Hintergrundinformation

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Deutschland/Germany
www.pilz.com

Schutz für Unternehmen, Maschinen und Produkte

Safety und Industrial Security – Alles aus einer Hand

Ostfildern, Oktober 2025 - **Gegenstand von Security-Vorfällen sind nicht mehr nur IT-Systeme, sondern zunehmend das produzierende Umfeld (OT). Als Vorfälle im Bereich der Industrial Security gelten nicht nur gezielte Angriffe, sondern auch unbewusste Manipulationen. Aufgabe der Industrial Security in der Produktion ist es, die Verfügbarkeit von Maschinen und Anlagen, sowie die Integrität und Vertraulichkeit von maschinellen Daten und Prozessen zu gewährleisten. Das höchste Schutzziel ist jedoch die funktionale Sicherheit. Denn letztlich gilt: Wenn Unternehmen nicht die Hoheit über ihre Daten haben, dann steht das Unternehmen und die Sicherheit der Mitarbeiter auf dem Spiel: Ohne Security keine Safety und ohne Safety kein Schutz des Menschen!**

Innerhalb der EU wurde die zunehmende Bedrohungslage erkannt und die Gesetzgebung daran angepasst: Auf Unternehmensebene fordert die **Richtlinie NIS 2** Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, beispielsweise durch ein Informationssicherheitsmanagementsystem.

Die **EU-Maschinenverordnung 2023/1230** sieht für Maschinen und Anlagen jetzt den Schutz gegen Korrumpierung vor, und verlangt Industrial Security-Maßnahmen für die Teile der Maschine mit Einfluss auf die funktionale Sicherheit.

Der **Cyber Resilience Act (CRA)**, fordert Security-Maßnahmen für Produkte mit digitalen Elementen. Darunter fallen auch Steuerungen,

IO-Systeme und weitere Komponenten, die in Maschinen eingesetzt werden.

Unternehmen, Maschinen und Produkte – Auf jeder Ebene kommen unterschiedliche Herausforderungen und unterschiedliche gesetzliche Rahmenbedingungen auf Maschinenbauer und -betreiber zu.

State-of-the-art Sicherheit

Unabhängig davon, dass die Gesetzgebung Industrial Security verpflichtend macht, gibt es eine Reihe guter Gründe sich frühzeitig mit dem Thema zu beschäftigen und beraten zu lassen. Etablierte Abläufe und Gegebenheiten für den Betrieb von Maschinen können Manipulationen begünstigen, wenn sie nicht regelmäßig hinterfragt werden. Beispielsweise führt eine lange Lebensdauer von Maschinen häufig dazu, dass die dazugehörigen Systeme in die Jahre kommen und irgendwann nicht mehr den aktuellen Standards der Security entsprechen. Diese Systeme verfügen über Sicherheitslücken, die nicht mehr geschlossen werden können, weil der Anbieter keine Security-Updates mehr liefert. Auch kann der Schutz vor Schadsoftware häufig nicht auf den Endgeräten implementiert werden, da diese teilweise zu alt und deren Perfomance dadurch leiden würde, so dass es zu Ausfällen der Produktion kommen kann.

Schrittweise zu mehr Industrial Security

Letztlich geht es darum, dass der Geschäftsbetrieb geschützt bleibt, doch dafür müssen Unternehmen unterschiedliche Herausforderungen meistern: Das reicht von der Identifizierung der geltenden gesetzlichen Vorschriften, der Erkennung und Behebung von Schwachstellen in Systemen, über die Sensibilisierung und Schulung der Mitarbeiter bis hin zur anschließenden Implementierung von Kontrollen. Da Security ein sogenanntes „moving target“ ist, ist zudem eine regelmäßige Überprüfung des Industrial Security Status

der Maschinen notwendig. Wichtig sind dabei klare Verantwortlichkeiten im Unternehmen, ein systematisches Vorgehen, das den Aufbau des erforderlichen Fachwissens einschließt.

Das Automatisierungsunternehmen Pilz hat sich auf diese Anforderungen eingestellt und für Maschinenbauer und Anwender international ein maßgeschneidertes Dienstleistungsportfolio aufgebaut, das ganzheitlich alle Aspekte für den Schutz von Mensch und Maschine einbezieht. Die Experten von Pilz kennen die aktuellen gesetzlichen und normativen Anforderungen und lassen diese in ihre Beratung einfließen. Um das Security-Wissen in Unternehmen aufzubauen oder auf Stand zu bringen, ergänzen Trainings das Angebot. Die praktische Umsetzung erfolgt auch mithilfe von Pilz Produktlösungen, wie etwa dem Angebot zum Identification and Access Management – I.A.M. für mehr Safety und Industrial Security.

Das richtige Fundament legen

Um Industrial Security an den eigenen Maschinen sicherzustellen, benötigen Fachkräfte im Maschinen- und Anlagenbau fundiertes Grundlagenwissen – insbesondere zu Gesetzgebung sowie geltenden Normen. Die Experten von Pilz geben in der Schulung „Grundlagen Industrial Security“ dieses Know-how weiter. Teilnehmer lernen Security Bedrohungen, passende Schutzmaßnahmen und Best Practices im Kontext von Maschinen- und Netzwerksicherheit zu verstehen. Damit lernen auch Einsteiger in das Thema Security, mit welchen Maßnahmen sie Maschinen vor Cyber-Attacken und Manipulation auf maschineller Produktionsebene wirkungsvoll schützen können.

Mit der Qualifizierung zum „CESA – Certified Expert for Security in Automation“ bietet Pilz einen zweitägigen Expertenlehrgang, der den Teilnehmern vertiefendes Security-Wissen auf dem aktuellen Stand

der Normenlage, insbesondere unter Beachtung der Normenreihe IEC 62443 („Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“), vermittelt. Darüber hinaus werden praktische Maßnahmen zur Risikominderung behandelt, wie Zugangskontrolle, Erhöhung der Netzwerk-Sicherheit mit technischen Mitteln sowie organisatorische Maßnahmen zur Verminderung von Security-Risiken. Die Teilnehmer lernen, wie sie die Norm korrekt anwenden und nachweisen können, dass ihre Automatisierungssysteme den Anforderungen an die Cybersicherheit entsprechen. Bei bestandener Prüfung erhalten die Teilnehmer das weltweit anerkannte TÜV NORD -Zertifikat zum "CESA – Certified Expert for Security in Automation".

Theoretisches Wissen in die Praxis umsetzen

Aufbauend auf den theoretischen Grundlagen und den Schulungen, besteht der nächste Schritt zur Stärkung der Industrial Security in der Anwendung strukturierter, praxisorientierter Prozesse. Die Beratung im Bereich Operational Technology (OT) schafft den Übergang der theoretischen Basis zu umsetzbaren Strategien. Mithilfe eines schrittweisen Vorgehens werden im Zuge der Industrial Security Services Schwachstellen in komplexen Systemen identifiziert und Maßnahmen zur Risikominderung entwickelt. Daraus ergibt sich ein ganzheitlich gedachtes Sicherheitskonzept.

Vier Schritte für mehr Industrial Security

Die OT-Security Prozessschritte umfassen vier Schritte: Schutzbedarfsanalyse, Industrial-Security-Risikobewertung, Industrial-Security-Konzept und Industrial-Security-System-Verifikation.

Bei der Schutzbedarfsanalyse werden im Unternehmen der Schutzbedarf der einzelnen "Assets" in der Maschine oder Anlage sowie deren Schutzziele ermittelt. Im zweiten Schritt, der

Risikobewertung, werden sämtliche Risiken und mit welcher Wahrscheinlichkeit sie eintreten betrachtet, und zwar für jeden Teilbereich über den kompletten Lebenszyklus des Systems hinweg. Der nächste Schritt sieht die Erstellung eines detaillierten Industrial-Security-Konzepts mit Strategien und Maßnahmen zur Abwehr und Milderung von Risiken, hervorgerufen durch Angriffe, Manipulationen und Fehlbedienungen, vor. Hinzu kommt die Erstellung von Policies, Regeln und Richtlinien für den weiteren sicheren Betrieb oder Aufbau des Systems. Im letzten Schritt, der Industrial-Security-System-Verifikation, wird die Wirksamkeit der implementierten Gegenmaßnahmen überprüft.

Maschinenverfügbarkeit sichern

Der Prozess der Industrial Security Services hilft, Cyberangriffe abzumildern oder zu verhindern. Auch die Zahl unbeabsichtigt ausgelöster Security-Vorfälle sinkt. Das wiederum erhöht die Maschinenverfügbarkeit und sorgt letzten Endes für Kostenersparnis und die Wahrung der Wirtschaftlichkeit.

Diese Vorgehensweise schützt vor allem Menschen an der Maschine mit entsprechenden Security-Maßnahmen. Denn ein Security-Vorfall kann zum Hindernis von Safety-Maßnahmen werden. So sorgt beispielsweise ein Lichtgitter vor Maschinen dafür, dass der Bediener nicht in einen Gefahrenbereich übertritt. Wenn jedoch ein Angreifer Einfluss auf die entsprechende Steuerung und den Mechanismus nehmen kann, kann die Schutzfunktion des Lichtgitters nicht mehr gewährleistet werden. Security schützt Safety!

Bei der konkreten Umsetzung an der Maschine macht also eine gemeinsame Betrachtung von Safety und Security Sinn. Denn: ohne Security keine Safety und ohne Safety kein Schutz des Menschen.

Klar geregelt: Wer darf was an der Maschine?

Die Sicherheit einer Maschine und ihrer Bediener steht und fällt mit der Regelung der Zugänge – egal ob für Mensch oder Netzwerk. Zugänge müssen gegen unbefugten Zugriff gesichert werden, damit sich beispielsweise beim Betrieb der Maschine keine Personen im Gefährdungsbereich aufhalten. Denn selbst das gut gemeinte Bedienen oder Warten einer Anlage – ob vor Ort oder über ein Netzwerk – könnte fatale Folgen haben.

Ein wichtiger Baustein ist ein Identification and Access Management (I.A.M.), das Berechtigungen und Zugänge an Maschinen und Anlagen in Unternehmen klar regelt. Dazu gehören organisatorische Maßnahmen und Vorgaben genauso wie passende Sicherheitsfunktionen. Ein Zugangsberechtigungssystem wie PITreader von Pilz stellt dabei den passenden Produkt-Baustein dar. Damit können Anwender die Anforderungen bezüglich Mitarbeiterschutz, Haftungsschutz, maximaler Produktivität sowie des Schutzes Ihrer Daten meistern.

Nur eine ganzheitliche Betrachtung von Safety und Security gewährleistet einen umfassenden Schutz von Mensch und Maschine. Ob und in welcher Tiefe sich ein Unternehmen mit Security auseinandersetzen will, ist nicht länger Ermessenssache des Unternehmens. Inzwischen ist es eine gesetzliche Vorgabe. Im Maschinenbau ist Security in Form von Industrial Security nicht allein Aufgabe der IT, sondern integraler Bestandteil der Konzeption und Konstruktion. Security im Nachhinein zu implementieren ist aufwändig und bedeutet meist Einbußen bei Anwenderfreundlichkeit, Funktionalität und Produktivität.

((Zeichen: 9.784))

((Kasten:))

Die EU-Gesetzgebung zum Thema Industrial Security im Überblick:

Insbesondere in Europa reagiert der Gesetzgeber auf die Bedrohungslage mit einer Reihe von Gesetzen. Damit gelten in Europa die weltweit schärfsten Vorgaben. Aber es laufen bereits Abstimmungen mit anderen Ländern, und auch dort werden solche Gesetze kommen. Es ist also eine weltweite Harmonisierung bei Industrial Security zu erwarten.

NIS 2: Mehr Pflichten für Unternehmen

NIS (Netz- und Informationssicherheit) ist eine Richtlinie der Europäischen Union zur Stärkung der Cybersicherheit. Diese Richtlinie gibt es bereits seit 2016 und sie galt bislang für Anbieter im Bereich kritische Infrastrukturen, darunter Energie, Verkehr, Banken und Finanzen, Gesundheit, Trinkwasserversorgung und -verteilung sowie digitale Infrastruktur. Anbieter in diesen Sektoren mussten mit Blick auf die Security „angemessene Sicherheitsvorkehrungen“ treffen und gravierende Cybersicherheitsvorfälle melden. Die neue NIS-2-Richtlinie ((EU) 2022/2555 ... über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union) verpflichtet künftig deutlich mehr Unternehmen, Risikomanagementmaßnahmen für die Cybersicherheit zu ergreifen. NIS 2 erweitert die Sektoren beispielsweise um das herstellende/produzierende Gewerbe, darunter auch Maschinenbau und Hersteller von elektrischen Ausrüstungen.

Gefordert werden Risikoanalysen und Sicherheitskonzepte für Informationssysteme, den Schutz der Lieferkette und die Sicherheit des Personals. Ebenso zählen Konzepte für die Zugriffskontrolle und

das Management von Anlagen hinzu, sowie verpflichtende Schulungen für das Management.

Die Richtlinie wurde Ende 2022 durch das Europäische Parlament und den Rat der EU verabschiedet. Wie alle EU-Richtlinien ist auch NIS 2 in den einzelnen EU-Mitgliedsstaaten nicht unmittelbar wirksam und verbindlich, sondern muss durch die Mitgliedsstaaten in nationales Recht umgesetzt werden. Unternehmen tun gut daran, sich baldmöglichst mit NIS 2 zu beschäftigen und eine umfassende Security-Betrachtung für das Unternehmen durchzuführen. Dazu gehört beispielsweise der Aufbau eines Managementsystems für Informationssicherheit (ISMS). Hilfreich ist in diesem Zusammenhang eine Zertifizierung nach der Informationssicherheits-Norm ISO 27001.

NIS 2 am Beispiel Windkraftanlagen: Mit NIS 2 müssen künftig auch Maschinenbauer, wie etwa ein Hersteller von Anlagen zur Stromerzeugung (z.B. Windkraftanlagen), die Vorgaben erfüllen. Der Hersteller der Windkraftanlage wiederum benötigt etwa Automatisierungslösungen, Steuerungen oder Sensoren. Ab einer bestimmten Größe fallen auch Hersteller von elektrischen Komponenten unter NIS 2. Und da NIS 2 auch die Berücksichtigung von Lieferanten vorschreibt, muss sich auch ein Unternehmen wie Pilz um sichere Lieferketten kümmern und Anforderungen an seine Lieferanten stellen. NIS 2 deckt also die komplette Lieferkette ab.

Die neue Maschinenverordnung: Ohne Security keine CE-Kennzeichnung

Im Rahmen der funktionalen Sicherheit von Maschinen kommt der Maschinenrichtlinie 2006/42/EG eine besondere Bedeutung zu.

Seit jeher müssen Maschinenbauer, um Maschinen in Europa einführen zu können, ein entsprechendes Konformitätsbewertungsverfahren durchlaufen an dessen Ende die CE-Kennzeichnung steht.

Im Juni 2023 neu als Maschinenverordnung veröffentlicht, wurden die Vorgaben auf den aktuellen Stand der Technik gebracht. Da sie eine Verordnung ist, muss sie nicht erst in nationales Recht übertragen werden. Maschinenhersteller haben bis 20. Januar 2027 Zeit, auf die neuen Anforderungen umzustellen und diese ab dem Stichtag zu erfüllen.

Die Maschinenverordnung ersetzt die bisherige Maschinenrichtlinie und macht, im Unterschied zur Vorgängerin, Cybersecurity verpflichtend. War die Maschinenrichtlinie eine reine Betrachtung der Safety, wurde in der Verordnung das Schutzziel Security unter „Protection against corruption“ in die „Essential health and safety requirements (EHSR)” mit aufgenommen: Die Sicherheitsfunktionen der Maschine dürfen durch unbeabsichtigte oder vorsätzliche Verfälschung nicht beeinträchtigt werden.

Dieser neue Weg zur CE-Kennzeichnung wirft für Maschinenbauer und -betreiber eine Reihe neuer Fragestellungen auf, denn sie werden ihre bisherigen Sicherheitskonzepte für Safety und Security überarbeiten müssen.

Cyber Resilience Act: Security über den kompletten Produkt-Lebenszyklus

Neben Betrachtung des Unternehmens und der Maschinen ist es unbedingt erforderlich, auch Security-Maßnahmen direkt in den Geräten (wie etwa Steuerungen) zu implementieren. Im September

2022 hat die Europäische Kommission 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 Produkte sowohl aus dem B2C-Bereich, wie Smartphones oder Staubsaugerroboter, als auch aus dem B2B-Bereich, wie Steuerungen und Sensoren, aber auch reine Softwareprodukte wie Betriebssysteme oder die Maschine selbst.

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

Wie groß die Auswirkungen des CRA tatsächlich sein werden, hängt davon ab, welche Kriterien am Ende für die Einstufung der Produkte angelegt werden. Laut CRA dürfen nur noch Produkte in Verkehr gebracht werden, die ein angemessenes Cybersicherheitsniveau gewährleisten – und zwar über den gesamten Lebenszyklus eines Produkts. Security beginnt also in der Produkt-Entwicklung. Seit einigen Jahren richtet Pilz seine Entwicklungsprozesse daher auch an der IEC 62443-4-1 „Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements“ aus und entwickelte beispielsweise die SecurityBridge nachweislich „secure“.

((Zeichen: 6.062))

Pilz – The Spirit of Safety

Pilz ist globaler Anbieter von Produkten, Systemen und Dienstleistungen für die Automatisierungstechnik. Als Pionier der sicheren Automation schafft Pilz Sicherheit für Mensch, Maschine und Umwelt. Gegründet 1948 ist das Familienunternehmen mit Stammsitz in Ostfildern heute weltweit mit 2.500 Mitarbeiterinnen und Mitarbeitern in 42 Tochtergesellschaften und Niederlassungen vertreten.

Der Technologieführer bietet komplette Automatisierungslösungen für Safety und Industrial Security an der Maschine. Diese umfassen Sensorik sowie Steuerungs- und Antriebstechnik – inklusive Systemen für die industrielle Kommunikation, Diagnose und Visualisierung. Ein internationales Dienstleistungsangebot mit Beratung, Engineering und Schulungen rundet das Portfolio ab. Lösungen von Pilz kommen über den Maschinen- und Anlagenbau hinaus in zahlreichen Branchen zum Einsatz, wie etwa der Intralogistik, der Verpackung und der Bahntechnik oder im Bereich Robotik.

www.pilz.com

Pilz in sozialen Netzwerken:

Auf unseren Social-Media-Kanälen geben wir Hintergrundinformationen rund um das Unternehmen sowie die Menschen bei Pilz und berichten über Aktuelles aus der Automatisierungstechnik.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Kontakt für die Presse:

Martin Kurth
Unternehmens- und Fachpresse
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer
Fach- und Unternehmenspresse
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman
Fachpresse
Tel: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rössle
Fachpresse
Tel: +49 711 3409-7147
e.roessle@pilz.de