT-Security (Information Technology) ist die Sicherung von Daten abseits von physischen Prozessen.

OT-Security (Operational Technology) ist die Sicherung von Maschinen und Anlagen, die an physischen Prozessen beteiligt sind.

IACS ist eine Abkürzung aus IEC 62443 und steht für Industrial Automation and Control System(s) – zu deutsch industrielles Automatisierungssystem.

Security Level aus der Normenreihe IEC 62443 ist der Level, der den erforderlichen Maßnahmen und den inhärenten Sicherheitseigenschaften von Geräten und Systemen für eine Zone oder ein Conduit entspricht, basierend auf der Bewertung des Risikos für die Zone oder das Conduit.

Zone ist die Zusammenfassung von Einheiten, die eine Aufteilung eines betrachteten Systems auf der Grundlage ihrer funktionalen, logischen oder physikalischen Beziehungen (einschließlich des Ortes) wiedergeben.

Conduit ist die logische Gruppierung von Kommunikationskanälen, die zwei oder mehr Zonen verbindet, für die gemeinsame IT-Sicherheitsanforderungen gelten.

7.2. IEC 62443 – Grundnorm für Industrial Security

IEC 62443 ist eine internationale Normenreihe für „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“.

7.2.1. Überblick

Die Normenfamilie IEC 62443 besteht aus verschiedenen Teilen, von denen die folgenden Normen zum jetzigen Zeitpunkt bereits veröffentlicht wurden.

In Teil 1 geht es um die allgemeinen Grundlagen:
- IEC TS 62443-1-1: Teil 1: Begriffe und Modelle
- IEC TS 62443-1-5: Teil 1–5: Schema für IT-Sicherheitsprofile aus IEC 62443

Teil 2 bezieht sich auf die Sicherheitsanforderungen für Betreiber und Dienstleister:
- IEC 62443-2-1: Einrichten eines Programms zur IT-Sicherheit für industrielle Automatisierungssysteme
- IEC 62443-2-2: IACS-Sicherheitsprogramm-Einstufungen
- IEC TR 62443-2-3: Patch-Management für industrielle Automatisierungssysteme
- IEC 62443-2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme

Teil 3 bezieht sich auf die Sicherheitsanforderungen an Automatisierungssysteme
- IEC TR 62443-3-1: Techniken für industrielle Automatisierungssysteme
- IEC TR 62443-3-2: Sicherheitsrisikobeurteilung und Systemgestaltung
- IEC 62443-3-3: Systemanforderungen zur IT-Sicherheit und Security-Level

Teil 4 beschreibt die Sicherheitsanforderungen an Automatisierungskomponenten
- IEC 62443-4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung
- IEC 62443-4-2: Anforderungen an Komponenten industrieller Automatisierungssysteme

Teil 5 legt Profile der IEC 62443 fest
- IEC TS 62443-1-5: Schema für IT-Sicherheitsprofile aus IEC 62443

Teil 6 beschreibt die Evaluationsmethodik
- IEC 62443-6-1: Methodik der Sicherheitsevaluation für IEC 62443-2-4

7.2.2. Security Level (SL)

Die Anforderungen an Systeme und Komponenten werden mit Security-Levels beschrieben. Diese sind wie folgt definiert:

- Security Level 0: Keine besondere Anforderung oder Schutz erforderlich
- Security Level 1: Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
- Security Level 2: Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation
- Security Level 3: Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln mit moderaten Ressourcen, IACS-spezifischen Kenntnissen und moderater Motivation
- Security Level 4: Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel mit umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation

Das heißt, je höher der geforderte Security Level, desto wirksamere Maßnahmen müssen umgesetzt werden.

Es gibt sieben grundlegende Anforderungen (englisch: Foundational Requirements, FR):

- FR 1 – Identifizierung und Authentifizierung
- FR 2 – Nutzungskontrolle
- FR 3 – Systemintegrität
- FR 4 – Vertraulichkeit der Daten
- FR 5 – Eingeschränkter Datenfluss
- FR 6 – Rechtzeitige Reaktion auf Ereignisse
- FR 7 – Ressourcenverfügbarkeit

Hinter jeder dieser grundlegenden Anforderungen verbergen sich Maßnahmen unterschiedlicher Qualität, die angewendet werden können, um den erforderlichen Level zu erreichen. Typische Maßnahmen sind Multifaktor-Authentifizierung oder Verschlüsselungsmechanismen.

Welches Schutzniveau erreicht werden muss, hängt vom Cyberrisiko ab. Der europäische Gesetzgeber unterscheidet beispielsweise zwischen wichtigen und wesentlichen Einrichtungen. Von welchem Cyberrisiko ausgegangen werden muss, hängt also von der Art des Unternehmens, der Größe des Unternehmens und den möglichen Auswirkungen ab. Derzeit befassen sich verschiedene Normungsorganisationen mit der Thematik und sind dabei, allgemeingültige Anforderungen für Branchen und Maschinenarten zu definieren.

7.2.3. Information Security Management System (ISMS)

Neben den technischen Anforderungen an Komponenten und Systeme gibt es auch organisatorische Maßnahmen, die umgesetzt werden müssen, um das Risiko eines erfolgreichen Angriffs zu reduzieren. Hierbei muss jedes Unternehmen für sich entscheiden, wie es das Information Security Management System (ISMS) aufbauen möchte. Allgemein bekannt und etabliert ist die Normenreihe ISO/IEC 27000. IEC 62443-2-1 kann als Leitfaden zur Umsetzung von ISO/IEC 27001 auf die industriellen Automatisierungssysteme angesehen werden. Daneben gibt es unter anderem noch das Zertifizierungsprogramm der Automobilindustrie TISAX, welches sich ebenfalls als geeignet erweist.

Im ISMS werden die Risiken benannt, klassifiziert, bewertet und der Umgang mit ihnen beschrieben. Typischerweise müssen zunächst der Anwendungsbereich und die Schnittstellen zu weiteren Bereichen definiert werden. Ebenfalls essenziell ist:
- die Übernahme der Verantwortung für Security durch die Geschäftsleitung
- die Klärung der Verantwortlichkeiten
- die Definition von Fortbildungsmaßnahmen
- die Erstellung von Sicherheitsrichtlinien im Unternehmen

Das ISMS hilft dabei, systematisch die Risiken zu betrachten und entsprechende Maßnahmen abzuleiten.

Unternehmensrisiken können unter anderem sein:
- wirtschaftliche Schäden durch Produktionsausfall
- die Verletzung von Mitarbeitern
- Datenschutzverstöße
- Umweltschäden
- der Verlust des Kundenvertrauens

Typische Maßnahmen sind unter anderem:
- die Ausarbeitung anzuwendender Notfallpläne
- die Definition von berechtigten Benutzern
- physische und virtuelle Zugangskontrollen
- Netzwerksegmentierung

Auch die Implementierung von Maßnahmen wird durch das ISMS beschrieben. Hierzu gehören:
- die Systementwicklung
- die Systemwartung
- die Datensicherung
- die Planung und der Umgang mit Vorfällen

7.3. Weitere wegweisende Dokumente für Maschinenhersteller und Betreiber

Neben der Normenfamilie IEC 62443 gibt es bereits weitere Security-Normen, die den Maschinenbau betreffen und Anforderungen festlegen.

IEC TS 63074 beschreibt die Sicherheitsaspekte im Zusammenhang mit der funktionalen Sicherheit von sicherheitsbezogenen Steuerungssystemen. In dieser technischen Spezifikation werden die relevanten Aspekte der Normenfamilie IEC 62443 festgelegt, die berücksichtigt werden müssen, um den sicheren Betrieb einer Maschine zu gewährleisten.

Für die Anforderung „Schutz gegen Korrumpierung“ aus der Maschinenverordnung wird derzeit eine neue europäische Norm, EN 50742, entwickelt. Pilz arbeitet aktiv im Normengremium mit.

Aus der Funkanlagenrichtlinie 2014/53/EU bzw. deren delegierten Verordnung (EU) 2022/30 ergeben sich ebenfalls Security-Anforderungen. Für diese Anforderungen wurde die Normenreihe EN 18031 entwickelt.

7.4. Netzwerksegmentierung anhand des Purdue-Modells

Um das Thema Netzwerksegmentierung zu veranschaulichen, hilft das Purdue-Modell, das Theodore Joseph Williams (Professor für Ingenieurwesen an der US-amerikanischen Purdue-Universität) bereits 1990 veröffentlicht hat. In der folgenden Abbildung wurde das Purdue-Modell für unseren Zweck um beispielhafte Maßnahmen erweitert.

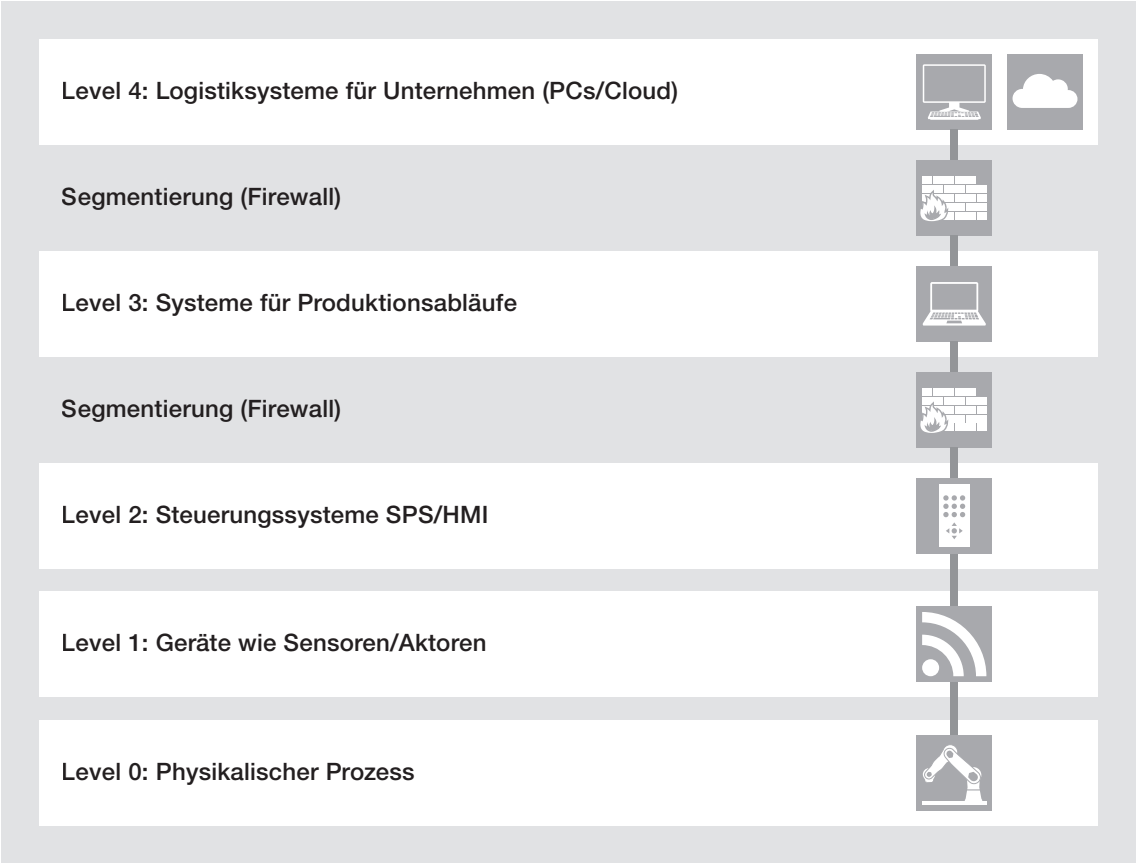

Abbildung 13: Netzwerksegmentierung anhand des Purdue-Modells

Level 0 ist der eigentliche physikalische Prozess, der typischerweise im produzierenden Gewerbe ausgeführt wird. Dieser wird in der Regel mit Sensoren und Aktoren überwacht und angetrieben. Diese Geräte gehören zu Level 1. Gesteuert wird der Prozess typischerweise von einer speicherprogrammierbaren Steuerung (SPS), die Level 2 angehört. Die Programmierung der SPS erfolgt über die Systeme für Produktionsabläufe in Level 3. Die eigentlichen Aufträge kommen aus dem Logistiksystem in Level 4.

Level 0 bis 3 fallen unter die Bezeichnung Operational Technology (OT), Level 4 und alles, was darüber hinausgeht, fällt unter die Bezeichnung Information Technology (IT).

Die Abbildung zeigt bereits eine Art der Segmentierung, die in diesem Beispiel über Firewalls funktioniert, die den Datentransfer zwischen Level 4 und 3 bzw. 3 und 2 einschränken, um die potenzielle Angriffsfläche zu minimieren.

Ziel ist es, eine erfolgreiche Segmentierung zu realisieren, das heißt sowohl eine wirksame Reduzierung der Angriffsmöglichkeiten als auch ein System zu haben, das in der Performance nicht eingeschränkt wird. Dafür ist es erforderlich, dass die Schnittstellen klar definiert sind, mit dem Ergebnis, dass beispielsweise alle notwendigen Ports und Protokollarten bei der Konfiguration der Firewalls berücksichtigt werden.

Die korrekte Auswahl der richtigen Komponenten ist für einen sicheren Betrieb unabdingbar. Schließlich bringt die beste Firewall nichts, wenn durch die Komponenten in den unteren Levels weitere Schwachstellen entstehen. Je nach erforderlichem Security Level kann es notwendig sein, dass sich die Komponenten im System gegenseitig authentifizieren und somit Änderungen am System überwacht werden. Dies muss bei der Auswahl der Komponenten und deren Konfiguration ebenfalls berücksichtigt werden.

In diesem Beispiel sind alle Komponenten ab Level 3 fest miteinander verdrahtet, und der Informationsfluss wird durch zwei Firewalls abgesichert. Es ist im industriellen Umfeld durchaus üblich, dass die Systeme auch kabellose Schnittstellen (z. B. bei fahrerlosen Transportsystemen) haben. Hier muss geprüft werden, wie man Sicherheitsmaßnahmen wirksam umsetzen kann.

Praxistipp:
Praktische Beispiele zur Konfiguration Ihrer Geräte erhalten Sie auf **www.pilz.com**, nutzen Sie hierfür einfach die Suchfunktion mit dem Stichwort „application notes“.

8. Literatur

- 1. Reference model for computer integrated manufacturing (CIM): a description from the viewpoint of industrial automation. Edited by Theodore J. Williams, 1989
- 2. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels IEC 62443-3-3:2013
- 3. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components IEC 62443-4-2:2019
- 4. EU-Maschinenverordnung 2023/1230 (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32023R1230)
- 5. Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555)
- 6. Cyber Resilience Act P9_TA(2024)0130 (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.pdf)
- 7. Richtlinie 2009/104/EG (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32009L0104)
- 8. Agentur der Europäischen Union für Cybersicherheit (https://www.enisa.europa.eu/)
- 9. Pilz GmbH & Co. KG (https://www.pilz.com/de-DE/produkte/industrial-security/security-incident-management)
- 10. VDMA e. V. (https://www.vdma.org/cybersecurity)
- 11. Information security, cybersecurity and privacy protection – Information security management systems – Requirements ISO/IEC 27001
- 12. Whitepaper Industrial Security (Pilz 2018) (www.pilz.com/security)
- 13. Whitepaper Leitfaden zur Maschinenverordnung (Pilz 2023) (www.pilz.com/mr)
- 14. https://de.statista.com/statistik/kategorien/kategorie/21/themen/896/branche/cyberkriminalitaet/#overview (gesehen 20.01.2025)
- 15. Cybersecurity Act EU 2019/881, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1728407971719

Support

Technische Unterstützung von Pilz erhalten Sie rund um die Uhr.

Amerika
Brasilien
+55 11 97569-2804
Kanada
+1 888 315 7459
Mexiko
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asien
China
+86 400-088-3566
Japan
+81 45 471-2281
Südkorea
+82 31 778 3390

Australien und Ozeanien
Australien
+61 3 95600621
Neuseeland
+64 9 6345350

Europa
Belgien, Luxemburg
+32 9 3217570
Deutschland
+49 711 3409-444
Frankreich
+33 3 88104003
Großbritannien
+44 1536 460866
Irland
+353 21 4804983
Italien, Malta
+39 0362 1826711
Niederlande
+31 347 320477
Österreich
+43 1 7986263-444
Schweiz
+41 62 88979-32
Skandinavien
+45 74436332
Spanien
+34 938497433
Türkiye
+90 216 5775552

Unsere internationale Hotline erreichen Sie unter:
+49 711 3409-222
support@pilz.com

Pilz entwickelt umweltfreundliche Produkte unter Verwendung ökologischer Werkstoffe und energiesparender Techniken. In ökologisch gestalteten Gebäuden wird umweltbewusst und energiesparend produziert und gearbeitet. So bietet Pilz Ihnen Nachhaltigkeit mit der Sicherheit, energieeffiziente Produkte und umweltfreundliche Lösungen zu erhalten.

BLUECOMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

German Standards BRAND OF THE CENTURY 2022

Qualitätsmanagement ISO 9001:2015 REG. NR. 2462
Umweltmanagement ISO 14001 REG. NR. 2462
Energiemanagement ISO 50001 REG. NR. 2462

Überreicht durch:

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Deutschland
Telefon: +49 711 3409-0
E-Mail: info@pilz.com, Internet: www.pilz.com

Wir sind international vertreten. Nähere Informationen entnehmen Sie bitte unserer Homepage www.pilz.com oder nehmen Sie Kontakt mit unserem Stammhaus auf.

Stammhaus: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Deutschland
Telefon: +49 711 3409-0, E-Mail: info@pilz.de, Internet: www.pilz.com

Der Umwelt zuliebe gedruckt auf 100 % Recyclingpapier.

PILZ
THE SPIRIT OF SAFETY

8-4-de-3-023, 2025-04 Printed in Germany