EU-Vorgaben zur Cybersicherheit

Würde man den Grad der Cybersicherheit aller vernetzten Automatisierungsanwendungen mit Ampelfarben klassifizieren, hätte man sehr viel Rot, etwas Gelb und sehr wenig Grün. Das sollte sich aus Sicht der Betreiber, aber auch der Anbieter, möglichst umgehend ändern. Den einen drohen Bußgelder, den anderen Nachteile hinsichtlich der Wettbewerbsfähigkeit.

Einige neuere EU-Regularien, die in 2022 und 2023 veröffentlicht wurden und nun in den einzelnen Mitgliedsländern in nationales Recht umgesetzt werden, verschaffen der Cybersicherheit besonders in der Automatisierung eine völlig neue Bedeutung. Zu diesen Regelwerken zählen die EU-NIS-2-Direktive zur Netzwerk- und Informationssicherheit (EU-Richtlinie 2022/2555) zusammen mit der Resilienz-Richtlinie 2022/2557, die EU-Maschinenverordnung 2023/1230 sowie die Entwürfe zum EU-Cyber Resilience Act (CRA). Aber auch der EU-Kommissionsentwurf für ein neues Produkthaftungsrecht gehört dazu, also das ProdHaftRL-E aus Dezember 2022 (weitere Details: siehe den EU-Vorschlag für eine Richtlinie über die Haftung für fehlerhafte Produkte). Dadurch wird beispielsweise Software zum Produkt. Das dürfte einige gravierende Veränderungen für die vernetzten Steuerungen von Maschinen und Anlagen zur Folge haben. Aber auch KI-Implementierungen und 3D-CAD-Daten werden zukünftig in die Produkthaftung einbezogen. Man könnte auch noch den Entwurf der KI-Haftungsrichtlinie (KI-HaftRL-E) oder das neue Funkanlagenrecht (EU-Verordnung 2022/30) einbeziehen. Schließlich sind Maschinen mit Bluetooth, WLAN, 4G oder 5G hinsichtlich der Cybersecurity auch von diesem EU-Regelwerk betroffen.

NIS-2 als Startpunkt

Der auf den ersten Blick beeindruckenden Verordnungsflut sollte man durch ein systematisches Vorgehen begegnen und zunächst einmal prüfen, inwieweit man durch die jeweilige Verordnung betroffen ist und ab wann das Regelwerk gilt. Die neue Maschinenverordnung ist zwar im Juli 2023 formal in Kraft getreten. Sie ist z. B. aber erst nach einer dreieinhalbjährigen Übergangszeit verbindlich anzuwenden. Beim CRA existiert ein Entwurf aus September 2022. Er ist sehr weitreichend und betrifft praktisch alle Produkte mit digitalen Elementen, also auch die gesamte Konsumerelektronik. Wann und wie der CRA in den EU-Mitgliedsstaaten in nationales Recht umgesetzt wird, ist noch nicht vollständig geklärt. Sehr ähnlich sieht es beim ProdHaftRL-E aus. Hier gibt es wohl auch noch größeren Diskussionsbedarf, z. B. über die Schnittmengen zur EU-KI-Verordnung, den Umgang mit Beweismitteln, Sammelklagenaspekte durch den Wegfall des 500-Euro-Selbstbehalt usw.

Befassen Sie sich mit der NIS-2-Direktive!

Stand heute (Herbst 2023) sollten sich Managementverantwortliche in Organisationen mit Maschinen und Anlagen zunächst einmal mit der NIS-2-Direktive eingehender befassen. Sie richtet sich an die „wesentlichen“ und „wichtigen“ Betreiber von Netzwerken und IT-Systemen in verschiedenen Marktsegmenten. Diese Vorgabe wird im Oktober 2024 EU-weit gesetzlich verpflichtend. Der entsprechende Referentenentwurf aus dem Bundesinnenministerium zur NIS-2-Umsetzung existiert unter dem Namen „NIS2UmsuCG“ seit Juli 2023 auch schon. Hier wurden nicht nur die Regeln einiger seit vielen Jahren existierender EU-Rechtsvorschriften (also die NIS-1-Richtlinie 2016/1148 sowie die 910/2014 und 2018/1972) überarbeitet, sondern auch erhebliche Strafzahlungen für Gesetzesverstöße spezifiziert – ähnlich zur Datenschutzgrundverordnung, allerdings mit einer deutlichen Ausweitung der privaten Managerhaftung. Gleichzeitig wurde aber auch der Anwendungsbereich hinsichtlich der betroffenen Organisationen deutlich ausgedehnt. NIS-1 umfasst ja praktisch nur die sogenannten „Sektoren mit hoher Kritikalität“, also im Wesentlichen die kritische Infrastruktur. Durch die neue NIS-2-Richtlinie werden nun zum Beispiel auch die Hersteller von elektrischer Ausrüstung und

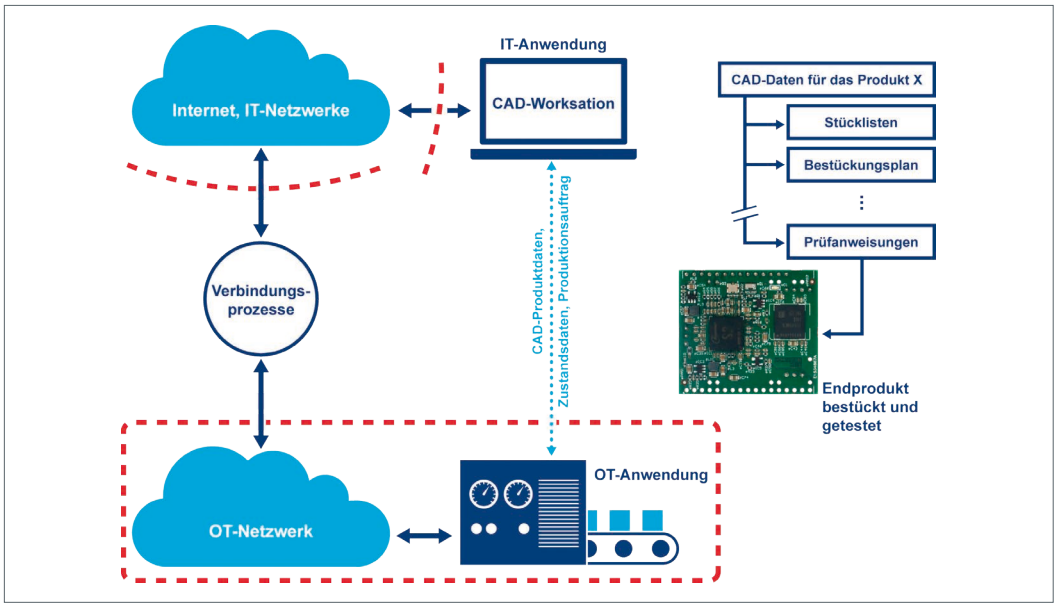

Bild 1: IT-Anwendungen in produzierenden Unternehmen, die bis in das OT-Umfeld reichen, bieten zahlreiche Angriffsvektoren. Ein EMS-Dienstleister erhält z. B. per Cloud die CAD-Produktdaten der Kunden. Diese Daten durchlaufen verschiedene Instanzen an unterschiedlichen Orten. Dabei werden auch externe Teilfertigungsprozesse angestoßen. Häufig bleibt unklar, ob für die CAD-Daten die Quellenauthentizität, Datenintegrität und Vertraulichkeit 100%ig garantiert werden kann.

Autor
Klaus-Dieter Walter
CEO
SSV Software Systems GmbH
www.ssv-embedded.de

Geräten, Maschinen, PKWs usw. ab einer gewissen Betriebsgröße (50+ Mitarbeiter und/oder 10+ Mio. Euro Umsatz) einbezogen. Sie werden in der Richtlinie als „sonstige kritische Sektoren“ bezeichnet. Schätzungen gehen davon aus, dass im Vergleich zu NIS-1 allein in Deutschland ca. 29.000 Unternehmen zusätzlich unter die neuen gesetzlichen Vorgaben zur Netzwerk- und Informationssicherheit fallen. Ungefähr 80 % dieser neu Betroffenen wissen zurzeit allerdings vermutlich noch nicht einmal, dass die NIS-2-Vorgaben auf sie zutreffen.

Mindestanforderungen des Artikel 21

Die deutschsprachige Übersetzung der NIS-2-EU-Verordnung besteht aus 46 Artikeln, sowie den Anhängen I bis III, von denen Anhang I und II in dreispaltigen Tabellen die jeweils betroffenen Organisationen spezifizieren (Sektor, Teilsektor, Art der Einrichtung). Das gesamte PDF umfasst insgesamt 73 Seiten (aus Sicht der betroffenen Organisationen sind die beiden Artikel 21 und 23 von besonderer Bedeutung; siehe Link). Tabelle 1 liefert eine Übersicht der zu erfüllenden NIS-2-Mindestanforderungen für ein einheitliches Cybersicherheitsniveau. Damit will die EU erreichen, dass in den einzelnen Mitgliedstaaten wesentliche und wichtige Einrichtungen (essential and important entities) bzw. Organisationen mit Hilfe von technischen und organisatorischen Maßnahmen einen sicheren Betrieb ihrer operativ erforderlichen Netzwerk- und Informationssysteme gewährleisten. Die Verordnung fordert des Weiteren geeignete Aktivitäten, um die Auswirkungen von Sicherheitsvorfällen in den betroffenen Organisationen möglichst gering zu halten und die Nutzer der Dienstleistungen und Produkte einer unter NIS-2 fallenden Einrichtung entsprechend zu unterstützen.

Artikel 23

Zusammen mit den Registrierungs- und Meldepflichten des Artikel 23 wirken die Anforderungen auf den ersten Blick in Bezug auf lokale Netzwerke und IT-Systeme insgesamt umsetzbar. Durch die Forderung der „Operativen Kontinuität“ in der Tabelle 1 wird allerdings deutlich, dass sich die NIS-2-Vorgaben nicht nur auf die Unternehmens-IT beziehen, sondern auch auf die vernetzten Maschinen und Anlagen in den Produktionsanlagen, ja sogar auf den einzelnen Schaltschrank mit einem Profinet- oder TSN-basierten Netzwerk zur Steuerung einer Verpackungsanlage sowie auf das Modbus-Netzwerk für das Gebäudemanagement; also auch auf alles, was man mittlerweile unter dem Oberbegriff „Operation Technology“ (OT) zusammenfasst.

Übersicht der erforderlichen Mindestmaßnahmen zur Cybersicherheit gemäß Artikel 21 des EU-Amtsblatt 2022/2555.

Anforderung	Kurzbeschreibung
Strategien zur Risikoanalyse	Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme.
Umgang mit Sicherheitsvorfällen	Bewältigung von Sicherheitsvorfällen (Incident Handling).
Operative Kontinuität bzw. Geschäftskontinuität	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall sowie ein geeignetes Krisenmanagement.
Lieferkettensicherheit	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern.
Allgemeine Betriebsrichtlinien	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen.
Bewertungs- und Messsystem	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit.
Kontextbezogene Mitarbeiterschulung	Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit.
Kryptographierichtlinien	Konzepte und Verfahren für den Einsatz von Kryptographie und gegebenenfalls Verschlüsselung.
Personal- und Anlagensicherheit	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Anlagenmanagement.
Richtlinien zur Authentifizierung und sicheren Kommunikation	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Tabelle 1: Betroffene Unternehmen müssen diese Anforderungen plus einige zusätzliche Registrierungs- und Meldepflichten sowohl für IT- als OT-Netzwerke und Systeme in Zukunft erfüllen. Ansonsten sind erhebliche Bußgeldzahlungen möglich.

Grundlegende Aufgaben angehen

In vielen Organisationen sind zunächst einmal grundlegende Aufgaben zu lösen, um NIS-2 umzusetzen. Es beginnt schon mit dem erforderlichen Expertenwissen, um einen Cyberangriff überhaupt zu erkennen und zieht sich wie ein roter Faden bis zu den Auswirkungen einer erfolgreichen Attacke durch das gesamte Thema. In der IT-Welt könnte ein Angreifer beispielsweise den Datenbestand eines Unternehmens verschlüsseln, um einen Erpressungsversuch zu starten. Dass mit einem Mal der Zugriff auf die Unternehmensdatenbanken nicht mehr möglich ist, merken die meisten Opfer in der Regel sofort. Trotzdem können Sie Ihren operativen Betrieb vermutlich in einem Notfallmodus fortsetzen. Mit etwas Glück und einer guten Backup-Strategie lässt sich das Problem eventuell sogar in relativ kurzer Zeit lösen.

Vorsicht in der OT-Welt

In der OT-Welt sind z. B. durch eine kleine Datenmanipulation an einer Produktionsmaschine oder einer Softwarekomponente fehlerhafte Produkte erzeugbar, die unter Umständen die automatischen Endtests erfolgreich durchlaufen und an Kunden und Handelspartner geliefert werden. Hier meldet sich der Angreifer evtl. erst nach einem Jahr, also nachdem beispielsweise schon zigtausende fehlerhafte Baugruppen ausgeliefert wurden und sogar mit der Manipulation immer noch weiter produziert wird, weil ja bisher auf Grund fehlender Erfahrungswerte niemand etwas gemerkt hat (siehe hierzu Bild 1). Eine weitere Herausforderung ist das in den von NIS-2 betroffenen Unternehmen vorhandene Systemverständnis: für die IT-Netzwerke und die IT-Systeme gibt es in der Regel firmeninterne Experten, die mit den Zusammenhängen vertraut sind. Hinsichtlich der vernetzten OT-Baugruppen und Systeme ist das in der Regel nicht immer der Fall.

Eine Firewall reicht nicht

Tabelle 1 verdeutlicht allerdings auch, dass es keine rein technische Lösung gibt, um eine NIS-2-gerechte Cybersecurity in vernetzten OT/IT-Umgebungen zu realisieren. Es ist in jedem Fall eine Managementkomponente erforderlich (die

Cybergefahren, z. B. durch Manipulation

Manipulationsart	Kurzbeschreibung
Zutritt	Durch den Austausch eines Sensors oder Aktors wird die Gesamtfunktion einer Maschinensteuerung verändert. Dadurch könnte sich die Lebensdauer bestimmter mechanischer Komponenten verringern, was letztendlich zu höheren Betriebskosten, aber auch Mehreinnahmen auf Seiten der Servicepartner führt.
Zugriff	Jede extern zugängliche Kommunikationsschnittstelle einer Maschine bzw. Anlage ist auch ein möglicher Angriffspunkt, beispielsweise für unberechtigte Nutzerzugriffe. Mit Hilfe eines solchen Zugriffs könnte ein Angreifer mit entsprechendem Expertenwissen auf die jeweilige Steuerung zugreifen und die Software verändern.
Umgebungsbedingungen	Bei der Funkkommunikation in einem lizenzfreien ISM-Band geht man davon aus, dass sich alle Sender an bestimmte Regeln halten, z. B. die Einhaltung eines Duty Cycle in einem bestimmten Frequenzband. Wird beispielsweise mit Hilfe einer preiswerten Hobby-Drohne ein 868 MHz-Störsender auf einem Hallendach platziert, ist das als Denial of Service (DoS)-Angriff auf die drahtlosen Kommunikationssysteme in der Produktionshalle zu werten.

Tabelle 2: Für die vernetzten Automatisierungslösungen eines Produktionsbetriebs existieren viele Cybergefahren, z. B. durch Manipulation. Dabei ist zu berücksichtigen, dass nicht nur externe Zugriffe auf Schnittstellen als Angriffspunkte in Frage kommen. Auch die Zutrittsmöglichkeiten für Servicetechniker sind eine potenzielle Gefahrenquelle. Darüber hinaus sind auch Funk-basierte Attacken möglich.

recht verbreitete Minimalmaßnahme „Wir segmentieren unsere Vernetzungslandschaft, kaufen ein paar Firewalls und installieren die an den neuralgischen Punkten." funktioniert hier nicht).

Praxistaugliche Strategien entwerfen

Um NIS-2 in der Praxis effektiv umzusetzen, ist eine praxistaugliche Strategie erforderlich, die sowohl IT als auch OT umfasst. In Bezug auf die OT/IT-Verbindungen kann man sich die dafür erforderliche Cybersecurity-Strategie vereinfacht als vierstufige Handlungsschleife vorstellen, also als einen Cybersecurity-Management-Prozess: In der Praxis eignet sich dafür eine „Check-Measure-Plan-Do and Document-Loop", die analog zu den Aktivitäten eines ISO 9001:2015-basierten Qualitätsmanagementsystems immer wieder durchlaufen wird, um die NIS-2-Pflichten möglichst vollständig zu erfüllen sowie die Cybersicherheit und Cyberresilienz Schritt für Schritt zu verbessern und das auch nachweisen zu können (siehe rechten Teil der Bild 2).

Prozessgrundbausteine

Die dafür erforderlichen vier elementaren Prozessgrundbausteine wären beispielsweise:

- eine Cyber-Bedrohungsanalyse für die eigene Organisation bzw. die vorhandene IT- und OT-Infrastruktur (Check),
- die Bewertung des Reifegrads der existierenden Sicherheitsmaßnahmen (Measure),
- das Erstellen einer Beschreibung bzw. eines Plans, was sich an den bestehenden Sicherheitsmaßnahmen verbessern lässt (Plan)
- die Umsetzung der Sicherheitsmaßnahmen aus dem Plan (Do) sowie die Dokumentation, aus der jeweils der aktuelle Stand der Cybersecurity-Strategie hervorgeht (Document).

Wichtig ist, dass jeder einzelne Datenfluss zwischen allen OT- und IT-Anwendungen vollständig transparent erfasst und mit allen Schnittstellen in einem Datenflussdiagramm visualisiert wird, um weitere Analysen zu ermöglichen. Diese Transparenz ist vielfach schon der entscheidende Schritt zu sicheren OT/IT-Systemlösungen.

Link

Link zur deutschsprachigen Version des EU-Amtsblatt 2022/2555: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555&qid=1693720032548 ◄

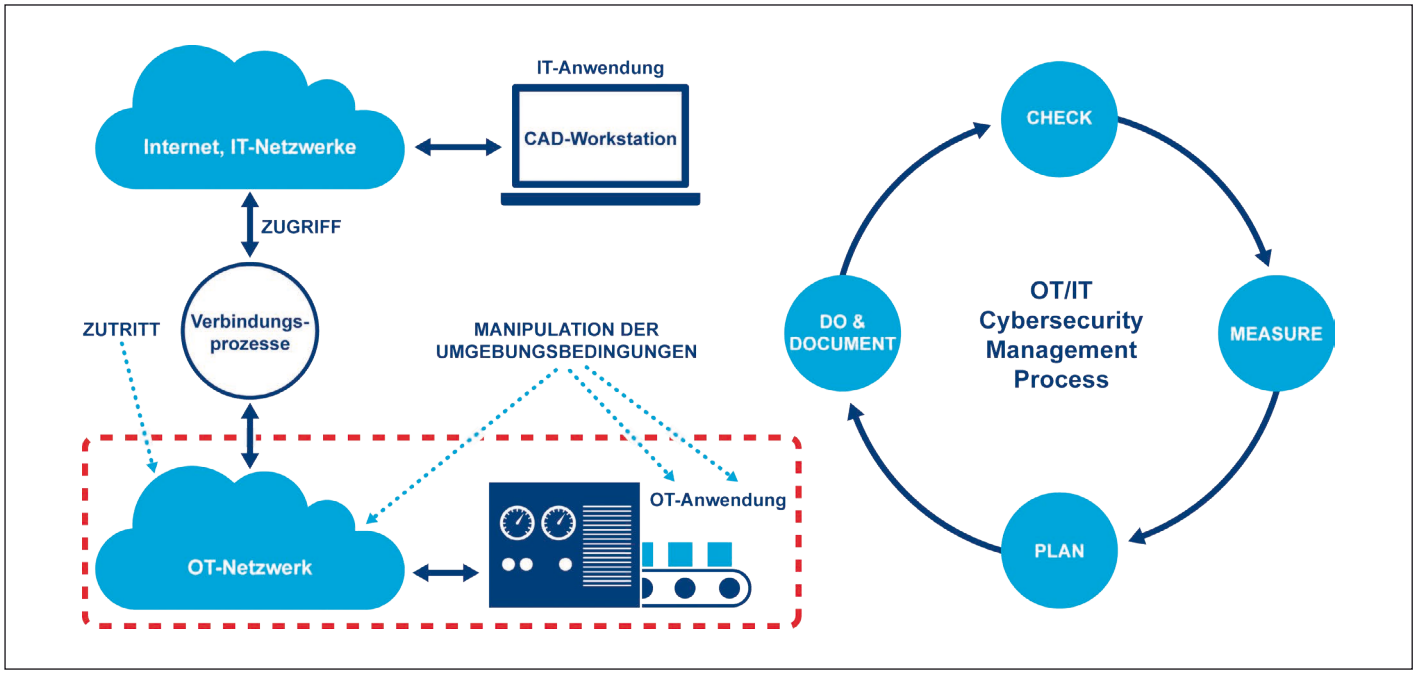

Bild 2: OT-Anwendungen bieten verschiedene Angriffsflächen. Cyberangreifer könnten sich physischen Zutritt zur Anlage verschaffen, um technische Manipulationen durchzuführen. Auch Cyberattacken per Fernwartungszugriff sind denkbar, um Anlagen zu stören. Vielfach übersehen werden die Manipulationsmöglichkeiten der Anlagenumgebung: z. B. in einem gewissen Abstand zur Anlage einen geeigneten Störsender zu platzieren, um die Funkkommunikation zu kompromittieren.