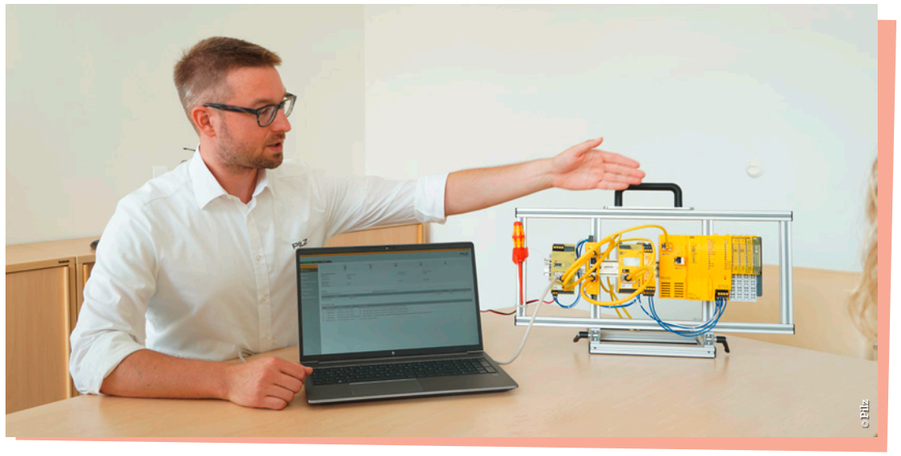


NIS 2: Cybersecurity ist niemals statisch

Die NIS 2 adressiert nicht nur die kritische Infrastruktur, sondern weitet die Sektoren massiv auf wesentliche und wichtige Einrichtungen aus. Beispielsweise das verarbeitende/herstellende Gewerbe.

Künftig werden Maschinen und Anlagen kein CE-Zertifikat erhalten und damit nicht auf dem Markt angeboten werden können, ohne dass Security-Risiken analysiert worden sind. „Keine Safety ohne Security" ist jedoch nur ein Teilbereich mehrerer, umfassender gesetzlicher Maßnahmenpakete. Unternehmer:innen und generell Branchen, für die es bisher keine gesetzlich induzierte Notwendigkeit gab, Cybersecurity-Maßnahmen umzusetzen, sehen sich künftig durch die Maschinenverordnung (MVO) EU 2023/1230, dem Cyber Resiliance Act (CRA) EU 2022/0272 und der Richtlinie für Netzwerk- und Informationssicherheit 2 (NIS 2) EU 2023/2555 erstmalig mit Verpflichtungen konfrontiert. Mit Produkten, Dienstleistungen und Expertenlehrgängen von PILZ werden Maschinen sowie Produktionsanlagen geschaffen und betrieben, die nicht nur safe, sondern auch secure sind – um den kommenden gesetzlichen und normativen Anforderungen zu entsprechen.

Geltungsbereich ausgeweitet

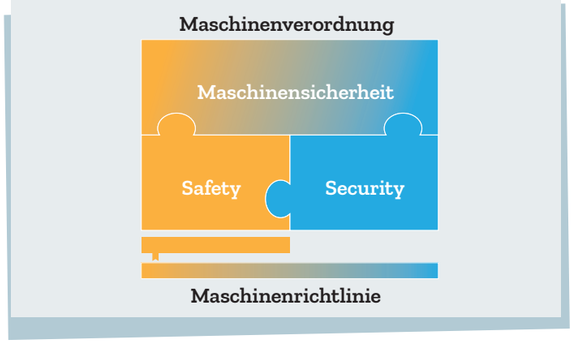
Die NIS 2 adressiert nicht nur die kritische Infrastruktur, sondern weitet die Sektoren massiv durch wesentliche und wichtige Einrichtungen aus. Zu zweiterer zählt das verarbeitende/herstellende Gewerbe: Maschinenbau, Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, elektrischer Ausrüstungen sowie Hersteller von Kraftwagen, Kraftwagenteilen und sonstiger Fahrzeugbau. Unternehmen, die sich darin wiederfinden und mehr als 50 Personen beschäftigen oder mehr als 10 Mio. Euro Jahresumsatz/Jahresbilanz erwirtschaften, also laut Empfehlung der EU-Kommission ein Unternehmen mittlerer Größe sind, benötigen aktiv einen verbesserten Risikomanagementansatz (NIS 2, Kap. IV, Art. 21). Risiken und technische sowie organisatorische Milderungsmaßnahmen müssen nicht nur im (Office-)IT-Netzwerk betrachtet werden, sondern ebenso im (Produktions-) OT-Netzwerk. Die internationale Normenreihe IEC 62443 betrachtet hierfür die Security von Industrial Automation and Control Systems (IACS).

Grundlegendes Verständnis

Wer ist für die Sicherheit Ihres Produktionsnetzwerks zuständig? Obwohl der Werkzeugkasten von IT- und OT-Netzwerkspezialisten Schnittmengen hat, so gehören Industriesteuerungen und Industrieprotokolle nicht zum üblichen Standard-Repertoire eines IT-Systemadministrators. Die Schutzziele, also Confidentiality,

Integrity und Availability sind zwischen IT und OT, bis auf Ausnahmen, meist völlig konträr. In Büroumgebungen ist ein temporärer Ausfall der Computersysteme verkraftbar. Eine Fertigungsanlage, die für einige Stunden zum Stillstand gezwungen wird, ist meist verheerend. Auch die Sicherheit der Lieferketten und Abhängigkeiten von Partnerunternehmen müssen betrachtet und inkludiert werden. Cybersecurity-Schulungen für das Top-Management werden verpflichtend, um ein grundlegendes Verständnis über diese Thematik sicherzustellen, denn die Maßnahmen haben von der Führungsebene auszugehen. Bei Nichterfüllung drohen Sanktionen von 7 Mio. Euro oder 1,4 % des Gesamtjahresumsatzes des Unternehmens bei wichtigen Einrichtungen. Auch können natürliche Personen als leitende Angestellte können für Pflichtverletzungen haftbar gemacht werden. Österreich hat, wie alle EU-Mitgliedsstaaten, die NIS 2-Richtlinie bis zum 17. Oktober 2024 in nationales Gesetz zu überführen.

Die Maschinenverordnung EU 2023/1230 hingegen hat immanenten Gesetzescharakter in der Europäischen Union. Die bisherige Maschinenrichtlinie 2006/42/EG stand traditionell für Maschinen-Safety, also Schutz des Menschen vor Gefahren der Maschine, etwa durch bewegliche Maschinenteile. Völlig neu für viele Maschinen- und Anlagenbauer, adressiert die Maschinenverordnung EU 2023/1230 jedoch auch Security-Maßnahmen für den Schutz der Maschine vor Korrumpierung durch Menschen, die andere Menschen sowie die Maschine selbst gefährden, z.B. Schutz vor unautorisierten Zugriffen und ungewollte Modifikation von Signalen oder Daten. Ursächlich hierfür ist nicht nur böswillige und vorsätzliche Manipulation durch Dritte, sondern auch unbeabsichtigte/zufällige Fehlbedienungen. Dabei ist nicht nur die Korrumpierung industrieller Steuerungssysteme und Edge Devices zu bewerten, die im Internet exponiert sind, sondern auch jene die nur im lokalen Netzwerk eingebunden oder gar vollständig offline sind. Ein offline geglaubter Industriecomputer ist schnell im Internet, wenn ein Wartungs-Notebook, das mit einem Hotspot verbunden ist, in die Anlage eingesteckt wird. Die Liste der Angriffsvektoren ist nicht endend. Die MVO ist am 19.07.2023 in Kraft getreten. Der Übergangszeitraum endet per 31.12.2026. Am 20.01.2027 erlangt die MVO ihre alleinige Gültigkeit.



Geschlossener Kreis gesetzlicher Maßnahmen

Der Cyber Resiliance Act (CRA) 2022/0272 ist ein Vorschlag für eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, d.h. die Software enthalten und vernetzt sind – von Konsumgütern bis hin zu Industriekomponenten. Der CRA wird künftig eines der wichtigsten Cybersecurity-Gesetze für den europäischen Markt. Produkthersteller sollten Vorgaben daraus bereits heute umsetzen, um künftig die Konformität ihrer Produkte im Rahmen der CE-Kennzeichnung sicherzustellen. Die europäische Kommission begründet den CRA mit der Tatsache, dass Hardware- und Softwareprodukte zunehmend zum Ziel erfolgreicher Cyberangriffe werden. Jährlich entstehen Kosten der Cyberkriminalität in Höhe von 5,5 Billionen EUR. Beispielhaft werden der Ransomware-Wurm WannaCry genannt, der 200.000 Computer in 150 Ländern befallen hatte und einen Schaden in Höhe von einigen Milliarden USD verursachte sowie der Angriff auf die Lieferkette von Kaseya VSA, bei dem erfolgreich mehr als 1.000 Unternehmen angegriffen wurden und eine Supermarktkette zur Schließung aller ihrer 500 Ladengeschäfte in ganz Schweden gezwungen hatte. Nur 9 % aller Unternehmen in Europa verfügen über einen ausreichenden Reifegrad, um gegen moderne Cyber-Bedrohungen dieser Art gerüstet zu sein. Produkte, die in Maschinen eingesetzt werden, sollten künftig auch CRA-konform sein. Für die Ausstellung einer EU-Konformitätserklärung ist die Erfüllung der zuvor beschriebenen Gesundheits- und Sicherheitsanforderungen aus der MVO erforderlich. Hiermit schließt sich der Kreis der gesetzlichen Maßnahmenpakete für Hersteller, Integratoren und Betreiber.

Security ist kein statisches, sondern ein sich dynamisch bewegendes Ziel. Es ist nichts, was man einmal macht und dann einen Haken dahinter setzt. Neu entdeckte Schwachstellen und Angriffsvektoren erfordern für Hersteller, Integratoren und Betreiber eine Aufnahme holistischer und kontinuierlicher Security-Aktivitäten in den PDCA-Zyklus gemäß VDI/VDE 2182, gemeinsam mit allen anderen Qualitätsmaßnahmen.

Daher der Appell:

- Konsultieren Sie Spezialisten,
- treffen Sie technische und organisatorische Maßnahmen und
- beschäftigen Sie sich rechtzeitig mit dem Thema der Industrial Security – nämlich jetzt!

Andreas Willert