WHITEPAPER

Cobot Safety

Der Cyber Resilience Act im Maschinenbau

Anforderungen, Normen, Pflichten und praktische Umsetzung für Maschinenbauer

CYBER-SICHERHEIT

ANFORDERUNGEN & PFLICHTEN

PRODUKT-COMPLIANCE

LIEFERKETTEN-SICHERHEIT



COBOT SAFETY | Eichenflur 9, 56242 Nordhofen | info@cobot-safety.de

Praxisorientierter Leitfaden für Hersteller von Maschinen und Anlagen

Inhaltsverzeichnis

Inhaltsverzeichnis 1
1 Warum der CRA den Maschinenbau betrifft 4
2 Der Cyber Resilience Act im Überblick 5
2.1 Zielsetzung des CRA 5
2.2 Rechtliche Einordnung als EU-Verordnung 6
2.3 Verhältnis zu Maschinenverordnung und anderen Dokumenten 6
2.4 Was sich gegenüber bisherigen CE-Prozessen ändert 7
3 Termine und Übergangsfristen 8
3.1 Veröffentlichung und Inkrafttreten 9
3.2 Erste relevante Pflichten ab 11. Juni 2026 10
3.3 Meldepflichten ab 11. September 2026 10
3.4 Vollständige Anwendung ab 11. Dezember 2027 11
3.5 Übergangsregelungen für bereits in Verkehr gebrachte Produkte 12
4 Anwendungsbereich und Ausschlussbereich 13
4.1 Was ist ein „Produkt mit digitalen Elementen“? 13
4.2 Wann ist eine Maschine vom CRA betroffen? 14
4.3 Beispiele aus dem Maschinenbau 15
4.4 Komponenten, Ersatzteile und separat bereitgestellte Software 17
4.5 Remote Data Processing / Cloud-Anbindung 17
4.6 Ausnahmen und Abgrenzungen 18
4.7 Bedeutung von „wesentlicher Änderung“ und Produktänderungen nach 2027 19
5 Welche Pflichten kommen auf Maschinenbauer zu? 21
5.1 Cybersecurity Risk Assessment als neue Pflicht im CE-Prozess 21
5.2 Security by Design und Security by Default 22
5.3 Anforderungen an Entwicklung, Produktion und Wartung 23
5.4 Schwachstellenmanagement über den Supportzeitraum 24
5.5 Update- und Patch-Management 25
5.6 Meldepflichten bei aktiv ausgenutzten Schwachstellen 25
5.7 Techn. Dokumentation, EU-Konformitätserklärung und CE-Kennzeichnung 26
5.8 Benutzerinformation und Betriebsanleitung 27
5.9 Lieferantenmanagement und Software-/Komponentenverzeichnis 28
6 Harmonisierte Normen und Normungslandschaft 29
6.1 Bedeutung harmonisierter Normen und Vermutungswirkung 29

6.2 Stand der CRA-Normung 30
6.3 Bereits vorhandene Normen mit Relevanz für den Maschinenbau 31
6.4 EN IEC 62443 als Normenreihe für industrielle Automatisierung 32
6.5 EN 18031 und Abgrenzung zur Funkanlagenrichtlinie / RED 33
6.6 Welche Normen durch den CRA noch zu erwarten sind 34
6.7 Horizontale Normen vs. vertikale / produktspezifische Normen 35
6.8 Relevanz von CLC/TC 65X WG 3 für industrielle Automatisierung 36
7 Klassifizierung von Produkten nach CRA 37
7.1 Standardprodukt mit digitalen Elementen 38
7.2 Wichtige Produkte Klasse I 39
7.3 Wichtige Produkte Klasse II 40
7.4 Kritische Produkte 41
7.5 Bedeutung der Klassifizierung für die Konformitätsbewertung 42
7.6 Was ist bei Maschinen typischerweise zu erwarten? 44
8 Konformitätsbewertung und CE-Kennzeichnung 45
8.1 Interne Fertigungskontrolle / Selbstbewertung 45
8.2 Wann eine notifizierte Stelle erforderlich wird 46
8.3 Zusammenhang mit harmonisierten Normen 47
8.4 Erweiterung der technischen Dokumentation 47
8.5 Einbindung in bestehende CE-Prozesse im Maschinenbau 49
9 Was muss der Maschinenbauer praktisch beachten? 50
9.1 Frühe Einbindung der Cybersecurity in die Konstruktion 50
9.2 Festlegung der digitalen Grenzen der Maschine 51
9.3 Schnittstellenanalyse: Ethernet, WLAN, USB, Feldbus, Remote Service 52
9.4 Rollenklärung: Hersteller, Integrator, Importeur, Betreiber 53
9.5 Umgang mit Zukaufkomponenten 54
9.6 Anforderungen an Passwörter, Benutzerrollen und Zugriffsschutz 55
9.7 Logging, Backup, Wiederherstellung und sichere Konfiguration 56
9.8 Patchfähigkeit und Update-Konzept 57
9.9 Informationspflichten gegenüber dem Betreiber 57
9.10 Interne Prozesse: Schwachstellenmonitoring, Incident Handling 58
10 Schnittstelle zwischen Safety und Security 59
10.1 Warum Cybersecurity für Maschinensicherheit relevant wird 59
10.2 Manipulation sicherheitsbezogener Steuerungen 60
10.3 Fernwartung und Zugriff auf sicherheitsrelevante Parameter 61

10.4 Security als Voraussetzung für die Integrität von Safety-Funktionen 62
10.5 Risikobeurteilung nach MVO vs. Cybersecurity Risk Assessment nach CRA 63
11 Lösungsansatz am Beispiel einer einfachen Maschine 64
11.1 Beschreibung der Beispielmaschine 64
11.2 Digitale Elemente und Schnittstellen der Maschine 65
11.3 Erste CRA-Einstufung 66
11.4 Beispielhafte Cybersecurity-Risikobewertung 67
11.5 Technische Maßnahmen 68
11.6 Organisatorische Maßnahmen beim Hersteller 69
11.7 Anforderungen an die Betriebsanleitung 70
11.8 Technische Dokumentation 71
11.9 Update- und Schwachstellenprozess 72
11.10 Ergebnis: pragmatischer CRA-konformer Umgang 72
12 Marktaufsicht, Sanktionen und Umsetzungshilfen 73
12.1 Sanktionsrahmen nach Artikel 64 CRA 73
12.2 Marktüberwachung in Deutschland 74
12.3 BSI TR-03183 als Umsetzungshilfe 74
12.4 Praktische Bedeutung für Maschinenbauer 75
13 Fazit 75

1 Warum der CRA den Maschinenbau betrifft

Der Maschinenbau befindet sich seit Jahren in einem tiefgreifenden Wandel. Maschinen und Anlagen bestehen längst nicht mehr nur aus mechanischen, elektrischen und steuerungstechnischen Komponenten. Moderne Maschinen verfügen über SPS-Steuerungen, HMI-Systeme, Industrie-PCs, Frequenzumrichter, Robotersteuerungen, Netzwerkschnittstellen, USB-Ports, Fernwartungszugänge, Softwarefunktionen, Firmware, Cloud-Anbindungen oder digitale Servicefunktionen. Damit entstehen nicht nur neue Möglichkeiten für Diagnose, Wartung, Produktivität und Vernetzung, sondern auch neue Angriffsflächen für Cyberangriffe.

Mit dem Cyber Resilience Act, kurz CRA, schafft die Europäische Union erstmals einen horizontalen Rechtsrahmen für die Cybersicherheit von Hardware- und Softwareprodukten mit digitalen Elementen. Die Verordnung gilt nicht nur für klassische IT-Produkte, sondern grundsätzlich auch für Produkte, die im Maschinenbau eine digitale Funktion oder eine direkte bzw. indirekte Datenverbindung zu anderen Geräten oder Netzwerken besitzen. Die EU-Kommission beschreibt den CRA als Regelwerk für Hardware- und Softwareprodukte, die als „Produkte mit digitalen Elementen“ auf dem Unionsmarkt bereitgestellt werden; dazu gehören sowohl Endprodukte als auch separat in Verkehr gebrachte Komponenten.

Für Maschinenbauer bedeutet dies: Cybersecurity wird künftig zu einem festen Bestandteil des CE-Prozesses. Neben der klassischen Maschinensicherheit, der Risikobeurteilung nach Maschinenverordnung und EN ISO 12100 sowie der funktionalen Sicherheit nach z. B. EN ISO 13849-1 müssen Hersteller künftig auch die Cyberresilienz ihrer Produkte systematisch betrachten, bewerten, dokumentieren und über einen definierten Supportzeitraum aufrechterhalten.

Der CRA verfolgt dabei zwei zentrale Ziele. Zum einen sollen Produkte bereits bei ihrer Entwicklung, Konstruktion und Herstellung ein angemessenes Cybersicherheitsniveau aufweisen. Zum anderen sollen Hersteller während der erwarteten Nutzungsdauer des Produkts wirksame Prozesse für den Umgang mit Schwachstellen, Sicherheitsupdates und sicherheitsrelevanten Vorfällen etablieren. Die Pflichten betreffen damit nicht nur den Zeitpunkt des Inverkehrbringens, sondern auch die Zeit nach der Auslieferung.

Gerade im Maschinenbau ist diese Entwicklung besonders relevant. Wird beispielsweise über einen Fernwartungszugang auf eine Maschine zugegriffen, werden sicherheitsrelevante Parameter über Software konfiguriert, kommuniziert eine Steuerung mit einem übergeordneten Netzwerk oder werden Updates für HMI, SPS, Robotersteuerung oder Industrie-PC bereitgestellt, kann Cybersecurity unmittelbar Einfluss auf die sichere Funktion der Maschine haben. Safety und Security lassen sich daher zunehmend nicht mehr vollständig getrennt betrachten.

Dieses Whitepaper gibt einen praxisnahen Überblick darüber, was der Cyber Resilience Act für Maschinenbauer bedeutet. Es erläutert die wichtigsten Termine, den Anwendungs- und Ausschlussbereich, die derzeit absehbare Normungssituation, die neuen Pflichten für Hersteller sowie konkrete Lösungsansätze für den konformen Umgang mit dem CRA. Abschließend wird anhand einer einfachen Maschine gezeigt, wie Maschinenbauer das Thema strukturiert in ihre bestehenden CE- und Entwicklungsprozesse integrieren können.

2 Der Cyber Resilience Act im Überblick

Der Cyber Resilience Act, kurz CRA, ist eine europäische Verordnung zur Festlegung horizontaler Cybersicherheitsanforderungen an Produkte mit digitalen Elementen. Er richtet sich damit nicht nur an klassische IT-Produkte wie Software, Apps, Router oder Betriebssysteme, sondern grundsätzlich auch an Hardware- und Softwareprodukte, die in anderen Branchen eingesetzt werden. Für den Maschinenbau ist dies besonders relevant, weil moderne Maschinen zunehmend digitale Komponenten, Netzwerkschnittstellen, Fernwartungszugänge, Softwarefunktionen und updatefähige Steuerungssysteme enthalten.

Der CRA ist Teil einer umfassenderen europäischen Cybersecurity-Strategie. Während frühere Regelungen häufig bestimmte Branchen, Betreiber kritischer Infrastrukturen oder einzelne Produktgruppen adressiert, verfolgt der CRA einen horizontalen Produktansatz. Im Mittelpunkt steht nicht der Betreiber einer Anlage, sondern das Produkt selbst und damit der Hersteller, der dieses Produkt auf dem europäischen Markt bereitstellt.

Für Maschinenbauer bedeutet dies, dass Cybersecurity künftig nicht mehr nur als IT-Thema des Betreibers verstanden wird. Sobald eine Maschine digitale Elemente enthält und eine direkte oder indirekte Datenverbindung zu anderen Geräten oder Netzwerken vorgesehen oder vernünftigerweise vorhersehbar ist, muss der Hersteller prüfen, ob und in welchem Umfang der CRA anzuwenden ist.

2.1 Zielsetzung des CRA

Ziel des Cyber Resilience Act ist es, das Cybersicherheitsniveau von Produkten mit digitalen Elementen innerhalb der Europäischen Union zu erhöhen. Produkte sollen so entwickelt, hergestellt, ausgeliefert und über ihren vorgesehenen Nutzungszeitraum betreut werden, dass Cyberrisiken angemessen reduziert werden.

Der CRA verfolgt dabei im Wesentlichen zwei Grundgedanken. Erstens sollen Produkte bereits zum Zeitpunkt des Inverkehrbringens ein angemessenes Sicherheitsniveau aufweisen. Cybersecurity soll also nicht erst nachträglich durch Patches, Zusatzsoftware oder Betreibermaßnahmen hergestellt werden, sondern von Beginn an in Planung, Entwicklung, Konstruktion, Herstellung und Auslieferung berücksichtigt werden. Dies entspricht dem Prinzip „Security by Design“ und „Security by Default“.

Zweitens soll der Hersteller auch nach dem Inverkehrbringen Verantwortung für sein Produkt übernehmen. Dazu gehört insbesondere der Umgang mit Schwachstellen, die Bereitstellung von Sicherheitsupdates, die Information der Nutzer sowie die Meldung aktiv ausgenutzter Schwachstellen und schwerwiegender Sicherheitsvorfälle. Der CRA betrachtet Cybersecurity damit nicht nur als Produkteigenschaft zum Zeitpunkt der CE-Kennzeichnung, sondern als Lebenszyklusanforderung.

Für den Maschinenbau ist dieser Ansatz neu, aber in seiner Logik nicht völlig fremd. Auch bei der Maschinensicherheit reicht es nicht aus, nur eine technische Einzelmaßnahme vorzusehen. Vielmehr müssen Gefährdungen systematisch ermittelt, Risiken bewertet, geeignete Maßnahmen umgesetzt und Restrisiken dokumentiert werden. Der CRA überträgt eine vergleichbare Denkweise auf Cyberrisiken: Der Hersteller muss Cybersecurity systematisch analysieren, bewerten, technisch und organisatorisch behandeln und nachvollziehbar dokumentieren.

2.2 Rechtliche Einordnung als EU-Verordnung

Der Cyber Resilience Act ist eine EU-Verordnung. Anders als eine Richtlinie muss eine Verordnung nicht erst in nationales Recht umgesetzt werden, sondern gilt unmittelbar in allen Mitgliedstaaten der Europäischen Union. Damit entsteht ein einheitlicher Rechtsrahmen für Produkte mit digitalen Elementen auf dem europäischen Binnenmarkt.

Rechtlich ist der CRA dem europäischen Produktsicherheits- und Marktzugangsrecht zuzuordnen. Er legt Anforderungen fest, die erfüllt sein müssen, damit ein Produkt mit digitalen Elementen auf dem europäischen Markt bereitgestellt werden darf. Damit steht der CRA in einer ähnlichen Systematik wie andere europäische Harmonisierungsrechtsvorschriften, etwa die Maschinenverordnung, die Niederspannungsrichtlinie, die EMV-Richtlinie oder die Funkanlagenrichtlinie.

Für Hersteller ist besonders wichtig, dass der CRA in den CE-Konformitätsprozess eingebunden ist. Für Produkte im Anwendungsbereich des CRA müssen die einschlägigen Anforderungen bewertet und erfüllt werden. Nach erfolgreicher Konformitätsbewertung wird die EU-Konformitätserklärung erstellt und die CE-Kennzeichnung angebracht. Für Maschinenbauer bedeutet dies: Der CRA kann künftig ein zusätzlicher Rechtsakt sein, der in der EU-Konformitätserklärung berücksichtigt werden muss.

Der CRA erweitert damit nicht nur die technische Betrachtung, sondern auch die rechtliche Verantwortung des Herstellers. Cybersecurity wird zu einer produktbezogenen Konformitätsanforderung. Die Frage lautet künftig nicht mehr nur, ob eine Maschine mechanisch, elektrisch und funktional sicher ist, sondern auch, ob ihre digitalen Elemente angemessen gegen Cyberrisiken ausgelegt, dokumentiert und über den vorgesehenen Supportzeitraum betreut werden.

2.3 Verhältnis zu Maschinenverordnung und anderen Dokumenten

Der CRA steht nicht isoliert, sondern ergänzt bestehende europäische Rechtsakte und Normen. Für den Maschinenbau ist vor allem das Zusammenspiel mit der Maschinenverordnung, der Funkanlagenrichtlinie, der NIS2-Richtlinie, dem Cybersecurity Act und der IEC-/EN-Normung relevant.

Die Maschinenverordnung betrachtet Cybersecurity vor allem dort, wo eine Manipulation, Beschädigung oder unbeabsichtigte Veränderung digitaler Systeme zu einer sicherheitsrelevanten Gefährdung führen kann. Im Mittelpunkt steht also der Schutz von Menschen vor Gefährdungen, die durch die Maschine entstehen können. Cybersecurity ist in diesem Zusammenhang vor allem dann relevant, wenn sie Einfluss auf die Sicherheit der Maschine hat, zum Beispiel bei sicherheitsbezogenen Steuerungsfunktionen, Parametrierungen, Fernzugriffen oder Softwareänderungen.

Der CRA geht darüber hinaus. Er betrachtet nicht nur Cyberangriffe, die unmittelbar zu einer Personengefährdung führen können, sondern die Cyberresilienz des Produkts mit digitalen Elementen insgesamt. Dazu gehören beispielsweise sichere Standardkonfigurationen, Zugriffsschutz, Schutz vor unbefugter Manipulation, Schwachstellenmanagement, Sicherheitsupdates, technische Dokumentation und Informationen für den Nutzer. Während die Maschinenverordnung also primär auf Safety abzielt, adressiert der CRA die produktbezogene Security.

Die Funkanlagenrichtlinie, kurz RED, ist insbesondere dann relevant, wenn Maschinen oder Maschinenkomponenten Funktechnologien enthalten, zum Beispiel WLAN, Bluetooth, Mobilfunk oder andere Funkmodule. Für bestimmte Funkanlagen wurden bereits zusätzliche Cybersicherheitsanforderungen akti-

viert. In solchen Fällen muss der Maschinenbauer prüfen, ob neben der Maschinenverordnung und dem CRA auch RED-Anforderungen zu berücksichtigen sind. Praktisch betrifft dies zum Beispiel Fernwartungsrouter, Funkmodule, drahtlose Bedieneinheiten oder andere kommunikationsfähige Komponenten.

Die NIS2-Richtlinie verfolgt einen anderen Ansatz. Sie richtet sich in erster Linie an bestimmte Einrichtungen und Betreiber, insbesondere in kritischen oder wichtigen Sektoren. Während der CRA produktbezogene Anforderungen an Hersteller stellt, adressiert NIS2 organisatorische Cybersicherheitsanforderungen an Unternehmen und Betreiber. Für Maschinenbauer kann NIS2 dennoch indirekt relevant werden, etwa wenn Kunden aus regulierten Sektoren zusätzliche Anforderungen an Maschinen, Komponenten, Fernwartung, Lieferkette oder Schwachstellenmanagement stellen.

Der Cybersecurity Act bildet den europäischen Rahmen für Cybersicherheitszertifizierungen. Er schafft die Grundlage für europäische Zertifizierungsschemata, mit denen die Cybersicherheit bestimmter Produkte, Dienste oder Prozesse nachgewiesen werden kann. Im Kontext des CRA können solche Zertifizierungsschemata künftig eine Rolle spielen, wenn sie zur Konformitätsbewertung oder als zusätzlicher Nachweis der Cybersicherheit herangezogen werden.

IEC- und EN-Normen werden für die praktische Umsetzung des CRA eine zentrale Rolle spielen. Wie bei anderen CE-Rechtsakten können harmonisierte Normen eine Vermutungswirkung auslösen. Das bedeutet: Werden die einschlägigen harmonisierten Normen korrekt angewendet, kann der Hersteller davon ausgehen, dass die darin abgedeckten Anforderungen des CRA erfüllt sind. Für den Maschinenbau sind insbesondere Normen aus dem Bereich der industriellen Automatisierung und Steuerungstechnik relevant, vor allem die Normenreihe IEC 62443 bzw. deren europäische Übernahmen. Zusätzlich ist mit weiteren horizontalen und produktspezifischen Normen zu rechnen, die speziell zur Unterstützung des CRA erarbeitet werden.

Für Maschinenbauer ergibt sich daraus eine wichtige Konsequenz: Die Cybersecurity-Betrachtung darf nicht isoliert neben der CE-Bewertung stehen. Sie muss mit Maschinenverordnung, funktionaler Sicherheit, elektrischer Ausrüstung, Steuerungstechnik, Software, Fernwartung und Dokumentation verknüpft werden. In der Praxis wird es daher darauf ankommen, einen integrierten Prozess zu schaffen, der Safety und Security gemeinsam betrachtet, ohne die unterschiedlichen Zielrichtungen der Rechtsakte zu vermischen.

2.4 Was sich gegenüber bisherigen CE-Prozessen ändert

Für viele Maschinenbauer bestand der klassische CE-Prozess bisher vor allem aus der Klärung des Anwendungsbereichs, der Risikobeurteilung, der Auswahl und Umsetzung von Schutzmaßnahmen, der Validierung sicherheitsbezogener Funktionen, der technischen Dokumentation, der Betriebsanleitung und der EU-Konformitätserklärung. Cybersecurity wurde dabei häufig nur am Rand betrachtet, zum Beispiel bei Fernwartung, Netzwerkzugängen oder der Parametrierung sicherheitsbezogener Steuerungen.

Mit dem CRA wird Cybersecurity zu einem verbindlichen Bestandteil der Produktkonformität. Der Hersteller muss systematisch prüfen, welche digitalen Elemente sein Produkt enthält, welche Schnittstellen vorhanden sind, welche Cyberrisiken sich daraus ergeben und welche Maßnahmen erforderlich sind. Diese Betrachtung muss dokumentiert und in die technische Dokumentation aufgenommen werden.

Neu ist insbesondere, dass der Hersteller nicht nur den Zustand des Produkts zum Zeitpunkt der Auslieferung betrachten darf. Er muss auch festlegen, wie lange das Produkt unterstützt wird, wie mit Schwachstellen umgegangen wird, wie Sicherheitsupdates bereitgestellt werden und wie Nutzer über relevante Risiken, Maßnahmen und Supportzeiträume informiert werden. Damit verschiebt sich der CE-Prozess teilweise von einer einmaligen Produktprüfung hin zu einem lebenszyklusorientierten Compliance-Prozess.

Für Maschinenbauer ergeben sich dadurch zusätzliche Aufgabenbereiche. Dazu gehören unter anderem die Ermittlung und Dokumentation digitaler Elemente, die Bewertung von Cyberrisiken, die Absicherung von Schnittstellen, die Verwaltung von Software- und Firmwareständen, der Umgang mit Drittkomponenten, die Festlegung eines Update- und Patchkonzepts, ein Verfahren zum Schwachstellenmanagement sowie eine angepasste Benutzerinformation.

Auch die Lieferkette wird an Bedeutung gewinnen. Maschinenhersteller verwenden häufig zugekaufte Steuerungen, HMI-Systeme, Robotersteuerungen, Frequenzumrichter, Remote-Service-Router, Kamerasysteme, Sensoren oder Softwarebibliotheken. Der CRA führt dazu, dass der Hersteller stärker prüfen muss, ob solche Komponenten die Cybersicherheit der Gesamtmaschine beeinträchtigen können und welche Informationen vom Lieferanten benötigt werden. Dies betrifft zum Beispiel Dokumentation, Sicherheitsupdates, bekannte Schwachstellen, Supportzeiträume und sichere Konfigurationsmöglichkeiten.

Gleichzeitig sollte der CRA nicht als völlig neuer, losgelöster Prozess verstanden werden. Maschinenbauer können viele bestehende Strukturen nutzen: Risikobeurteilung, Anforderungsmanagement, Lieferantenbewertung, technische Dokumentation, Validierung, Änderungsmanagement und Betriebsanleitung sind bereits etablierte Bestandteile des CE-Prozesses. Der entscheidende Schritt besteht darin, diese Strukturen um Cybersecurity-Aspekte zu erweitern und systematisch miteinander zu verknüpfen.

Der CRA verändert den CE-Prozess damit nicht in seinem Grundprinzip, wohl aber in seinem Inhalt und in seiner zeitlichen Reichweite. Aus der Frage „Ist die Maschine zum Zeitpunkt des Inverkehrbringens sicher?“ wird zusätzlich die Frage: „Ist die Maschine als Produkt mit digitalen Elementen angemessen cyberresilient, dokumentiert, updatefähig und über den vorgesehenen Supportzeitraum betreut?“

3 Termine und Übergangsfristen

Der Cyber Resilience Act enthält keine sofortige Vollanwendung aller Anforderungen, sondern sieht eine gestufte Anwendung mit mehreren Übergangsfristen vor. Für Maschinenbauer ist diese zeitliche Staffelung besonders wichtig, weil Entwicklungszyklen, Lieferantenqualifikation, Steuerungsarchitektur, Softwarepflege, technische Dokumentation und CE-Prozesse in der Regel nicht kurzfristig angepasst werden können.

Die wesentlichen Stichtage sind:

- Veröffentlichung im Amtsblatt der Europäischen Union: 20. November 2024
- Inkrafttreten: 10. Dezember 2024
- Anwendung der Vorschriften zur Notifizierung von Konformitätsbewertungsstellen: 11. Juni 2026
- Anwendung der Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle: 11. September 2026
- Vollständige Anwendung der Hauptpflichten des CRA: 11. Dezember 2027

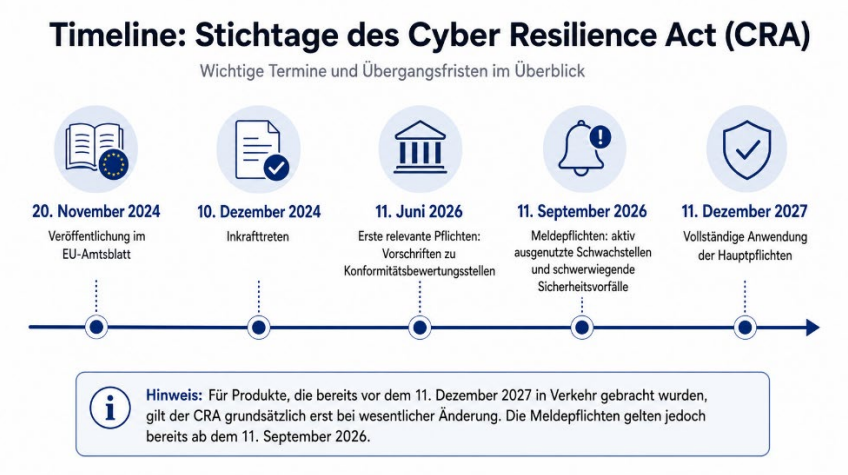


Abb. 1: Stichtage des Cyber Resilience Act

Damit steht Herstellern zwar grundsätzlich eine mehrjährige Übergangszeit zur Verfügung. Diese sollte jedoch nicht als Wartezeit verstanden werden. Gerade im Maschinenbau müssen viele Anforderungen bereits deutlich vor dem 11. Dezember 2027 vorbereitet werden, damit neue Maschinen, Steuerungssysteme und digitale Komponenten ab diesem Zeitpunkt CRA-konform in Verkehr gebracht werden können.

3.1 Veröffentlichung und Inkrafttreten

Der Cyber Resilience Act wurde als Verordnung (EU) 2024/2847 im Amtsblatt der Europäischen Union veröffentlicht. Die Verordnung ist am 10. Dezember 2024 in Kraft getreten. Da es sich um eine EU-Verordnung handelt, gilt sie unmittelbar in allen Mitgliedstaaten und muss nicht erst durch nationale Gesetze umgesetzt werden.

Das Inkrafttreten bedeutet jedoch noch nicht, dass sämtliche materiellen Anforderungen sofort anzuwenden sind. Vielmehr beginnt mit dem Inkrafttreten die Übergangsphase. In dieser Zeit können Hersteller, Importeure, Händler, Konformitätsbewertungsstellen, Marktüberwachungsbehörden und Normungsorganisationen die notwendigen Voraussetzungen für die spätere Anwendung schaffen.

Für Maschinenbauer beginnt damit die strategische Vorbereitungsphase. In dieser Phase sollte insbesondere geprüft werden, welche Maschinen und Komponenten künftig unter den CRA fallen können, welche digitalen Elemente vorhanden sind, welche Schnittstellen bestehen und welche internen Prozesse für Cybersecurity, Schwachstellenmanagement, Updates und technische Dokumentation aufgebaut oder erweitert werden müssen.

Praktisch ist es sinnvoll, den CRA bereits bei neuen Entwicklungsprojekten zu berücksichtigen. Eine Maschine, die heute entwickelt wird, kann aufgrund typischer Entwicklungs-, Projektierungs- und Lieferzeiten erst nach dem 11. Dezember 2027 in Verkehr gebracht werden. Wird der CRA erst am Ende des Projekts betrachtet, können nachträgliche Änderungen an Steuerungsarchitektur, Software, Zugriffskonzept, Updatefähigkeit oder Dokumentation erforderlich werden.

3.2 Erste relevante Pflichten ab 11. Juni 2026

Ab dem 11. Juni 2026 gelten die Vorschriften des CRA zur Notifizierung von Konformitätsbewertungsstellen. Dieser Termin betrifft zunächst vor allem die Mitgliedstaaten, notifizierenden Behörden und Konformitätsbewertungsstellen. Die Mitgliedstaaten müssen die organisatorischen Voraussetzungen dafür schaffen, dass geeignete Stellen benannt und notifiziert werden können.

Für Maschinenbauer entsteht daraus nicht automatisch für jede Maschine eine unmittelbare Prüfpflicht durch eine externe Stelle. Der Termin ist dennoch wichtig, weil er die Infrastruktur für spätere Konformitätsbewertungen vorbereitet. Bestimmte Produkte mit digitalen Elementen können je nach Einstufung als wichtige oder kritische Produkte strengeren Konformitätsbewertungsverfahren unterliegen. In solchen Fällen kann eine notifizierte Stelle erforderlich werden.

Für Hersteller bedeutet dies: Spätestens ab diesem Zeitpunkt sollte geprüft werden, ob eigene Produkte möglicherweise in eine Kategorie fallen, bei der eine externe Konformitätsbewertung erforderlich werden kann. Dies betrifft im Maschinenbau insbesondere digitale Komponenten oder Systeme, deren Kernfunktion einer im CRA besonders geregelten Produktkategorie entspricht. Auch wenn eine typische Maschine nicht automatisch eine Drittprüfung auslöst, können einzelne digitale Komponenten, Steuerungssysteme oder Softwarebestandteile gesondert relevant sein.

Der 11. Juni 2026 ist daher vor allem als organisatorischer Meilenstein zu verstehen. Die Behörden- und Prüfstellenstruktur für den CRA entsteht. Für Maschinenbauer ist dies ein Signal, die eigene Produktklassifizierung, die Lieferanteninformationen und die geplanten Konformitätsbewertungswege rechtzeitig vorzubereiten.

3.3 Meldepflichten ab 11. September 2026

Ab dem 11. September 2026 gelten die Meldepflichten nach Artikel 14 CRA. Hersteller müssen ab diesem Zeitpunkt aktiv ausgenutzte Schwachstellen sowie schwerwiegende Sicherheitsvorfälle, die Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen haben, melden.

Diese Pflicht ist für Maschinenbauer besonders bedeutsam, weil sie nicht erst mit der vollständigen Anwendung des CRA am 11. Dezember 2027 beginnt. Die Meldepflichten gelten auch für Produkte mit digitalen Elementen, die bereits vor dem 11. Dezember 2027 auf dem Unionsmarkt bereitgestellt bzw. in Verkehr gebracht wurden, sofern diese Produkte grundsätzlich in den Anwendungsbereich des CRA fallen.

Hersteller müssen daher bereits vor der Vollanwendung des CRA über geeignete Prozesse verfügen, um Schwachstellen und Sicherheitsvorfälle erkennen, bewerten, intern zuordnen und fristgerecht melden zu können. Dazu gehören insbesondere:

- ein Verfahren zur Entgegennahme von Schwachstellenmeldungen,
- eine interne Bewertung, ob eine Schwachstelle aktiv ausgenutzt wird,
- eine Bewertung, ob ein schwerwiegender Sicherheitsvorfall vorliegt,
- Zuständigkeiten für die Meldung an die zuständigen Stellen,
- eine technische und organisatorische Dokumentation der Bewertung,
- ein Prozess zur Bereitstellung von Korrektur- oder Minderungsmaßnahmen.

Die Meldepflichten sind zeitkritisch. Der CRA sieht unter anderem eine frühe Warnmeldung innerhalb von 24 Stunden sowie eine Hauptmeldung innerhalb von 72 Stunden vor. Je nach Fall sind anschließend

Abschlussberichte innerhalb der vorgesehenen Fristen erforderlich. Diese Fristen zeigen deutlich, dass ein rein reaktiver Umgang mit Cybersecurity nicht ausreicht. Hersteller benötigen vorab definierte Verantwortlichkeiten, Kommunikationswege und Entscheidungsprozesse.

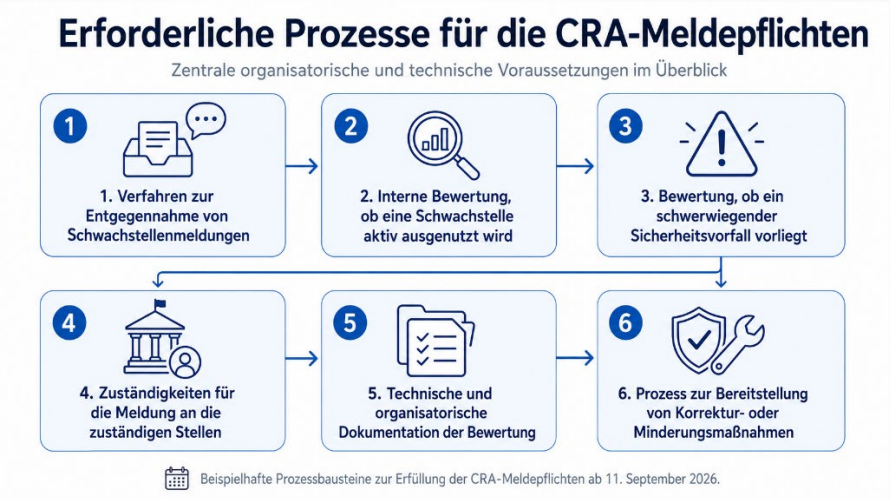


Abb. 2: CRA Meldepflicht - Zu etablierende Prozess

Für Maschinenbauer bedeutet dies praktisch: Auch wenn die vollständigen Produktanforderungen erst Ende 2027 gelten, muss der Prozess für Schwachstellen- und Vorfallmeldungen bereits deutlich früher funktionsfähig sein. Dies betrifft nicht nur neue Produkte, sondern auch bereits ausgelieferte Maschinen mit digitalen Elementen, soweit sie in den Anwendungsbereich des CRA fallen.

3.4 Vollständige Anwendung ab 11. Dezember 2027

Ab dem 11. Dezember 2027 gelten die Hauptpflichten des CRA vollständig. Ab diesem Zeitpunkt dürfen Produkte mit digitalen Elementen, die in den Anwendungsbereich des CRA fallen, grundsätzlich nur noch in Verkehr gebracht werden, wenn sie die einschlägigen Anforderungen des CRA erfüllen.



Abb. 3: Stichtag 11. Dezember 2027

Für Maschinenbauer bedeutet dies insbesondere, dass neue Maschinen mit digitalen Elementen ab diesem Stichtag nur noch dann auf dem europäischen Markt bereitgestellt werden dürfen, wenn die Cybersecurity-Anforderungen in Entwicklung, Konstruktion, Herstellung, Auslieferung und Dokumentation berücksichtigt wurden. Dazu gehören insbesondere die wesentlichen Cybersicherheitsanforderungen, die Cybersecurity-Risikobewertung, die technische Dokumentation, die Konformitätsbewertung, die Benutzerinformationen, die Festlegung des Supportzeitraums sowie die Anforderungen an Schwachstellenbehandlung und Sicherheitsupdates.

Der CRA wird damit ab dem 11. Dezember 2027 zu einem relevanten Bestandteil des CE-Prozesses. Für Produkte im Anwendungsbereich des CRA muss der Hersteller nachweisen können, dass die Anforderungen erfüllt wurden. Die EU-Konformitätserklärung und die technische Dokumentation müssen entsprechend angepasst werden. Die CE-Kennzeichnung steht dann nicht nur für die Einhaltung klassischer Produktsicherheitsanforderungen, sondern bei anwendbarem CRA auch für die Einhaltung der produktbezogenen Cybersecurity-Anforderungen.

Für Maschinenbauer ist entscheidend, dass der Stichtag an das Inverkehrbringen anknüpft. Maßgeblich ist also nicht allein, wann eine Maschine konstruiert oder gebaut wurde, sondern wann das konkrete Produkt erstmals auf dem Unionsmarkt bereitgestellt wird. Eine Maschine, die nach dem 11. Dezember 2027 neu in Verkehr gebracht wird, muss die dann geltenden Anforderungen erfüllen, sofern sie in den Anwendungsbereich des CRA fällt.

Deshalb sollten Maschinenbauer nicht bis Ende 2027 warten. Neue Projekte, Plattformen und Maschinenkonzepte sollten bereits jetzt so geplant werden, dass sie die Anforderungen des CRA erfüllen können. Dies betrifft insbesondere Steuerungskonzepte, Remote-Zugänge, Rollen- und Rechtekonzepte, Updatefähigkeit, sichere Standardkonfigurationen, Lieferantenanforderungen und die technische Dokumentation.

3.5 Übergangsregelungen für bereits in Verkehr gebrachte Produkte

Für Produkte mit digitalen Elementen, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden, enthält der CRA eine wichtige Übergangsregelung. Solche Produkte unterliegen den Anforderungen des CRA grundsätzlich nur dann, wenn sie ab dem 11. Dezember 2027 einer wesentlichen Änderung unterzogen werden.

Diese Regelung ist für den Maschinenbau von erheblicher praktischer Bedeutung. Bereits ausgelieferte Maschinen müssen also nicht allein aufgrund des Stichtags vollständig nachträglich an sämtliche CRA-Anforderungen angepasst werden. Wird eine Maschine jedoch nach dem 11. Dezember 2027 wesentlich geändert, kann der CRA wieder relevant werden. Dies kann zum Beispiel der Fall sein, wenn digitale Funktionen, Schnittstellen, Fernzugänge, Softwarearchitektur oder der bestimmungsgemäße Verwendungszweck so verändert werden, dass sich die Cyberrisiken wesentlich ändern.

Unabhängig davon gelten die Meldepflichten nach Artikel 14 CRA auch für Produkte mit digitalen Elementen, die bereits vor dem 11. Dezember 2027 in Verkehr gebracht wurden, sofern diese Produkte in den Anwendungsbereich des CRA fallen. Für Hersteller bedeutet dies, dass sie auch für Bestandsprodukte Prozesse benötigen, um aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle behandeln und melden zu können.

Wichtig ist außerdem die Unterscheidung zwischen einer bereits in Verkehr gebrachten einzelnen Maschine und später neu in Verkehr gebrachten Maschinen desselben Typs. Die Übergangsregelung schützt nicht automatisch eine ganze Baureihe oder Produktfamilie für die Zukunft. Entscheidend ist das konkrete Inverkehrbringen des jeweiligen Produkts. Wird eine Maschine desselben Typs nach dem 11. Dezember 2027 neu auf dem Markt bereitgestellt, muss sie die Anforderungen des CRA erfüllen, sofern sie in den Anwendungsbereich fällt.

Für Maschinenbauer ergibt sich daraus eine klare Handlungsempfehlung: Bestandsprodukte sollten daraufhin überprüft werden, ob sie ab dem 11. September 2026 von den Meldepflichten betroffen sein können. Parallel sollten neue Produkte, Produktplattformen und Maschinenvarianten so entwickelt werden, dass sie ab dem 11. Dezember 2027 CRA-konform in Verkehr gebracht werden können. Bei Änderungen an bereits ausgelieferten Maschinen ist künftig sorgfältig zu prüfen und zu dokumentieren, ob eine wesentliche Änderung im Sinne des CRA vorliegt.

4 Anwendungsbereich und Ausschlussbereich

Die zentrale Frage für Maschinenbauer lautet nicht: „Ist der Cyber Resilience Act ein IT-Gesetz?“ Die entscheidende Frage lautet vielmehr: „Bringt der Maschinenhersteller ein Produkt mit digitalen Elementen auf den Markt, dessen bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte Datenverbindung zu einem Gerät oder Netzwerk umfasst?“

Damit ist der Anwendungsbereich des CRA deutlich weiter, als es auf den ersten Blick erscheinen mag. Der CRA betrifft nicht nur klassische IT-Produkte wie Router, Software, Betriebssysteme oder Apps. Auch Maschinen, Anlagen, Steuerungen, Bedienterminals, Robotersteuerungen , Fernwartungsmodule, Softwarekomponenten etc. können betroffen sein, wenn sie die Voraussetzungen des CRA erfüllen.

Für den Maschinenbau ist daher eine sorgfältige Abgrenzung erforderlich. Nicht jede Maschine fällt automatisch unter den CRA. Eine rein mechanische Maschine ohne digitale Elemente und ohne Datenverbindung wird in der Regel nicht vom CRA erfasst. Moderne Maschinen enthalten jedoch häufig elektronische Informationssysteme, Software, Firmware, Netzwerkschnittstellen oder Fernzugänge. In solchen Fällen muss der Hersteller prüfen, ob die Maschine oder einzelne digitale Komponenten in den Anwendungsbereich des CRA fallen.

4.1 Was ist ein „Produkt mit digitalen Elementen“?

Der CRA verwendet den Begriff „Produkt mit digitalen Elementen“. Darunter fallen Software- oder Hardwareprodukte einschließlich ihrer Lösungen zur entfernten Datenverarbeitung. Ebenfalls erfasst sein können Software- oder Hardwarekomponenten, die separat auf dem Markt bereitgestellt werden.

Für den Maschinenbau bedeutet dies: Es geht nicht nur um klassische IT-Produkte. Auch elektronische und softwarebasierte Bestandteile einer Maschine können digitale Elemente sein. Dazu gehören beispielsweise Steuerungen, Bediengeräte, Industrie-PCs, Firmware, Kommunikationsmodule, Sensorik mit Datenverarbeitung, digitale Antriebstechnik oder separat bereitgestellte Maschinen-Software.

Wichtig ist außerdem, dass der CRA nicht nur das physische Produkt betrachtet. Auch eine zugehörige entfernte Datenverarbeitung kann Teil des Produkts mit digitalen Elementen sein, wenn sie vom Hersteller

entwickelt wurde oder unter dessen Verantwortung entwickelt wurde und wenn das Produkt ohne diese entfernte Datenverarbeitung eine seiner Funktionen nicht erfüllen könnte.

Der Begriff ist damit sehr weit. Eine Maschine kann als Gesamtprodukt ein Produkt mit digitalen Elementen sein, wenn sie digitale Hardware oder Software enthält und die weiteren Voraussetzungen des CRA erfüllt. Gleichzeitig können auch einzelne Komponenten innerhalb oder außerhalb der Maschine eigenständig als Produkte mit digitalen Elementen betrachtet werden, wenn sie separat auf dem Markt bereitgestellt werden.

4.2 Wann ist eine Maschine vom CRA betroffen?

Eine Maschine ist nicht allein deshalb vom CRA betroffen, weil sie elektrisch betrieben wird oder eine Steuerung enthält. Entscheidend ist, ob sie als Produkt mit digitalen Elementen auf dem Markt bereitgestellt wird und ob ihre bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netzwerk umfasst.

Eine Datenverbindung kann physisch sein, zum Beispiel über Ethernet, USB, serielle Schnittstellen, Feldbusse, WLAN, Bluetooth, Mobilfunk oder andere Funkverbindungen. Sie kann aber auch logisch sein, also über eine Software-Schnittstelle, ein Kommunikationsprotokoll, eine API oder eine sonstige virtuelle Verbindung erfolgen.

Für Maschinenbauer ist dabei besonders wichtig, dass nicht nur die ausdrücklich bestimmungsgemäße Nutzung zählt. Auch eine vernünftigerweise vorhersehbare Verwendung ist zu berücksichtigen. Wird eine Maschine beispielsweise mit einer Netzwerkschnittstelle, einem HMI mit Ethernet-Port, einem USB-Servicezugang oder einer vorgesehenen Fernwartung ausgeliefert, kann eine Datenverbindung regelmäßig nicht als rein theoretisch betrachtet werden.

Typische Fälle, in denen eine Maschine vom CRA betroffen sein kann, sind zum Beispiel:

- eine Maschine mit SPS und Ethernet-Schnittstelle,
- eine Maschine mit HMI und Benutzerverwaltung,
- eine Maschine mit Industrie-PC,
- eine Maschine mit Fernwartungszugang,
- eine Maschine mit Cloud-Anbindung für Monitoring oder Diagnose,
- eine Maschine mit updatefähiger Firmware oder Software,
- eine Anlage, die über OPC UA, MQTT, Profinet, EtherNet/IP o.ä. kommuniziert,
- eine Maschine mit WLAN-, Bluetooth- oder Mobilfunkmodul,
- eine Maschine, deren sicherheitsrelevante Parameter softwarebasiert konfiguriert oder übertragen werden.

Nicht jede dieser Eigenschaften führt automatisch zur gleichen Risikoeinstufung oder zum gleichen Konformitätsbewertungsverfahren. Sie sind jedoch starke Hinweise darauf, dass eine CRA-Prüfung erforderlich ist.

Für die Praxis empfiehlt sich daher eine einfache Vorprüfung:

1. Enthält die Maschine digitale Hardware, Software oder Firmware?
2. Wird die Maschine im Rahmen einer gewerblichen Tätigkeit auf dem EU-Markt bereitgestellt?

3. Gibt es eine direkte oder indirekte physische oder logische Datenverbindung zu einem Gerät oder Netzwerk?
4. Ist diese Verbindung bestimmungsgemäß vorgesehen oder vernünftigerweise vorhersehbar?
5. Gibt es digitale Komponenten oder Softwarebestandteile, die separat auf dem Markt bereitgestellt werden?
6. Gibt es entfernte Datenverarbeitung, Cloud-Funktionen oder Fernwartungsfunktionen, die für eine Maschinenfunktion erforderlich sind?

Werden diese Fragen ganz oder teilweise bejaht, sollte die Maschine im Hinblick auf den CRA genauer betrachtet werden.

4.3 Beispiele aus dem Maschinenbau

Im Maschinenbau gibt es zahlreiche typische Komponenten, bei denen eine CRA-Relevanz naheliegt. Entscheidend ist dabei immer der konkrete Zusammenhang: Wird die Komponente separat auf dem Markt bereitgestellt? Ist sie Bestandteil einer Maschine? Verfügt sie über eine Datenverbindung? Ist sie für eine Funktion der Maschine erforderlich? Und wird die Gesamtmaschine als Produkt mit digitalen Elementen in Verkehr gebracht?



Abb. 4: CRA-relevante Produkte mit digitalen Elementen

SPS-Steuerung

Eine SPS verarbeitet digitale Signale, führt Software bzw. Firmware aus und ist häufig über Feldbusse oder Ethernet mit anderen Geräten verbunden. Wird eine Maschine mit SPS und Kommunikationsschnittstellen ausgeliefert, ist eine CRA-Prüfung regelmäßig naheliegend. Dies gilt insbesondere, wenn die SPS

programmierbar, updatefähig, über Netzwerk erreichbar oder mit übergeordneten Systemen verbunden ist.

HMI-System

Ein HMI dient der Bedienung, Parametrierung und Diagnose der Maschine. Es enthält Software, Benutzeroberflächen, häufig Benutzerrollen, Passwörter, Rezepturen, Betriebsdaten und Kommunikationsschnittstellen. Wenn über das HMI Maschinenparameter verändert, Diagnosedaten übertragen oder Updates eingespielt werden können, ist das HMI ein zentrales digitales Element der Maschine.

Industrie-PC

Ein Industrie-PC ist in der Regel eindeutig ein digitales Hardwareprodukt mit Software- und Betriebssystemanteilen. Er kann Visualisierung, Datenverarbeitung, Rezepturverwaltung, Bildverarbeitung, Datenlogging, Edge-Computing oder Kommunikationsfunktionen übernehmen. Für Maschinenbauer ist besonders relevant, welche Softwarestände, Betriebssysteme, Benutzerrechte, Updatewege und Netzwerkschnittstellen vorhanden sind.

Robotersteuerung

Robotersteuerungen enthalten umfangreiche Software, Sicherheitsparameter, Bewegungsprogramme, Kommunikationsschnittstellen und häufig Fernzugriffsmöglichkeiten. Sie können mit SPS, HMI, Sicherheitssteuerung, Kamerasystemen, Greifern, Feldbussen und Netzwerken verbunden sein. Bei Roboterapplikationen ist daher regelmäßig zu prüfen, welche Teile der Robotersteuerung, der Applikationssoftware und der Schnittstellen in die CRA-Betrachtung der Gesamtmaschine einzubeziehen sind.

Fernwartungsmodul

Fernwartungsmodule sind aus CRA-Sicht besonders relevant, weil sie bewusst eine Verbindung von außen zur Maschine ermöglichen. Sie können ein erhebliches Cyberrisiko darstellen, wenn Zugriffsschutz, Authentifizierung, Benutzerrollen, Protokollierung, Abschaltbarkeit oder sichere Konfiguration unzureichend ausgelegt sind. Ein Fernwartungsmodul sollte daher nie nur als „Service-Zubehör“ betrachtet werden, sondern als sicherheits- und konformitätsrelevante Schnittstelle der Maschine.

Safety-Steuerung

Sicherheitssteuerungen sind im klassischen CE-Prozess vor allem unter dem Gesichtspunkt der funktionalen Sicherheit relevant. Im CRA-Kontext ist zusätzlich zu betrachten, ob sicherheitsrelevante Parameter, Logik, Programme oder Diagnosedaten digital zugänglich, übertragbar oder veränderbar sind. Manipulationen an Sicherheitsparametern können unmittelbaren Einfluss auf die Maschinensicherheit haben. Deshalb ist die Schnittstelle zwischen Safety und Security hier besonders wichtig.

Frequenzumrichter mit Netzwerkschnittstelle

Moderne Frequenzumrichter verfügen häufig über Parametrier-, Diagnose-, Update- und Kommunikationsschnittstellen. Werden Antriebsparameter über Netzwerk übertragen oder können sicherheitsrelevante Funktionen softwarebasiert konfiguriert werden, sollte auch der Frequenzumrichter in die CRA-Betrachtung einbezogen werden. Entscheidend ist, ob durch einen Cyberangriff Maschinenfunktionen, Verfügbarkeit, Integrität, Vertraulichkeit oder sicherheitsrelevante Parameter beeinträchtigt werden können.

Diese Beispiele zeigen: Im Maschinenbau ist der CRA selten nur ein Thema für die IT-Abteilung. Er betrifft die Konstruktion, Steuerungstechnik, Softwareentwicklung, funktionale Sicherheit, Lieferantenauswahl, Inbetriebnahme, Dokumentation und den Serviceprozess.

4.4 Komponenten, Ersatzteile und separat bereitgestellte Software

Der CRA erfasst nicht nur fertige Endprodukte, sondern grundsätzlich auch Software- und Hardwarekomponenten, wenn diese separat auf dem Markt bereitgestellt werden. Für Maschinenbauer ist das in zwei Richtungen relevant.

Zum einen kann der Maschinenhersteller selbst Komponenten oder Software separat bereitstellen. Dies kann zum Beispiel bei Maschinen-Apps, Konfigurationstools, HMI-Software, Firmwarepaketen, Diagnoseprogrammen, Edge-Software, Steuerungsmodulen oder Fernwartungskomponenten der Fall sein. Werden solche Produkte eigenständig auf dem Markt bereitgestellt, kann für sie eine eigene CRA-Betrachtung erforderlich sein.

Zum anderen integriert der Maschinenhersteller zahlreiche zugekaufte Komponenten in seine Maschine. Dazu gehören Steuerungen, Betriebssysteme, Bibliotheken, Kommunikationsmodule, Sensorik, Kameras, Frequenzumrichter, Robotersteuerungen, Fernwartungsrouter oder Softwarepakete. Auch wenn diese Komponenten bereits vom Lieferanten bereitgestellt werden, bleibt der Maschinenhersteller für die CRA-Konformität seiner Gesamtmaschine verantwortlich. Er muss daher mit angemessener Sorgfalt prüfen, ob die integrierten Komponenten die Cybersicherheit der Maschine beeinträchtigen können.

Eine wichtige Ausnahme betrifft Ersatzteile. Der CRA gilt nicht für Ersatzteile, die auf dem Markt bereitgestellt werden, um identische Komponenten in Produkten mit digitalen Elementen zu ersetzen, sofern sie nach denselben Spezifikationen hergestellt werden wie die zu ersetzenden Komponenten.

Diese Ausnahme ist für Maschinenbauer praktisch wichtig, darf aber nicht zu weit verstanden werden. Ein identisches Ersatzteil, das eine bestehende Komponente ohne Funktionsänderung ersetzt, ist anders zu bewerten als ein modernisiertes Ersatzteil mit neuen Schnittstellen, neuer Software, neuer Firmware, neuen Kommunikationsfunktionen oder geänderter Zweckbestimmung. Sobald das Ersatzteil nicht mehr lediglich identisch ersetzt, sondern die digitalen Eigenschaften oder die Cyberrisiken verändert, sollte die CRA-Relevanz erneut geprüft werden.

Auch separat bereitgestellte Software verdient besondere Aufmerksamkeit. Software kann eigenständig ein Produkt mit digitalen Elementen sein. Dies betrifft nicht nur klassische Anwenderprogramme, sondern auch Maschinen-Software, Konfigurationstools, Firmware, Treiber, Apps, Updatepakete oder digitale Servicefunktionen. Wird Software nachträglich bereitgestellt, verändert oder aktualisiert, sollte der Hersteller dokumentieren, ob es sich um eine reine Wartungs- bzw. Sicherheitsaktualisierung handelt oder ob dadurch Funktionen, Schnittstellen, Zweckbestimmung oder Cyberrisiken wesentlich verändert werden.

4.5 Remote Data Processing / Cloud-Anbindung

Der CRA berücksichtigt ausdrücklich auch Lösungen zur entfernten Datenverarbeitung. Für Maschinenbauer ist dies besonders relevant, weil viele Maschinen heute mit Cloud-, Edge- oder Remote-Service-Funktionen verbunden werden.

Eine entfernte Datenverarbeitung ist nicht automatisch jede beliebige Cloud-Nutzung. Entscheidend ist, ob die Datenverarbeitung aus der Ferne für eine Funktion des Produkts erforderlich ist und ob die entsprechende Software vom Hersteller entwickelt wurde oder unter dessen Verantwortung entwickelt wurde. Fehlt diese entfernte Datenverarbeitung und kann das Produkt dadurch eine seiner Funktionen

nicht erfüllen, spricht dies dafür, dass die entfernte Datenverarbeitung Teil des Produkts mit digitalen Elementen ist.

Beispiele aus dem Maschinenbau können sein:

- eine Cloud-Funktion, ohne die eine Maschinenfunktion nicht ausgeführt werden kann,
- ein Remote-Service, der für bestimmte Steuerungs-, Diagnose- oder Optimierungsfunktionen erforderlich ist,
- eine externe Bildverarbeitung oder KI-Auswertung, deren Ergebnis direkt für den Maschinenablauf benötigt wird,
- ein herstellerspezifisches Portal, über das Maschinenfunktionen freigeschaltet, konfiguriert oder sicherheitsrelevante Einstellungen verwaltet werden,
- ein Remote-Diagnosesystem, das integraler Bestandteil der ausgelieferten Maschinenfunktion ist.

Nicht jede Cloud-Anbindung ist jedoch automatisch Teil des Produkts im Sinne des CRA. Ein allgemeiner Cloud-Speicher, ein reines Dokumentationsportal, ein allgemeines Ticketsystem oder ein optionales Analyseportal kann anders zu bewerten sein, wenn diese Dienste nicht erforderlich sind, damit das Produkt eine seiner Funktionen erfüllt. Die Abgrenzung hängt stark vom konkreten Produktkonzept ab.

Für Maschinenbauer ergibt sich daraus eine wichtige Praxisfrage: Ist die Cloud- oder Remote-Funktion lediglich ein zusätzlicher Service, oder ist sie Bestandteil der Maschinenfunktion, wie sie dem Kunden bereitgestellt wird? Je stärker eine Maschine auf entfernte Datenverarbeitung angewiesen ist, desto eher muss diese in die CRA-Betrachtung einbezogen werden.

In der technischen Dokumentation sollte daher beschrieben werden:

- welche Remote- oder Cloud-Funktionen vorhanden sind,
- welche Daten übertragen, gespeichert oder verarbeitet werden,
- ob die entfernte Verarbeitung für eine Maschinenfunktion erforderlich ist,
- wer die entsprechende Software entwickelt oder verantwortet,
- welche Schnittstellen zwischen Maschine und Remote-System bestehen,
- welche Schutzmaßnahmen für Vertraulichkeit, Integrität, Verfügbarkeit und Zugriffsschutz umgesetzt sind,
- wie Sicherheitsupdates, Schwachstellen und Konfigurationsänderungen behandelt werden.

Gerade bei cloudgestützten Maschinenfunktionen verschwimmt die Grenze zwischen Produkt, Software, Service und Betreiberumgebung. Der CRA zwingt Hersteller deshalb dazu, diese Grenze bewusst zu definieren und nachvollziehbar zu dokumentieren.

4.6 Ausnahmen und Abgrenzungen

Der CRA hat einen weiten Anwendungsbereich, enthält aber auch ausdrückliche Ausnahmen und Abgrenzungen. Für Maschinenbauer sind insbesondere folgende Punkte relevant.

Nicht erfasst sind Produkte mit digitalen Elementen, die nicht auf dem Markt bereitgestellt werden. Wird ein digitales Produkt also nicht im Rahmen einer gewerblichen Tätigkeit geliefert oder bereitgestellt, fällt es grundsätzlich nicht in den typischen Anwendungsbereich des CRA. Für den klassischen Maschinen-

bauer, der Maschinen oder Komponenten an Kunden liefert, ist diese Ausnahme jedoch meist nicht einschlägig.

Ebenfalls ausgenommen sind bestimmte Produktgruppen, die bereits durch speziellere europäische Regelungen erfasst sind. Dazu gehören insbesondere Medizinprodukte, In-vitro-Diagnostika, bestimmte Kraftfahrzeugprodukte, bestimmte luftfahrtrechtlich zertifizierte Produkte sowie Schiffsausrüstung. Außerdem sind Produkte ausgenommen, die ausschließlich für nationale Sicherheits- oder Verteidigungszwecke entwickelt oder verändert wurden, sowie Produkte, die speziell zur Verarbeitung von Verschlusssachen bestimmt sind.

Für den Maschinenbau ist wichtig: Eine Maschine fällt nicht allein deshalb aus dem CRA heraus, weil sie bereits unter die Maschinenverordnung fällt. Die Maschinenverordnung und der CRA können nebeneinander anwendbar sein. Die Maschinenverordnung adressiert insbesondere die Sicherheit von Maschinen und den Schutz von Personen vor Gefährdungen. Der CRA adressiert die Cyberresilienz des Produkts mit digitalen Elementen. Beide Betrachtungen können sich überschneiden, ersetzen sich aber nicht automatisch.

Auch die Funkanlagenrichtlinie, die EMV-Richtlinie, die Niederspannungsrichtlinie oder andere CE-Rechtsakte schließen den CRA nicht automatisch aus. Vielmehr ist jeweils zu prüfen, ob ein spezieller Rechtsakt die betreffenden Cybersecurity-Risiken bereits vollständig oder teilweise abdeckt und ob der CRA insoweit eingeschränkt oder ausgeschlossen ist. Eine pauschale Aussage „Maschinen fallen nicht unter den CRA, weil es die Maschinenverordnung gibt“ wäre daher falsch.

Besonders sorgfältig ist außerdem bei folgenden Grenzfällen zu prüfen:

- rein interne Eigenentwicklungen für den eigenen Betrieb,
- Open-Source-Software ohne kommerzielle Bereitstellung,
- Cloud- oder SaaS-Dienste ohne Produktbezug,
- Ersatzteile, die identisch zu vorhandenen Komponenten sind,
- Softwarearchive, Testversionen oder Entwicklungsstände,
- Umbauten und Retrofit-Maßnahmen an bereits vorhandenen Maschinen,
- Anlagen, bei denen mehrere Hersteller, Integratoren und Betreiber digitale Funktionen beisteuern.

Für Maschinenbauer empfiehlt sich daher eine dokumentierte Abgrenzungsentscheidung. Auch wenn der Hersteller zu dem Ergebnis kommt, dass ein Produkt oder eine Funktion nicht in den Anwendungsbereich des CRA fällt, sollte diese Entscheidung nachvollziehbar begründet werden. Das ist insbesondere dann sinnvoll, wenn digitale Schnittstellen, Fernwartung, Cloud-Funktionen oder separat bereitgestellte Software vorhanden sind.

4.7 Bedeutung von „wesentlicher Änderung“ und Produktänderungen nach 2027

Die vollständige Anwendung der Hauptpflichten des CRA beginnt am 11. Dezember 2027. Für Produkte mit digitalen Elementen, die bereits vor diesem Datum in Verkehr gebracht wurden, sieht der CRA eine Übergangsregelung vor. Solche Produkte unterliegen den Anforderungen des CRA grundsätzlich nur dann, wenn sie ab dem 11. Dezember 2027 einer wesentlichen Änderung unterzogen werden.

Eine wesentliche Änderung liegt vor, wenn eine Änderung nach dem Inverkehrbringen die Konformität des Produkts mit den wesentlichen Cybersicherheitsanforderungen beeinflusst oder wenn sich dadurch der Zweck ändert, für den das Produkt bewertet wurde.

Für Maschinenbauer ist diese Regelung besonders relevant bei Retrofit, Modernisierung, Softwareänderungen und Nachrüstungen. Nicht jede Wartung, Reparatur oder Sicherheitsaktualisierung wird automatisch eine wesentliche Änderung darstellen. Eine reine Fehlerbehebung oder ein Sicherheitsupdate kann gerade dazu dienen, die vorhandene Konformität aufrechtzuerhalten. Anders kann es jedoch aussehen, wenn durch die Änderung neue digitale Funktionen, neue Schnittstellen, neue Fernzugriffe, neue Cloud-Anbindungen, neue Softwarearchitekturen oder neue Verwendungszwecke entstehen.

Beispiele, bei denen eine CRA-relevante Änderung geprüft werden sollte, sind:

- Nachrüstung eines Fernwartungszugangs,
- Umstellung von lokaler Bedienung auf cloudgestützte Bedienung oder Diagnose,
- Austausch einer einfachen Steuerung gegen eine vernetzte Steuerung,
- Integration eines Industrie-PCs mit Netzwerk- und Updatefunktion,
- Ergänzung einer App zur Maschinenbedienung oder Parametrierung,
- Änderung sicherheitsrelevanter Software oder Parametrierlogik,
- Erweiterung der Maschine um digitale Services,
- Änderung des bestimmungsgemäßen Verwendungszwecks durch Softwarefunktionen,
- Austausch einer Komponente gegen eine funktional erweiterte Komponente mit neuen Cyberrisiken.

Wichtig ist außerdem die Unterscheidung zwischen einem bereits vor dem 11. Dezember 2027 in Verkehr gebrachten Einzelprodukt und neuen Produkten derselben Baureihe. Die Übergangsregelung bedeutet nicht, dass eine Baureihe dauerhaft unverändert weiter ausgeliefert werden darf, ohne den CRA zu berücksichtigen. Wird ein Produkt nach dem 11. Dezember 2027 neu in Verkehr gebracht, muss es die dann geltenden CRA-Anforderungen erfüllen, sofern es in den Anwendungsbereich fällt.

Für die Praxis sollten Maschinenbauer daher ein Änderungsmanagement einführen, das Cybersecurity ausdrücklich berücksichtigt. Bei jeder relevanten Änderung an Steuerung, Software, Firmware, Kommunikation, Fernwartung, Cloud-Anbindung oder digitalen Funktionen sollte geprüft und dokumentiert werden:

- Welche digitale Änderung wird vorgenommen?
- Betrifft sie die bestimmungsgemäße Verwendung?
- Entstehen neue Schnittstellen oder Datenverbindungen?
- Ändert sich die Cybersecurity-Risikobewertung?
- Werden wesentliche Cybersicherheitsanforderungen neu oder anders berührt?
- Muss die technische Dokumentation angepasst werden?
- Ist eine neue oder ergänzende Konformitätsbewertung erforderlich?
- Müssen Benutzerinformationen, Supportzeitraum oder Updateprozesse angepasst werden?

Damit wird die „wesentliche Änderung“ zu einem wichtigen Prüfpunkte im Lebenszyklus der Maschine. Gerade bei Retrofit-Projekten, Nachrüstungen und Software-Updates sollte diese Bewertung nicht informell erfolgen, sondern nachvollziehbar dokumentiert werden.

5 Welche Pflichten kommen auf Maschinenbauer zu?

Der Cyber Resilience Act führt für Hersteller von Produkten mit digitalen Elementen eine Reihe neuer Pflichten ein. Für Maschinenbauer bedeutet dies nicht, dass der bestehende CE-Prozess vollständig ersetzt wird. Vielmehr wird der bekannte Produktkonformitätsprozess um eine systematische Cybersecurity-Betrachtung erweitert.

Während sich der klassische Maschinenbau bisher vor allem mit mechanischen, elektrischen, steuerungstechnischen und funktional sicheren Aspekten beschäftigt hat, verlangt der CRA zusätzlich eine produktbezogene Betrachtung der Cyberresilienz. Der Hersteller muss künftig nachweisen können, dass digitale Elemente, Software, Firmware, Schnittstellen, Kommunikationsfunktionen und updatefähige Systeme angemessen gegen Cyberrisiken ausgelegt und über den vorgesehenen Supportzeitraum betreut werden.

Für Maschinenbauer betrifft dies nicht nur die IT-Abteilung. Relevante Pflichten entstehen in der Konstruktion, Elektrotechnik, Steuerungstechnik, Softwareentwicklung, Lieferantenauswahl, Dokumentation, Inbetriebnahme, Serviceorganisation und im Änderungsmanagement.

5.1 Cybersecurity Risk Assessment als neue Pflicht im CE-Prozess

Eine zentrale neue Pflicht ist die Durchführung einer Cybersecurity-Risikobeurteilung. Diese dient dazu, die relevanten Cyberrisiken des Produkts mit digitalen Elementen zu identifizieren und daraus geeignete technische und organisatorische Maßnahmen abzuleiten.

Für Maschinenbauer bedeutet dies: Neben der klassischen Risikobeurteilung zur Maschinensicherheit muss künftig auch betrachtet werden, welche Cyberbedrohungen auf digitale Elemente der Maschine wirken können. Dabei geht es nicht nur um den Schutz von personenbezogenen Daten oder der Unternehmensnetzwerke, sondern auch um die Integrität, Verfügbarkeit und Vertraulichkeit der Maschine und ihrer digitalen Funktionen.

Typische Fragestellungen einer Cybersecurity-Risikobewertung im Maschinenbau sind zum Beispiel:

- Welche digitalen Elemente enthält die Maschine?
- Welche Software, Firmware und Kommunikationsschnittstellen sind vorhanden?
- Gibt es Fernwartungszugänge, Cloud-Funktionen oder Service-Schnittstellen?
- Können Maschinenparameter digital verändert werden?
- Können sicherheitsrelevante Einstellungen, Programme oder Grenzwerte manipuliert werden?
- Welche Auswirkungen hätte ein unbefugter Zugriff auf Verfügbarkeit, Qualität, Prozesssicherheit oder Maschinensicherheit?
- Welche Komponenten stammen von Dritten und welche Schwachstellen können dadurch eingebracht werden?
- Wie werden Updates, Patches und Konfigurationsänderungen kontrolliert?

Die Cybersecurity-Risikobewertung sollte bereits in der Entwicklungsphase beginnen. Wird sie erst am Ende eines Projekts durchgeführt, sind wirksame Maßnahmen häufig nur noch schwer oder mit erheblichem Aufwand umsetzbar. Besonders bei Maschinen mit vernetzter SPS, HMI, Industrie-PC, Robotersteuerung, Fernwartung, OPC-UA-Schnittstelle, Cloud-Anbindung oder updatefähiger Software sollte die Cybersecurity-Betrachtung daher ein fester Bestandteil der Projektierung sein.

Praktisch kann die Cybersecurity-Risikobewertung als eigener Abschnitt in den Entwicklungs- und CE-Prozess integriert werden. Sie ersetzt nicht die Risikobeurteilung nach Maschinenverordnung und EN ISO 12100, sondern ergänzt diese. Wo Cybersecurity-Auswirkungen Einfluss auf Safety-Funktionen oder sicherheitsbezogene Steuerungen haben können, müssen beide Betrachtungen miteinander verknüpft werden.

5.2 Security by Design und Security by Default

Der CRA verlangt, dass Produkte mit digitalen Elementen bereits so entworfen, entwickelt und hergestellt werden, dass ein angemessenes Cybersicherheitsniveau erreicht wird. Für Maschinenbauer bedeutet dies, dass Cybersecurity nicht als nachträgliche Zusatzfunktion verstanden werden darf. Sie muss von Anfang an in Architektur, Steuerungskonzept, Softwaredesign, Schnittstellenkonzept und Auslieferungszustand berücksichtigt werden.

Security by Design bedeutet, dass Sicherheitsmaßnahmen bereits im Produktdesign angelegt werden. Im Maschinenbau betrifft dies zum Beispiel die Auswahl geeigneter Steuerungskomponenten, die Trennung von Netzwerken, die Absicherung von Service-Schnittstellen, die Begrenzung von Benutzerrechten, die sichere Verwaltung von Zugangsdaten, die Absicherung von Update-Prozessen und die Vermeidung unnötiger offener Schnittstellen.

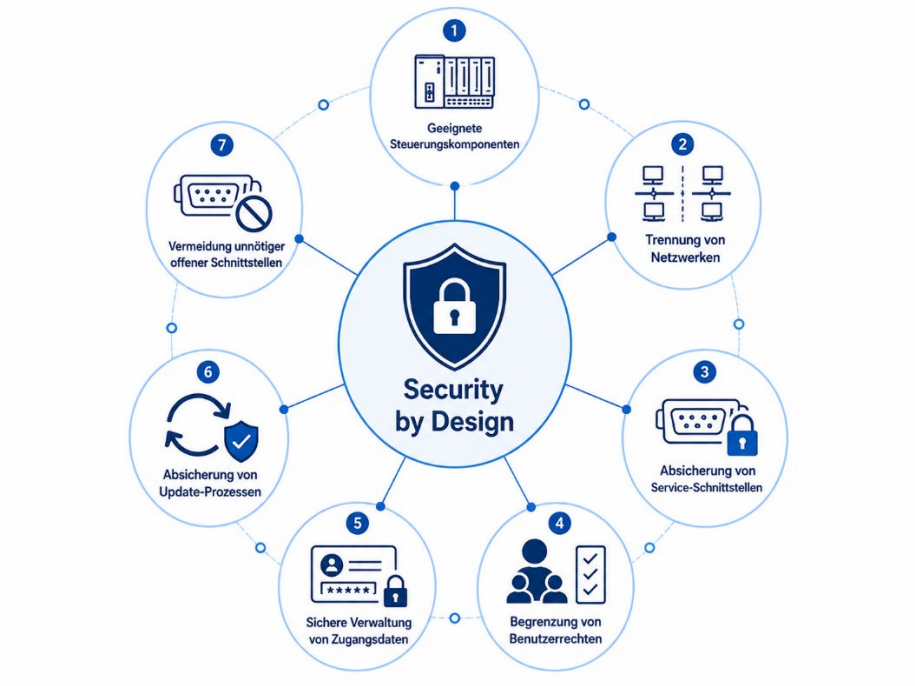


Abb. 5: Security by design

Security by Default bedeutet auch, dass die Maschine im Auslieferungszustand möglichst sicher konfiguriert ist. Unsichere Standardpasswörter, unnötig aktivierte Dienste, offene Fernzugänge, nicht benötigte Benutzerkonten oder ungeschützte Schnittstellen passen nicht zu diesem Grundsatz. Der Betreiber soll nicht erst durch umfangreiche Nacharbeiten einen sicheren Zustand herstellen müssen.

Typische Anforderungen an Security by Design und Security by Default im Maschinenbau können sein:

- keine allgemeinen Standardpasswörter wie „admin/admin“ oder „password“,

- individuelle oder bei Erstinbetriebnahme zu ändernde Zugangsdaten,
- deaktivierte Fernwartung im Auslieferungszustand, sofern sie nicht benötigt wird,
- Freigabe von Fernwartung nur durch den Betreiber oder autorisiertes Personal,
- rollenbasiertes Berechtigungskonzept für Bedienung, Parametrierung, Service und Administration,
- Absicherung von Update- und Backup-Prozessen,
- Protokollierung sicherheitsrelevanter Änderungen,
- Begrenzung der erreichbaren Dienste und Kommunikationsports,
- Schutz vor unbefugter Veränderung von Programmen, Rezepturen und Parametern,
- klare Trennung zwischen Bedienfunktionen, Servicefunktionen und sicherheitsrelevanter Parametrierung.

Für Maschinenbauer ist besonders wichtig, dass Security by Default nicht im Widerspruch zur Bedienbarkeit der Maschine stehen darf. Eine Maschine muss weiterhin wartbar und bedienbar bleiben. Die Herausforderung besteht darin, einen Auslieferungszustand zu schaffen, der sicher ist und gleichzeitig eine realistische Inbetriebnahme und Servicepraxis ermöglicht.

5.3 Anforderungen an Entwicklung, Produktion und Wartung

Der CRA betrachtet Cybersecurity nicht nur als Eigenschaft des fertigen Produkts. Die Anforderungen müssen über den gesamten Produktentstehungs- und Betreuungsprozess hinweg berücksichtigt werden. Für Maschinenbauer betrifft dies Entwicklung, Produktion, Auslieferung, Inbetriebnahme und Wartung.

In der Entwicklung müssen digitale Funktionen, Schnittstellen, Softwarekomponenten und Cybersecurity-Anforderungen systematisch spezifiziert werden. Dazu gehört auch, dass Änderungen an Software, Firmware oder Steuerungsarchitektur kontrolliert erfolgen. Die Maschine sollte nicht nur funktional getestet werden, sondern auch im Hinblick auf relevante Cybersecurity-Anforderungen.

In der Produktion muss sichergestellt werden, dass die tatsächlich ausgelieferte Maschine dem bewerteten und dokumentierten Stand entspricht. Das betrifft zum Beispiel Softwarestände, Firmwarestände, Konfigurationsdateien, Benutzerkonten, Netzwerkeinstellungen, Zertifikate, Remote-Service-Konfigurationen und sicherheitsrelevante Parameter. Eine Maschine, die in der technischen Dokumentation als sicher konfiguriert beschrieben ist, darf nicht mit abweichenden, unsicheren Werkseinstellungen ausgeliefert werden.

Bei der Auslieferung und Inbetriebnahme muss der sichere Zustand hergestellt und nachvollziehbar dokumentiert werden. Dazu gehören zum Beispiel die Änderung initialer Passwörter, die Aktivierung oder Deaktivierung von Fernwartung, die Dokumentation von Netzwerkadressen, die Übergabe von Benutzerrollen, die Festlegung von Updatewegen und die Einweisung des Betreibers in sicherheitsrelevante Cybersecurity-Funktionen.

In der Wartung und im Service muss der Hersteller sicherstellen, dass Cybersecurity nicht durch Serviceeingriffe verschlechtert wird. Wird beispielsweise ein alter Softwarestand eingespielt, ein Fernwartungszugang dauerhaft offen gelassen, ein Standardpasswort gesetzt oder eine unsichere Konfiguration wiederhergestellt, kann dies die Cyberresilienz der Maschine beeinträchtigen. Serviceprozesse müssen daher klare Vorgaben für sichere Konfiguration, Zugriff, Dokumentation und Rücksetzung enthalten.

Für Maschinenbauer empfiehlt sich deshalb ein durchgängiger Prozess, der Cybersecurity-Anforderungen von der Produktidee bis zum Ende des Supportzeitraums verfolgt. Dieser Prozess muss nicht zwingend ein komplett neues Managementsystem sein. Er kann in vorhandene Abläufe wie Entwicklungsfreigabe, Änderungsmanagement, Lieferantenbewertung, Werksabnahme, Inbetriebnahmeprotokoll, Serviceanweisung und technische Dokumentation integriert werden.

5.4 Schwachstellenmanagement über den Supportzeitraum

Eine der größten Veränderungen durch den CRA ist die Pflicht zum Schwachstellenmanagement über einen definierten Supportzeitraum. Der Hersteller muss festlegen, wie lange das Produkt mit digitalen Elementen unterstützt wird, und während dieses Zeitraums dafür sorgen, dass Schwachstellen wirksam behandelt werden.

Für Maschinenbauer ist dies besonders anspruchsvoll, weil Maschinen häufig deutlich länger genutzt werden als klassische IT-Produkte. Während einzelne IT-Komponenten nach einigen Jahren ersetzt werden, bleiben Maschinen, Anlagen, Steuerungen und Retrofit-Systeme oft zehn, fünfzehn oder zwanzig Jahre im Einsatz. Der Hersteller muss daher bewusst festlegen und begründen, für welchen Zeitraum Cybersecurity-Support für das Produkt geleistet wird.

Zum Schwachstellenmanagement gehören insbesondere:

- die Möglichkeit, Schwachstellenmeldungen entgegenzunehmen,
- ein klar benannter Kontaktpunkt für Schwachstellenmeldungen,
- interne Zuständigkeiten für die Bewertung von Schwachstellen,
- die Beobachtung relevanter Informationsquellen, z. B. Lieferanteninformationen, CERT-Meldungen, Schwachstellendatenbanken,
- die Bewertung, ob eine Schwachstelle das eigene Produkt betrifft,
- die Bewertung der Auswirkungen auf Maschinenfunktion, Sicherheit, Verfügbarkeit und Daten,
- die Festlegung von Korrektur- oder Minderungsmaßnahmen,
- die Kommunikation mit Lieferanten, Betreibern und zuständigen Stellen,
- die Dokumentation der Bewertung und der getroffenen Maßnahmen.

Besonders wichtig ist der Umgang mit Drittkomponenten. Maschinen enthalten häufig Steuerungen, Betriebssysteme, Softwarebibliotheken, Kommunikationsmodule, Router, HMI-Systeme, Robotersteuerungen, Sensoren, Kameras oder Frequenzumrichter von externen Herstellern. Wird in einer solchen Komponente eine Schwachstelle bekannt, muss der Maschinenhersteller bewerten können, ob seine Maschine betroffen ist und ob Maßnahmen erforderlich sind.

Damit wird Schwachstellenmanagement zu einem dauerhaften Prozess. Es reicht nicht aus, bei der Auslieferung der Maschine einen sicheren Zustand herzustellen. Der Hersteller muss während des Supportzeitraums handlungsfähig bleiben, neue Schwachstellen bewerten und erforderliche Maßnahmen bereitstellen können.

5.5 Update- und Patch-Management

Eng mit dem Schwachstellenmanagement verbunden ist das Update- und Patch-Management. Wenn Schwachstellen festgestellt werden, müssen Hersteller in der Lage sein, Sicherheitsupdates oder andere Minderungsmaßnahmen bereitzustellen. Für Maschinenbauer ist dies ein besonders sensibler Bereich, weil Updates nicht nur IT-Funktionen, sondern auch Maschinenfunktionen, Prozessverhalten und sicherheitsrelevante Steuerungen beeinflussen können.

Ein Updatekonzept für Maschinen sollte daher mehr leisten als nur die technische Möglichkeit, Software zu aktualisieren. Es muss festlegen, welche Komponenten updatefähig sind, wer Updates freigeben darf, wie Updates getestet werden, wie sie verteilt werden und wie verhindert wird, dass durch ein Update neue Risiken entstehen.

Wichtige Fragen für Maschinenbauer sind:

- Welche Software- und Firmwarestände sind in der Maschine enthalten?
- Welche Komponenten können aktualisiert werden?
- Sind Updates lokal, remote oder nur durch Servicepersonal möglich?
- Wie wird die Echtheit und Integrität eines Updates sichergestellt?
- Wie wird verhindert, dass unautorisierte Software eingespielt wird?
- Wie werden Updates vor der Freigabe getestet?
- Gibt es eine Möglichkeit zum Rollback oder zur Wiederherstellung eines sicheren Zustands?
- Wie werden Betreiber über Sicherheitsupdates informiert?
- Wie wird dokumentiert, welche Maschinen welchen Update-Stand haben?

Bei sicherheitsbezogenen Steuerungen ist besondere Vorsicht erforderlich. Ein Update darf nicht dazu führen, dass validierte Sicherheitsfunktionen unbemerkt verändert werden. Wenn sicherheitsrelevante Parameter, Programme oder Firmware betroffen sind, muss geprüft werden, ob eine erneute Validierung, eine Aktualisierung der technischen Dokumentation oder eine ergänzende Bewertung der funktionalen Sicherheit erforderlich ist.

Der CRA verlangt keine pauschale Fernupdatefähigkeit für jede Maschine. Dennoch muss der Hersteller ein realistisches Verfahren haben, um Schwachstellen zu behandeln und Sicherheitsupdates oder Minderungsmaßnahmen bereitzustellen. Je nach Maschine kann dies über automatische Updates, manuell freigegebene Updates, Serviceeinsätze, Betreiberanweisungen oder temporäre Risikominderungsmaßnahmen erfolgen.

5.6 Meldepflichten bei aktiv ausgenutzten Schwachstellen

Der CRA führt Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle ein. Diese Pflichten gelten bereits ab dem 11. September 2026 und damit früher als die vollständige Anwendung der Hauptpflichten.

Für Maschinenbauer bedeutet dies, dass nicht erst ab Dezember 2027 Prozesse aufgebaut werden dürfen. Hersteller müssen schon vorher in der Lage sein, relevante Schwachstellen und Sicherheitsvorfälle zu erkennen, intern zu bewerten und fristgerecht zu melden.

Besonders wichtig ist die Unterscheidung zwischen einer bekannten Schwachstelle und einer aktiv ausgenutzten Schwachstelle. Nicht jede theoretische Schwachstelle löst automatisch dieselbe Meldepflicht aus. Kritisch wird es insbesondere dann, wenn dem Hersteller bekannt wird, dass eine Schwachstelle tatsächlich ausgenutzt wird oder ein schwerwiegender Sicherheitsvorfall Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen hat.

Für Maschinenbauer sollte ein Meldeprozess mindestens folgende Elemente enthalten:

- Eingangskanal für interne und externe Meldungen,
- Erstbewertung der Meldung,
- technische Analyse der Betroffenheit,
- Entscheidung, ob eine aktiv ausgenutzte Schwachstelle oder ein schwerwiegender Sicherheitsvorfall vorliegt,
- Festlegung der Meldezuständigkeit,
- fristgerechte Meldung über die vorgesehene Meldeplattform,
- Information betroffener Betreiber, soweit erforderlich,
- Nachverfolgung von Korrektur- oder Minderungsmaßnahmen,
- Dokumentation des gesamten Vorgangs.

In der Praxis sollten diese Abläufe vorab festgelegt werden. Die kurzen Fristen für Frühwarnung und Hauptmeldung lassen im Ernstfall wenig Zeit für organisatorische Grundsatzentscheidungen. Maschinenbauer sollten daher bereits vor Eintritt eines Vorfalls klären, wer technisch bewertet, wer rechtlich prüft, wer meldet, wer Kunden informiert und wer Korrekturmaßnahmen koordiniert.

5.7 Techn. Dokumentation, EU-Konformitätserklärung und CE-Kennzeichnung

Der CRA wirkt sich unmittelbar auf die technische Dokumentation, die EU-Konformitätserklärung und die CE-Kennzeichnung aus. Für Produkte im Anwendungsbereich des CRA muss der Hersteller nachweisen können, dass die wesentlichen Cybersecurity-Anforderungen erfüllt wurden.

Die technische Dokumentation muss daher künftig auch Cybersecurity-Aspekte enthalten. Dazu gehören insbesondere die Cybersecurity-Risikobeurteilung, die Beschreibung der digitalen Elemente, Schnittstellen und Datenverbindungen, die angewandten Normen oder technischen Spezifikationen, die gewählten Schutzmaßnahmen, die Bewertung von Drittkomponenten, das Schwachstellenmanagement, das Updatekonzept, die Benutzerinformationen und die Begründung des Supportzeitraums.

Für Maschinenbauer ist dabei entscheidend, dass die Cybersecurity-Dokumentation mit der übrigen CE-Dokumentation zusammenpasst. Die Beschreibung der Maschine, die Risikobeurteilung, die Steuerungsarchitektur, die funktionale Sicherheit, die Betriebsanleitung und die CRA-Dokumentation dürfen sich nicht widersprechen. Wenn zum Beispiel in der Betriebsanleitung ein Fernwartungszugang beschrieben wird, muss dieser auch in der Cybersecurity-Risikobewertung und im Schnittstellenkonzept berücksichtigt sein.

Vor dem Inverkehrbringen muss der Hersteller das geeignete Konformitätsbewertungsverfahren durchführen. Je nach Produktklassifizierung kann dies eine interne Fertigungskontrolle, eine Drittprüfung durch eine notifizierte Stelle oder ein anderes zulässiges Verfahren sein. Nach erfolgreicher

Konformitätsbewertung wird die EU-Konformitätserklärung erstellt und die CE-Kennzeichnung angebracht.

Für Maschinenbauer bedeutet dies: Der CRA kann künftig als zusätzlicher Rechtsakt in der EU-Konformitätserklärung aufzuführen sein. Bei Maschinen, die sowohl unter die Maschinenverordnung als auch unter den CRA fallen, muss die Konformität mit beiden Rechtsakten bewertet und dokumentiert werden. Die CE-Kennzeichnung bleibt dabei ein einheitliches Zeichen, steht aber für die Einhaltung aller anwendbaren EU-Harmonisierungsrechtsakte.

5.8 Benutzerinformation und Betriebsanleitung

Der CRA verlangt, dass Produkte mit digitalen Elementen von klaren, verständlichen und lesbaren Informationen und Anleitungen begleitet werden, die eine sichere Installation, Inbetriebnahme, Nutzung, Wartung und Außerbetriebnahme ermöglichen. Für Maschinenbauer bedeutet dies, dass die Betriebsanleitung künftig auch Cybersecurity-relevante Informationen enthalten muss.

Dabei geht es nicht darum, die Betriebsanleitung mit IT-Fachbegriffen zu überfrachten. Vielmehr muss der Betreiber die Informationen erhalten, die er benötigt, um die Maschine sicher und cyberresilient zu betreiben.

Typische Inhalte für die Betriebsanleitung können sein:

- Beschreibung vorhandener digitaler Schnittstellen,
- Hinweise zur sicheren Netzwerkintegration,
- Anforderungen an Passwörter und Benutzerrollen,
- Umgang mit Fernwartungszugängen,
- Aktivierung und Deaktivierung von Remote-Zugriffen,
- sichere Durchführung von Updates,
- Hinweise zu Backup und Wiederherstellung,
- Verhalten bei Verdacht auf Cyberangriff oder Manipulation,
- Kontaktstelle für Schwachstellenmeldungen,
- Supportzeitraum und Ende des Supports,
- Hinweise zur Außerbetriebnahme, Datenlöschung und Weitergabe der Maschine.

Gerade bei Maschinen mit Fernwartung ist eine klare Beschreibung erforderlich. Der Betreiber muss verstehen, wann ein Fernzugriff möglich ist, wer ihn freigeben darf, wie er beendet wird und welche organisatorischen Maßnahmen auf Betreiberseite erforderlich sind. Ebenso sollte klar geregelt sein, dass Zugangsdaten nicht unkontrolliert weitergegeben werden dürfen und dass Änderungen an sicherheitsrelevanten Parametern nur durch autorisierte Personen erfolgen dürfen.

Für Maschinenbauer bietet es sich an, einen eigenen Abschnitt „Cybersecurity“ oder „IT-Sicherheit und digitale Schnittstellen“ in die Betriebsanleitung aufzunehmen. Dieser Abschnitt sollte auf die konkrete Maschine zugeschnitten sein und nicht nur allgemeine Hinweise enthalten.

5.9 Lieferantenmanagement und Software-/Komponentenverzeichnis

Der CRA erhöht die Anforderungen an das Lieferantenmanagement erheblich. Maschinenhersteller integrieren in der Regel zahlreiche digitale Komponenten, die sie nicht selbst entwickeln. Trotzdem bleibt der Hersteller der Gesamtmaschine dafür verantwortlich, dass diese Komponenten die Cybersecurity der Maschine nicht beeinträchtigen.

Daher müssen Maschinenbauer künftig stärker prüfen, welche digitalen Komponenten, Softwarebestandteile, Firmwarestände, Betriebssysteme, Bibliotheken und Kommunikationsmodule in der Maschine verwendet werden. Dafür ist ein Software- und Komponentenverzeichnis erforderlich. In der IT-Security wird hierfür häufig der Begriff Software Bill of Materials, kurz SBOM, verwendet.

Ein solches Verzeichnis dient dazu, Abhängigkeiten nachvollziehbar zu machen. Wenn später eine Schwachstelle in einer bestimmten Softwarebibliothek, Firmwareversion oder Komponente bekannt wird, muss der Hersteller feststellen können, ob und welche Maschinen betroffen sind.

Für den Maschinenbau sollte ein Software- und Komponentenverzeichnis mindestens folgende Informationen enthalten:

- digitale Hauptkomponenten der Maschine,
- Hersteller und Typ der Komponente,
- Software- und Firmwarestände,
- Betriebssysteme und relevante Bibliotheken,
- Kommunikationsschnittstellen und Protokolle,
- sicherheitsrelevante Konfigurationsstände,
- Lieferanteninformationen zu Schwachstellen und Updates,
- Supportzeiträume der Komponenten,
- Zuordnung zu Maschinen, Seriennummern oder Produktvarianten.

Das Lieferantenmanagement sollte zusätzlich sicherstellen, dass relevante Cybersecurity-Informationen bereits beim Einkauf oder bei der Komponentenauswahl verfügbar sind. Dazu gehören zum Beispiel Angaben zu bekannten Schwachstellen, Updatefähigkeit, Supportzeitraum, sicheren Standardkonfigurationen, Zugriffsschutz, Dokumentation, Meldewegen und langfristiger Verfügbarkeit von Sicherheitsupdates.

Für Maschinenbauer bedeutet dies: Cybersecurity wird zu einem Auswahlkriterium bei Komponenten und Lieferanten. Eine technisch geeignete Steuerung, ein HMI oder ein Fernwartungsrouter ist künftig nicht nur nach Funktion, Preis und Lieferzeit zu bewerten, sondern auch danach, ob der Lieferant die für CRA-Konformität erforderlichen Informationen und Unterstützungsprozesse bereitstellen kann.

6 Harmonisierte Normen und Normungslandschaft

Harmonisierte Normen werden für die praktische Umsetzung des Cyber Resilience Act eine zentrale Rolle spielen. Sie übersetzen die rechtlich formulierten Anforderungen des CRA in technische, prüfbare und dokumentierbare Anforderungen. Für Maschinenbauer ist diese Normungslandschaft besonders wichtig, weil viele Unternehmen zwar mit CE-Prozessen, Risikobeurteilungen und funktionaler Sicherheit vertraut sind, jedoch noch keine etablierten Prozesse für produktbezogene Cybersecurity besitzen.

Stand Juni 2026 befindet sich die CRA-Normung noch im Aufbau. Es gibt dennoch bereits einige Normen, die fachlich für die Thematik Cybersecurity im Maschinenbau nützlich sind. Dazu gehören insbesondere die EN IEC 62443-Reihe für industrielle Automatisierungs- und Steuerungssysteme, Normen zum Schwachstellenmanagement sowie Normen zur Cybersecurity von Funkanlagen. Diese Normen sind jedoch nicht automatisch harmonisierte Normen zum CRA. Eine Vermutungswirkung im Sinne des CRA entsteht erst, wenn die jeweilige Norm im Amtsblatt der Europäischen Union als harmonisierte Norm zum CRA gelistet ist.

Für Maschinenbauer ergibt sich daraus eine zweistufige Betrachtung: Einerseits sollten vorhandene Normen bereits heute genutzt werden, um technische und organisatorische Cybersecurity-Maßnahmen strukturiert aufzubauen. Andererseits muss sorgfältig beobachtet werden, welche Normen künftig ausdrücklich zum CRA harmonisiert werden und damit eine formale Vermutungswirkung auslösen können.

6.1 Bedeutung harmonisierter Normen und Vermutungswirkung

Harmonisierte Normen sind europäische Normen, die auf Grundlage eines Standardisierungsauftrags der Europäischen Kommission erstellt und anschließend im Amtsblatt der Europäischen Union referenziert werden. Werden solche Normen korrekt angewendet, kann der Hersteller für die von der Norm abgedeckten Anforderungen von einer Vermutungswirkung ausgehen.

Diese Vermutungswirkung bedeutet nicht, dass eine Norm zwingend angewendet werden muss. Die Anwendung harmonisierter Normen bleibt grundsätzlich freiwillig. Der Hersteller kann die gesetzlichen Anforderungen auch auf anderem Wege erfüllen. In diesem Fall muss er jedoch selbst nachweisen und dokumentieren, dass seine technischen und organisatorischen Lösungen ein gleichwertiges Schutzniveau erreichen.

Für Maschinenbauer ist die Vermutungswirkung aus anderen CE-Bereichen bereits gut bekannt. Bei der Maschinenverordnung bzw. der bisherigen Maschinenrichtlinie erleichtern harmonisierte Normen den Nachweis, dass die jeweiligen grundlegenden Sicherheits- und Gesundheitsschutzanforderungen erfüllt wurden. Beim CRA wird eine vergleichbare Logik auf die wesentlichen Cybersicherheitsanforderungen angewendet.

Der praktische Nutzen harmonisierter CRA-Normen liegt vor allem in folgenden Punkten:

- Sie konkretisieren abstrakte gesetzliche Anforderungen.
- Sie schaffen ein gemeinsames technisches Verständnis für Hersteller, Prüfstellen und Marktüberwachungsbehörden.
- Sie erleichtern die Strukturierung der technischen Dokumentation.
- Sie unterstützen die Auswahl geeigneter technischer Maßnahmen.
- Sie können den Aufwand für die Konformitätsbewertung reduzieren.

- Sie schaffen mehr Rechtssicherheit bei der Bewertung von Cybersecurity-Maßnahmen.

Wichtig ist jedoch: Die Vermutungswirkung gilt nur für die Anforderungen, die von der jeweiligen Norm tatsächlich abgedeckt sind. Wird eine Norm nur teilweise angewendet oder deckt sie nur bestimmte Aspekte des CRA ab, muss der Hersteller die verbleibenden Anforderungen weiterhin eigenständig bewerten und dokumentieren.

6.2 Stand der CRA-Normung

Die Europäische Kommission hat mit dem Standardisierungsauftrag M/606 die Entwicklung von Normen zur Unterstützung des CRA angestoßen. Dieser Auftrag umfasst 41 Normungsvorhaben. Die Normen sollen sowohl horizontale Anforderungen als auch vertikale bzw. produktspezifische Anforderungen abdecken.

Horizontale Normen sollen produktübergreifend anwendbar sein. Sie legen allgemeine Anforderungen, Begriffe, Prozesse, Risikobewertungsmethoden, Schwachstellenmanagement und generische Sicherheitsanforderungen fest. Diese Normen sind für nahezu alle Hersteller von Produkten mit digitalen Elementen relevant, unabhängig davon, ob es sich um Consumer-Produkte, Software, industrielle Komponenten oder Maschinen handelt.

Vertikale Normen sollen dagegen bestimmte Produktgruppen adressieren. Sie konkretisieren Anforderungen für bestimmte Kategorien von Produkten mit digitalen Elementen, zum Beispiel Betriebssysteme, Netzwerkkomponenten, VPN-Systeme, Netzwerkmanagementsysteme oder andere im CRA besonders geregelte Produktgruppen.

Stand Juni 2026 ist wichtig zu unterscheiden:
Bereits vorhandene Cybersecurity-Normen können fachlich hilfreich sein, sind aber nicht automatisch CRA-harmonisiert. Die eigentlichen CRA-harmonisierten Normen befinden sich noch in Erarbeitung. Maschinenbauer sollten daher bestehende Normen bereits heute als Stand der Technik und als Orientierung nutzen, gleichzeitig aber die Entwicklung der CRA-spezifischen Normen aktiv beobachten.

Besonders relevant ist die entstehende Normenreihe EN 40000. Sie soll horizontale Anforderungen für Produkte mit digitalen Elementen strukturieren. Dazu gehören unter anderem Begriffe, Grundprinzipien der Cyberresilienz, Schwachstellenbehandlung, generische Sicherheitsanforderungen sowie unterstützende Dokumente zu Bedrohungen und Sicherheitszielen. Für Maschinenbauer dürfte insbesondere der Teil zu generischen Sicherheitsanforderungen von Bedeutung sein, weil er technische Maßnahmen mit den wesentlichen Anforderungen des CRA verknüpft.

Für die Praxis bedeutet dies: Wer heute mit der CRA-Umsetzung beginnt, sollte nicht auf die endgültige Veröffentlichung aller harmonisierten Normen warten. Die Grundrichtung ist bereits erkennbar: risikobasierte Entwicklung, Security by Design, Security by Default, Schwachstellenmanagement, sichere Updates, nachvollziehbare technische Dokumentation und klare Benutzerinformationen.

Hinweis: Stand Juni 2026 sind aus der EN 40000er Reihe bereits einige Normen als Entwurf erhältlich. Wichtig dabei ist jedoch zu wissen, dass in diesem Status der Norm immer noch weitreichende technische Anpassungen vorgenommen werden können und der nächste Entwurf andere Vorgaben macht als der jetzige.

6.3 Bereits vorhandene Normen mit Relevanz für den Maschinenbau

Auch wenn CRA-spezifische harmonisierte Normen noch im Aufbau sind, gibt es bereits mehrere Normen und Normenreihen, die für Maschinenbauer fachlich relevant sein können. Sie können helfen, Prozesse und technische Maßnahmen vorzubereiten.

Besonders wichtig ist die EN IEC 62443-Reihe. Sie behandelt Cybersecurity für industrielle Automatisierungs- und Steuerungssysteme und ist damit für Maschinenbau, Anlagenbau, Robotik, Prozessautomation und vernetzte Produktionsanlagen besonders naheliegend. Die Reihe adressiert nicht nur technische Anforderungen, sondern auch Rollen, Prozesse, Sicherheitskonzepte, Zonen, Kommunikationsverbindungen, Produktentwicklung, Integration, Betrieb, Wartung und Patchmanagement.

Daneben sind Normen zum Schwachstellenmanagement relevant. Hierzu gehört z.B. die ISO/IEC 29147 für Vulnerability Disclosure und ISO/IEC 30111 für Vulnerability Handling. Diese Normen sind für den Aufbau eines Prozesses zur Entgegennahme, Bewertung, Behandlung und Kommunikation von Schwachstellen hilfreich. Gerade vor dem Hintergrund der CRA-Meldepflichten und der Pflicht zur Schwachstellenbehandlung über den Supportzeitraum sind solche Prozesse für Maschinenbauer wichtig.

Für Produkte mit Funkmodulen ist außerdem die Normenreihe EN 18031 relevant. Sie wurde im Zusammenhang mit der Funkanlagenrichtlinie und deren zusätzlichen Cybersecurity-Anforderungen entwickelt. Sie richtet sich nicht speziell an den CRA, zeigt aber, wie technische Cybersecurity-Anforderungen für vernetzte Funkprodukte konkretisiert werden können. Maschinenbauer mit WLAN-, Bluetooth-, Mobilfunk- oder anderen Funkmodulen sollten diese Normenreihe daher zumindest im Blick behalten.

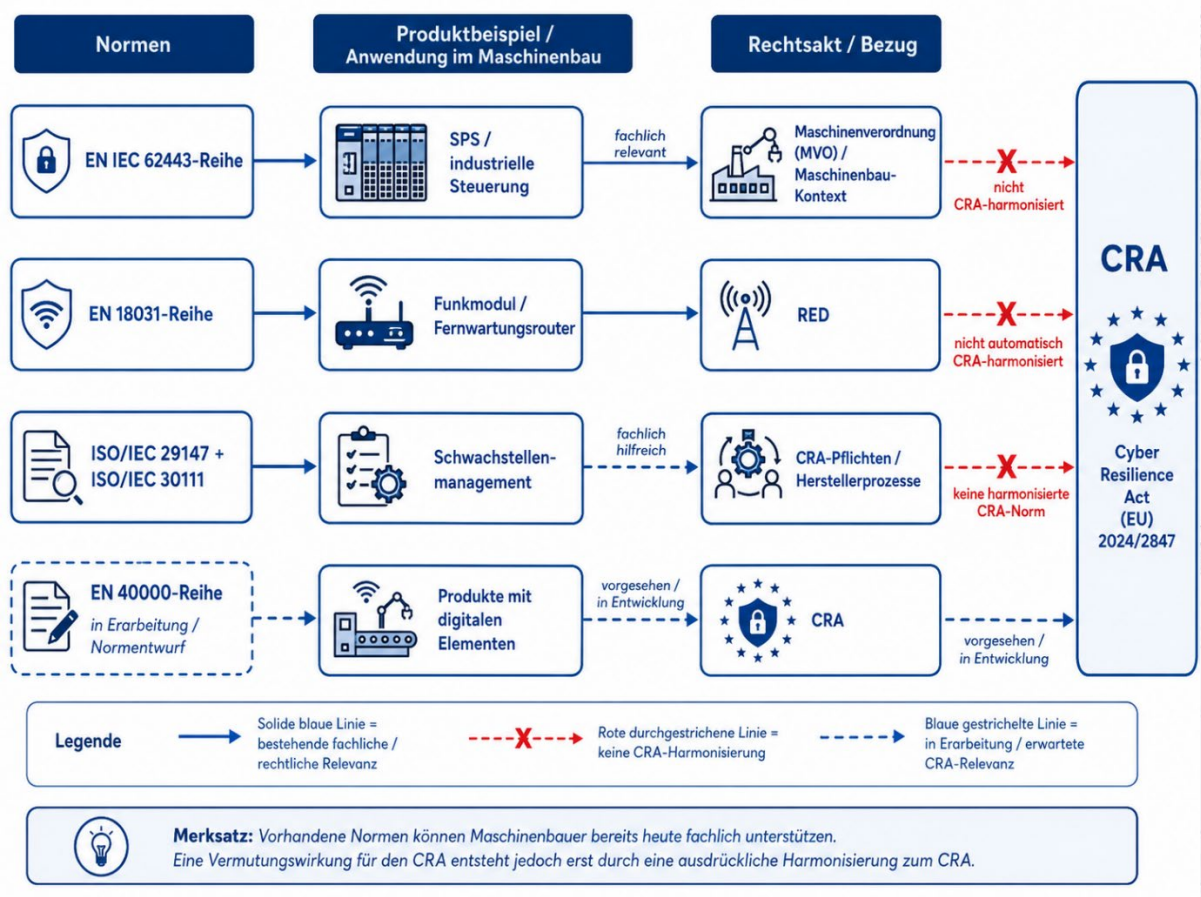


Abb. 6: Normen in Bezug auf den CRA

Für bestimmte Produktarten können außerdem weitere Normen hilfreich sein, z.B. ETSI EN 303 645 für Consumer-IoT-Produkte. Für den klassischen Maschinenbau ist diese Norm meist nicht unmittelbar passend, sie enthält jedoch grundlegende Prinzipien wie den Verzicht auf universelle Standardpasswörter, sichere Updates, Schutz von Kommunikationsschnittstellen und Schwach-stellenmanagement. Solche Prinzipien finden sich in ähnlicher Form auch in CRA-Anforderungen wieder.

Entscheidend ist: Diese Normen können bei der Umsetzung helfen, ersetzen aber nicht automatisch die CRA-Konformitätsbewertung. Solange eine Norm nicht ausdrücklich als harmonisierte Norm zum CRA im Amtsblatt gelistet ist, erzeugt sie keine CRA-Vermutungswirkung. Sie kann aber als technischer Nachweis, als Stand der Technik oder als Grundlage für eine strukturierte Umsetzung herangezogen werden.

6.4 EN IEC 62443 als Normenreihe für industrielle Automatisierung

Für den Maschinenbau ist die EN IEC 62443-Reihe die wichtigste bestehende Normenreihe im Bereich industrieller Cybersecurity. Sie wurde speziell für Industrial Automation and Control Systems, also industrielle Automatisierungs- und Steuerungssysteme, entwickelt. Damit passt sie deutlich besser zur Maschinenbaupraxis als viele rein IT-orientierte Normen.

Die EN IEC 62443-Reihe betrachtet Cybersecurity ganzheitlich. Sie unterscheidet verschiedene Rollen, zum Beispiel Betreiber, Integratoren, Service Provider und Produkthersteller. Außerdem berücksichtigt sie, dass industrielle Automatisierungssysteme andere Rahmenbedingungen haben als klassische Büro-IT. In Produktionsanlagen stehen Verfügbarkeit, Prozessstabilität, Safety, Wartbarkeit, lange Lebensdauer und kontrollierte Änderungen im Vordergrund.

Für Maschinenbauer sind insbesondere folgende Teile und Konzepte der EN IEC 62443-Reihe relevant:

- Security Risk Assessment für industrielle Systeme,
- Zonen- und Conduit-Modell zur Strukturierung von Netzwerken,
- Security Levels als risikobasierte Zielgrößen,
- Anforderungen an Systemarchitektur und Segmentierung,
- Anforderungen an Komponenten,
- sichere Produktentwicklung,
- Anforderungen an Integratoren und Serviceprozesse,
- Patchmanagement in industriellen Umgebungen,
- Remote Access und sichere Wartungszugänge,
- Benutzerverwaltung, Authentifizierung und Zugriffskontrolle,
- Ereignisprotokollierung und Überwachung,
- Backup, Wiederherstellung und Änderungsmanagement.

Gerade das Zonen- und Conduit-Modell ist für Maschinenbauer praktisch hilfreich. Es ermöglicht, eine Maschine oder Anlage nicht als unstrukturierte Ansammlung von Geräten zu betrachten, sondern in Sicherheitszonen zu gliedern. Beispielsweise können SPS, Safety-Steuerung, HMI, Industrie-PC, Fern-wartungsrouter, Robotersteuerung und Unternehmensnetzwerk unterschiedlichen Zonen zugeordnet werden. Die Kommunikation zwischen diesen Zonen erfolgt dann über definierte Verbindungen, die gezielt abgesichert werden können.

Auch die sichere Produktentwicklung nach IEC 62443-4-1 ist für Maschinenbauer relevant. Sie beschreibt Prozesse für Security-Anforderungen, sichere Architektur, sichere Implementierung, Verifikation, Validierung, Schwachstellenbehandlung, Patchmanagement und Produkt-Ende. Diese Themen überschneiden sich deutlich mit den Herstellerpflichten des CRA.

Die EN IEC 62443-Reihe ist damit keine vollständige „CRA-Lösung“, aber sie ist eine gute fachliche Grundlage für Maschinenbauer. Sie hilft insbesondere dort, wo Maschinen aus industriellen Steuerungssystemen, Netzwerken, Kommunikationsschnittstellen und langlebigen Komponenten bestehen.

6.5 EN 18031 und Abgrenzung zur Funkanlagenrichtlinie / RED

Die Normenreihe EN 18031 ist im Zusammenhang mit der Funkanlagenrichtlinie relevant. Sie konkretisiert Cybersecurity-Anforderungen für bestimmte Funkanlagen und wurde zur Unterstützung der Anforderungen aus Artikel 3 Absatz 3 Buchstaben d, e und f der Funkanlagenrichtlinie entwickelt. Diese Anforderungen wurden durch die Delegierte Verordnung (EU) 2022/30 für bestimmte Kategorien von Funkanlagen aktiviert und gelten seit dem 1. August 2025.

Die Normenreihe besteht aus mehreren Teilen:

- EN 18031-1: Common security requirements for internet connected radio equipment,
- EN 18031-2: Common security requirements for radio equipment processing data,
- EN 18031-3: Common security requirements for internet connected radio equipment processing virtual money or monetary value.

Für den Maschinenbau ist vor allem EN 18031-1 relevant, wenn Maschinen oder Maschinenkomponenten über Funktechnik verfügen und internetfähig sind. Das kann zum Beispiel bei WLAN-Modulen, Mobilfunkroutern, drahtlosen Bedieneinheiten, Bluetooth-Schnittstellen, Remote-Service-Routern oder anderen funkbasierten Kommunikationskomponenten relevant werden.

Wichtig ist jedoch die zeitliche Einordnung: Die RED-Cybersecurity-Anforderungen nach der Delegierten Verordnung (EU) 2022/30 gelten für betroffene Funkanlagen in der Übergangsphase vom 1. August 2025 bis zum 10. Dezember 2027. Ab dem 11. Dezember 2027 wird die Delegierte Verordnung (EU) 2022/30 aufgehoben. Grund hierfür ist, dass der Cyber Resilience Act ab diesem Datum vollständig anwendbar ist und die wesentlichen Cybersecurity-Anforderungen des CRA die entsprechenden RED-Cybersecurity-Anforderungen inhaltlich abdecken. Damit soll eine Doppelregulierung vermieden und Rechtssicherheit geschaffen werden.

Für Maschinenbauer bedeutet dies:
Bis zum 10. Dezember 2027 ist bei betroffenen Funkanlagen weiterhin zu prüfen, ob die Funkanlagenrichtlinie einschließlich der durch die Delegierte Verordnung (EU) 2022/30 aktivierten Cybersecurity-Anforderungen anwendbar ist. In diesem Zeitraum kann EN 18031 eine wichtige Rolle für den Nachweis der RED-Konformität spielen.

Ab dem 11. Dezember 2027 verschiebt sich die produktbezogene Cybersecurity-Betrachtung für Produkte mit digitalen Elementen grundsätzlich in den CRA. Für Produkte, die ab diesem Datum in Verkehr gebracht werden und in den Anwendungsbereich des CRA fallen, sind die CRA-Anforderungen maßgeblich. Eine dauerhafte doppelte Anwendung der RED-Cybersecurity-Anforderungen und der CRA-Anforderungen ist gerade nicht vorgesehen.

Die Funkanlagenrichtlinie bleibt für Funkanlagen weiterhin relevant, zum Beispiel für funktechnische Anforderungen, elektromagnetische Verträglichkeit und sichere Nutzung des Funkspektrums. Die speziell durch die Delegierte Verordnung (EU) 2022/30 aktivierten Cybersecurity-Anforderungen werden jedoch mit Wirkung zum 11. Dezember 2027 aufgehoben und durch das CRA-Regime abgelöst.

Für die Praxis ergibt sich daraus eine zweistufige Betrachtung:

1. Für Funkanlagen, die zwischen dem 1. August 2025 und dem 10. Dezember 2027 in Verkehr gebracht werden, sind die RED-Cybersecurity-Anforderungen zu beachten. EN 18031 kann in diesem Zeitraum als harmonisierte Norm zur RED-Konformität herangezogen werden.
2. Für Produkte mit digitalen Elementen, die ab dem 11. Dezember 2027 in Verkehr gebracht werden, ist die CRA-Konformität maßgeblich. EN 18031 kann fachlich weiterhin hilfreich sein, erzeugt aber nicht automatisch eine Vermutungswirkung für den CRA, solange sie nicht ausdrücklich als harmonisierte Norm zum CRA gelistet ist.

Für Maschinenbauer mit Funkkomponenten ist daher ein geordneter Übergang wichtig. Bestehende EN-18031-Bewertungen können eine wertvolle technische Grundlage für die spätere CRA-Bewertung bilden. Sie ersetzen jedoch nicht automatisch die CRA-spezifischen Anforderungen, insbesondere nicht die Pflichten zu Schwachstellenmanagement, Supportzeitraum, Sicherheitsupdates, technischer Dokumentation, Meldepflichten und Benutzerinformationen.

6.6 Welche Normen durch den CRA noch zu erwarten sind

Durch den CRA sind mehrere Gruppen neuer oder angepasster Normen zu erwarten. Die wichtigste Gruppe bilden die horizontalen Normen. Sie sollen für nahezu alle Produkte mit digitalen Elementen anwendbar sein und grundlegende Anforderungen an Cyberresilienz, Risikobewertung, Schwachstellenmanagement und generische Sicherheitsmaßnahmen beschreiben.

Dazu gehören insbesondere Normen zu folgenden Themen:

- Begriffe und Definitionen,
- Grundprinzipien der Cyberresilienz,
- risikobasierte Produktentwicklung,
- Security by Design,
- Security by Default,
- generische Sicherheitsanforderungen,
- Schwachstellenbehandlung,
- koordinierte Offenlegung von Schwachstellen,
- Bedrohungen und Sicherheitsziele,
- technische Dokumentation und Nachweisführung.

Daneben sind vertikale bzw. produktspezifische Normen zu erwarten. Diese betreffen Produktgruppen, die im CRA besonders hervorgehoben werden, zum Beispiel wichtige oder kritische Produkte mit digitalen Elementen. Dazu können u.a. Betriebssysteme, Netzwerkmanagementsysteme, VPN-Produkte, Router, Firewalls, SIEM-Systeme, physische und virtuelle Netzwerkschnittstellen oder andere IT- und OT-Komponenten gehören.

Für den Maschinenbau ist besonders relevant, dass es voraussichtlich nicht nur allgemeine IT-Normen geben wird. Die Normung berücksichtigt ausdrücklich auch industrielle Automatisierung und Steuerungstechnik. Hier ist zu erwarten, dass bestehende Konzepte der EN IEC 62443-Reihe aufgegriffen und für CRA-relevante Produktgruppen nutzbar gemacht werden.

Ob künftig auch eigenständige CRA-Normen speziell für Maschinen entstehen, bleibt abzuwarten. Naheliegend ist jedoch, dass Maschinenbauer zunächst mit horizontalen CRA-Normen, EN IEC 62443-basierten OT-Normen und produktspezifischen Normen für einzelne digitale Komponenten arbeiten werden. Für eine typische Maschine kann daher eine Kombination mehrerer Normen relevant werden.

6.7 Horizontale Normen vs. vertikale / produktspezifische Normen

Für das Verständnis der CRA-Normung ist die Unterscheidung zwischen horizontalen und vertikalen Normen besonders wichtig.

Horizontale Normen sind produktübergreifend. Sie geben allgemeine Anforderungen und Prozesse vor, die für viele verschiedene Produkte mit digitalen Elementen gelten. Für Maschinenbauer können solche Normen die Grundlage für einen unternehmensweiten CRA-Prozess bilden. Sie helfen zum Beispiel bei der Strukturierung der Cybersecurity-Risikobewertung, beim Schwachstellenmanagement, bei generischen Sicherheitsanforderungen und bei der technischen Dokumentation.

Vertikale oder produktspezifische Normen beziehen sich dagegen auf bestimmte Produktgruppen. Sie berücksichtigen die Besonderheiten eines konkreten Produkttyps und können dadurch deutlich präzisere technische Anforderungen enthalten. Beispiele können Normen für Betriebssysteme, Router, VPN-Produkte, Netzwerkmanagementsysteme oder andere im CRA besonders geregelte Produktarten sein.

Eine Maschine besteht häufig aus einer Kombination unterschiedlicher digitaler Elemente. Deshalb wird für Maschinenbauer in der Praxis oft eine Kombination aus horizontalen und vertikalen Normen erforderlich sein. Die horizontale Norm liefert den allgemeinen Rahmen. Vertikale Normen können für bestimmte Komponenten oder Funktionen ergänzend relevant sein.

Beispiel: Eine vernetzte Maschine mit SPS, HMI, Industrie-PC, Fernwartungsrouter und Robotersteuerung kann grundsätzlich anhand horizontaler CRA-Normen bewertet werden. Für den Fernwartungsrouter oder VPN-Zugang können zusätzlich produktspezifische Anforderungen relevant sein. Für die industrielle Steuerungsarchitektur kann die EN IEC 62443-Reihe herangezogen werden. Für ein Funkmodul kann zusätzlich EN 18031 im Rahmen der RED relevant sein.

Diese Kombination macht deutlich: CRA-Normung wird im Maschinenbau nicht immer aus „einer Norm für eine Maschine“ bestehen. Wahrscheinlicher ist ein normativer Baukasten, bei dem horizontale Produktanforderungen, industrielle OT-Security-Normen und produktspezifische Normen zusammengeführt werden müssen.

6.8 Relevanz von CLC/TC 65X WG 3 für industrielle Automatisierung

Für Maschinenbauer ist CLC/TC 65X WG 3 besonders relevant, weil dieses Gremium im Bereich industrieller Prozessmess-, Steuerungs- und Automatisierungstechnik arbeitet und die Verbindung zur bereits genannten EN IEC 62443-Reihe herstellt.

Die Bedeutung dieses Gremiums liegt darin, dass CRA-Anforderungen nicht ausschließlich aus der Perspektive klassischer IT-Produkte betrachtet werden dürfen. Industrielle Automatisierungssysteme haben eigene Randbedingungen: lange Lebensdauer, hohe Anforderungen an Verfügbarkeit, enge Verbindung zwischen Steuerungstechnik und Maschinensicherheit, komplexe Integrationsprojekte, viele Drittkomponenten und häufig eingeschränkte Möglichkeiten für automatische Updates.

CLC/TC 65X WG 3 kann dazu beitragen, CRA-Anforderungen für industrielle Automatisierungsprodukte praxisgerecht zu konkretisieren. Besonders relevant sind Security Profiles auf Basis der EN IEC 62443-Reihe. Solche Profile können helfen, Anforderungen für bestimmte Produktgruppen im industriellen Umfeld zu strukturieren, zum Beispiel für Netzwerkkomponenten, VPN-Funktionen, Netzwerkmanagementsysteme oder andere OT-relevante Komponenten.

Für Maschinenbauer ist das deshalb wichtig, weil viele CRA-relevante digitale Elemente nicht aus der klassischen IT stammen, sondern aus der industriellen Automatisierung. Eine SPS, ein HMI, eine Robotersteuerung, ein Fernwartungsrouter oder ein Frequenzumrichter mit Netzwerkschnittstelle muss anders betrachtet werden als ein Consumer-IoT-Gerät oder eine Bürosoftware.

Die Arbeit von CLC/TC 65X WG 3 dürfte daher eine wichtige Brücke zwischen CRA, EN IEC 62443 und Maschinenbaupraxis bilden. Maschinenbauer sollten diese Entwicklung beobachten, insbesondere wenn sie eigene Steuerungskomponenten, Fernwartungslösungen, industrielle Netzwerkkomponenten oder produktnahe Software bereitstellen.

Für die praktische Umsetzung empfiehlt sich bereits heute folgender Ansatz:

1. Bestehende digitale Elemente der Maschine erfassen.
2. Vorhandene Schnittstellen und Kommunikationswege dokumentieren.
3. IEC-/EN-62443 als fachliche Grundlage für industrielle Cybersecurity verwenden.
4. Die Entwicklung der horizontalen CRA-Normen beobachten.
5. Produktspezifische CRA-Normen für relevante Komponenten identifizieren.
6. Lieferanten frühzeitig nach CRA- und IEC-/EN-62443-relevanten Nachweisen fragen.
7. Die technische Dokumentation so aufbauen, dass sie später an harmonisierte CRA-Normen angepasst werden kann.

Damit wird die Normung nicht erst am Ende des CE-Prozesses relevant. Sie sollte bereits in Produktentwicklung, Komponentenwahl, Steuerungsarchitektur und Lieferantenmanagement einfließen.

7 Klassifizierung von Produkten nach CRA

Der Cyber Resilience Act unterscheidet nicht nur danach, ob ein Produkt überhaupt in den Anwendungsbereich fällt. Zusätzlich ist zu prüfen, welcher Produktkategorie es zuzuordnen ist. Diese Klassifizierung ist besonders wichtig, weil sie Einfluss auf das anzuwendende Konformitätsbewertungsverfahren haben kann.

Für Maschinenbauer ist dabei eine wichtige Grundregel zu beachten: Entscheidend ist nicht jede einzelne in der Maschine enthaltene digitale Komponente, sondern die Kernfunktionalität des jeweiligen Produkts mit digitalen Elementen. Ein Produkt wird also nicht allein dadurch zu einem wichtigen oder kritischen Produkt, dass es eine Komponente enthält, die ihrerseits einer wichtigen Produktkategorie zugeordnet werden könnte. Maßgeblich ist, welche Funktion das Produkt als Ganzes auf dem Markt bereitstellt.

Eine Maschine mit Fernwartungsrouter, HMI, SPS, Industrie-PC oder Betriebssystem muss daher sorgfältig betrachtet werden. Die Gesamtmaschine kann ein Produkt mit digitalen Elementen sein und damit unter den CRA fallen. Sie wird aber nicht automatisch zu einem wichtigen Produkt der Klasse I oder II, nur weil sie einen Router, ein Betriebssystem oder eine Netzwerkschnittstelle enthält. Anders kann es aussehen, wenn der Maschinenbauer ein solches Produkt separat bereitstellt oder wenn die Kernfunktion des bereitgestellten Produkts genau einer in den CRA-Anhängen genannten Kategorie entspricht.

Für die Praxis empfiehlt sich eine dreistufige Prüfung:

1. Fällt das Produkt überhaupt in den Anwendungsbereich des CRA?
2. Hat das Produkt die Kernfunktionalität einer wichtigen Produktkategorie nach Anhang III?
3. Hat das Produkt die Kernfunktionalität einer kritischen Produktkategorie nach Anhang IV?

Erst aus dieser Einordnung ergibt sich, ob das Produkt als Standardprodukt mit digitalen Elementen, als wichtiges Produkt der Klasse I, als wichtiges Produkt der Klasse II oder als kritisches Produkt zu behandeln ist.

Für die Klassifizierung wichtiger und kritischer Produkte sind nicht nur die Produktkategorien aus Anhang III und Anhang IV des CRA zu berücksichtigen. Zusätzlich ist die Durchführungsverordnung (EU) 2025/2392 der Kommission vom 28. November 2025 heranzuziehen. Diese konkretisiert die technischen Beschreibungen der Kategorien wichtiger und kritischer Produkte mit digitalen Elementen. Damit wird die bisher teilweise offene Frage präzisiert, wann ein Produkt tatsächlich die Kernfunktionalität einer der in Anhang III oder Anhang IV genannten Produktkategorien besitzt.

Die Durchführungsverordnung ist für die Praxis besonders wichtig, weil die bloße Bezeichnung einer Produktkategorie im CRA häufig noch nicht ausreicht, um eine eindeutige Einstufungsentscheidung zu treffen. Begriffe wie „Betriebssystem“, „VPN-Produkt“, „Router“, „Firewall“, „SIEM-System“, „Netzwerkmanagementsystem“ oder „manipulationssicherer Mikrocontroller“ müssen anhand der technischen Beschreibung geprüft werden. Erst wenn die Kernfunktionalität des konkret bereitgestellten Produkts mit der technischen Beschreibung übereinstimmt, ist das Produkt als wichtiges oder kritisches Produkt im Sinne des CRA einzustufen.

Für Maschinenbauer bedeutet dies: Die Klassifizierung darf nicht allein anhand einer groben Produktbezeichnung erfolgen. Es ist zu prüfen, welche Funktion das Produkt als Ganzes auf dem Markt bereitstellt. Die Integration einer Komponente, die ihrerseits einer wichtigen oder kritischen Produktkategorie entsprechen kann, macht die Gesamtmaschine nicht automatisch zu einem wichtigen oder

kritischen Produkt. Umgekehrt kann ein Produkt auch dann in eine Kategorie fallen, wenn es neben der beschriebenen Kernfunktionalität weitere Nebenfunktionen enthält.

Die Klassifizierungsentscheidung sollte daher künftig ausdrücklich auf folgende Grundlagen gestützt werden:

- Anwendungsbereich des CRA,
- Produktdefinition und digitale Produktgrenze,
- Kernfunktionalität des bereitgestellten Produkts,
- Anhang III CRA für wichtige Produkte Klasse I und Klasse II,
- Anhang IV CRA für kritische Produkte,
- technische Beschreibungen nach Durchführungsverordnung (EU) 2025/2392,
- Begründung, warum eine Kategorie erfüllt oder nicht erfüllt ist.

Damit wird die Klassifizierung belastbarer und besser gegenüber Kunden, Prüfstellen oder Marktüberwachungsbehörden begründbar.

7.1 Standardprodukt mit digitalen Elementen

Der Begriff „Standardprodukt mit digitalen Elementen“ ist kein eigener förmlicher Begriff des CRA, eignet sich aber als praktische Bezeichnung für Produkte, die zwar in den Anwendungsbereich des CRA fallen, jedoch nicht als wichtiges oder kritisches Produkt in den Anhängen III oder IV aufgeführt sind.

Für solche Produkte gelten die allgemeinen Herstellerpflichten des CRA. Dazu gehören insbesondere die Cybersecurity-Risikobewertung, die Umsetzung der wesentlichen Cybersicherheitsanforderungen, Security by Design und Security by Default, Schwachstellenmanagement, Update- und Patch-Prozesse, Benutzerinformationen, technische Dokumentation, EU-Konformitätserklärung und CE-Kennzeichnung.



Abb. 7: Standardprodukte mit digitalen Elementen

Der wesentliche Unterschied zu wichtigen oder kritischen Produkten liegt in der Konformitätsbewertung. Bei Standardprodukten kann der Hersteller grundsätzlich das Verfahren der internen Fertigungskontrolle bzw. internen Kontrolle nutzen. Er bewertet und erklärt also selbst, dass das Produkt und die zugehörigen Herstellerprozesse die Anforderungen des CRA erfüllen.

Für den Maschinenbau dürften viele Maschinen als Standardprodukte mit digitalen Elementen einzustufen sein, sofern sie zwar digitale Elemente und Datenverbindungen enthalten, ihre Kernfunktion aber nicht einer der besonders genannten wichtigen oder kritischen Produktkategorien entspricht.

Diese Produkte können CRA-pflichtig sein, sind aber nicht automatisch wichtige oder kritische Produkte. Trotzdem müssen alle einschlägigen CRA-Anforderungen erfüllt, bewertet und dokumentiert werden.

7.2 Wichtige Produkte Klasse I

Wichtige Produkte mit digitalen Elementen der Klasse I sind Produkte, die nach Anhang III des CRA eine erhöhte Cybersecurity-Relevanz haben. Sie erfüllen typischerweise Funktionen, die für die Cybersicherheit anderer Produkte, Netzwerke oder Dienste wichtig sind, oder sie können bei Manipulation erhebliche negative Auswirkungen verursachen.

Zu den wichtigen Produkten der Klasse I gehören unter anderem:

- Identitätsmanagementsysteme und Privileged-Access-Management-Produkte,
- Authentifizierungs- und Zugriffskontrollleser, einschließlich biometrischer Leser,
- eigenständige und eingebettete Browser,
- Passwortmanager,
- Antiviren- und Antimalware-Software,
- Produkte mit VPN-Funktion,
- Netzwerkmanagementsysteme,
- SIEM-Systeme,
- Bootmanager,
- Software zur Public-Key-Infrastruktur und Zertifikatsausstellung,
- physische und virtuelle Netzwerkschnittstellen,
- Betriebssysteme,
- Router, Modems für die Internetverbindung und Switches,
- Mikroprozessoren, Mikrocontroller, ASICs und FPGAs mit sicherheitsbezogenen Funktionen,
- bestimmte Smart-Home-Produkte, vernetzte Spielzeuge und Wearables.

Für Maschinenbauer sind insbesondere VPN-Produkte, Netzwerkmanagementsysteme, physische und virtuelle Netzwerkschnittstellen, Betriebssysteme, Router, Modems, Switches sowie bestimmte Mikrocontroller oder Mikroprozessoren relevant. Solche Produkte können in Maschinen integriert sein oder als separate Komponenten in Verkehr gebracht werden.

Wichtig ist jedoch die Abgrenzung über die Kernfunktionalität. Eine Maschine, die ein Betriebssystem enthält, wird dadurch nicht automatisch selbst zu einem Betriebssystem im Sinne der Klasse I. Eine Maschine mit integriertem VPN-Router wird dadurch nicht automatisch als Ganzes zu einem VPN-Produkt. Wird der VPN-Router jedoch separat bereitgestellt oder besteht die Kernfunktion des Produkts gerade in

der Bereitstellung eines VPN-Zugangs, kann eine Einstufung als wichtiges Produkt der Klasse I relevant werden.



Abb. 8: Wichtige Produkte der Klasse I

Für Klasse-I-Produkte gilt: Der Hersteller kann unter bestimmten Voraussetzungen weiterhin ein Selbstbewertungsverfahren nutzen, insbesondere wenn einschlägige harmonisierte Normen, gemeinsame Spezifikationen oder anwendbare europäische Cybersecurity-Zertifizierungsschemata vollständig genutzt werden. Fehlen solche Grundlagen oder werden sie nicht bzw. nur teilweise angewendet, ist ein strengeres Konformitätsbewertungsverfahren mit Einbindung einer notifizierten Stelle erforderlich.

7.3 Wichtige Produkte Klasse II

Wichtige Produkte der Klasse II weisen ein höheres Cybersecurity-Risiko auf als Produkte der Klasse I. Der CRA geht davon aus, dass Sicherheitsvorfälle bei diesen Produkten schwerwiegendere negative Auswirkungen haben können, etwa weil sie zentrale Schutzfunktionen bereitstellen oder weil ihre Manipulation weitreichende Folgen für andere Produkte, Netzwerke, Dienste oder Nutzer haben kann.

Zu den wichtigen Produkten der Klasse II gehören nach Anhang III:

- Hypervisoren und Container-Runtime-Systeme, die virtualisierte Ausführung von Betriebssystemen oder ähnlichen Umgebungen unterstützen,
- Firewalls,
- Intrusion-Detection- und Intrusion-Prevention-Systeme,
- manipulationssichere Mikroprozessoren,
- manipulationssichere Mikrocontroller.



Abb. 9: Wichtige Produkte der Klasse II

Für Maschinenbauer können Klasse-II-Produkte insbesondere dann relevant werden, wenn industrielle Firewalls, IDS/IPS-Systeme, Virtualisierungslösungen, Containerumgebungen oder besonders geschützte Sicherheitskomponenten eingesetzt oder separat bereitgestellt werden.

Auch hier gilt: Die Integration einer solchen Komponente macht nicht automatisch die gesamte Maschine zu einem wichtigen Produkt der Klasse II. Eine Maschine mit integrierter industrieller Firewall bleibt in ihrer Kernfunktion zunächst eine Maschine. Die Firewall selbst kann jedoch als Produkt der Klasse II relevant sein, wenn sie separat auf dem Markt bereitgestellt wird oder wenn die Kernfunktion des bereitgestellten Produkts in der Firewall- bzw. Intrusion-Detection-Funktion besteht.

Für Klasse-II-Produkte ist die Konformitätsbewertung strenger als bei Standardprodukten und Klasse-I-Produkten. Der Hersteller des Produkts kann hier nicht ohne Weiteres auf eine reine interne Kontrolle zurückgreifen. Er muss grundsätzlich eine EU-Baumusterprüfung mit anschließender interner Fertigungskontrolle, eine umfassende Qualitätssicherung oder, soweit verfügbar und anwendbar, ein europäisches Cybersecurity-Zertifizierungsschema mit mindestens dem erforderlichen Vertrauensniveau nutzen.

Für Maschinenbauer bedeutet dies vor allem: Werden Klasse-II-Produkte als Komponenten eingesetzt, sollten Lieferantennachweise, Konformitätsbewertungsverfahren, Zertifikate und technische Informationen frühzeitig eingeholt werden. Werden solche Produkte selbst entwickelt oder unter eigenem Namen bereitgestellt, steigt der CRA-Aufwand erheblich.

7.4 Kritische Produkte

Kritische Produkte mit digitalen Elementen sind in Anhang IV des CRA aufgeführt. Sie bilden die höchste Kategorie innerhalb der CRA-Klassifizierung. Zu den kritischen Produkten gehören:

- Hardwaregeräte mit Sicherheitsboxen,
- Smart-Meter-Gateways innerhalb intelligenter Messsysteme sowie andere Geräte für fortgeschrittene Sicherheitszwecke, einschließlich sicherer Kryptoverarbeitung,
- Smartcards oder ähnliche Geräte, einschließlich Secure Elements.



Abb. 10: Beipiele für kritische Produkte

Für den klassischen Maschinenbau wird diese Kategorie in vielen Fällen nicht unmittelbar einschlägig sein. Kritische Produkte betreffen vor allem besonders sicherheitsrelevante Hardware, kryptografische Sicherheitskomponenten, Smart-Meter-Infrastrukturen und vergleichbare Produkte mit hoher Bedeutung für sichere Identitäten, Verschlüsselung oder kritische Abhängigkeiten.

Trotzdem können kritische Produkte im Maschinenbau indirekt relevant werden, zum Beispiel wenn sichere Hardwaremodule, Secure Elements, Smartcards oder kryptografische Spezialkomponenten in Maschinen, Steuerungen, Zugangs- oder Lizenzsysteme integriert werden. In solchen Fällen sollte geprüft werden, ob die Komponente selbst als kritisches Produkt einzustufen ist und welche Nachweise vom Lieferanten erforderlich sind.

Für kritische Produkte kann die Europäische Kommission verlangen, dass ein europäisches Cybersecurity-Zertifikat auf einem bestimmten Vertrauensniveau vorliegt. Soweit kein entsprechendes Zertifizierungsschema oder keine entsprechende Verpflichtung anwendbar ist, greifen die strengeren Konformitätsbewertungsverfahren, die auch für wichtige Produkte der Klasse II vorgesehen sind.

7.5 Bedeutung der Klassifizierung für die Konformitätsbewertung

Die Klassifizierung hat unmittelbaren Einfluss auf die Konformitätsbewertung. Je höher die Einstufung, desto stärker wird die reine Selbstbewertung eingeschränkt und desto eher ist eine notifizierte Stelle oder ein europäisches Cybersecurity-Zertifizierungsschema einzubeziehen.

Vereinfacht lässt sich die Systematik wie folgt beschreiben:
Bei Standardprodukten mit digitalen Elementen kann der Hersteller grundsätzlich die interne Kontrolle nutzen. Er bewertet das Produkt und seine Prozesse selbst, erstellt die technische Dokumentation, führt die Konformitätsbewertung durch, erstellt die EU-Konformitätserklärung und bringt die CE-Kennzeichnung an.

Bei wichtigen Produkten der Klasse I ist eine Selbstbewertung nur unter zusätzlichen Voraussetzungen möglich. Insbesondere müssen harmonisierte Normen, gemeinsame Spezifikationen oder geeignete

europäische Cybersecurity-Zertifizierungsschemata vollständig angewendet werden. Andernfalls muss eine notifizierte Stelle über eine EU-Baumusterprüfung mit anschließender interner Fertigungskontrolle oder über ein Verfahren der umfassenden Qualitätssicherung eingebunden werden.

Bei wichtigen Produkten der Klasse II ist eine reine interne Kontrolle grundsätzlich nicht ausreichend. Hier sind strengere Verfahren erforderlich, insbesondere EU-Baumusterprüfung mit anschließender interner Fertigungskontrolle, umfassende Qualitätssicherung oder ein geeignetes europäisches Cybersecurity-Zertifizierungsschema.

Bei kritischen Produkten kann eine europäische Cybersecurity-Zertifizierung erforderlich werden. Soweit die Voraussetzungen hierfür noch nicht vorliegen, sind ebenfalls die strengeren Verfahren für Produkte der Klasse II maßgeblich.



Abb. 11: Konformitätsbewertungsverfahren nach Produktgruppe

Für Maschinenbauer ist die Klassifizierung daher nicht nur eine theoretische Einordnung. Sie entscheidet darüber, ob der Hersteller seine CRA-Konformität im Wesentlichen selbst erklären kann oder ob externe Stellen, Zertifizierungsschemata und zusätzliche Prüfverfahren erforderlich werden.

Besonders wichtig ist die Dokumentation der Klassifizierungsentscheidung. Der Hersteller sollte nachvollziehbar festhalten:

- welches Produkt mit digitalen Elementen betrachtet wird,
- welche Kernfunktionalität dieses Produkt besitzt,
- ob eine Kategorie aus Anhang III oder IV einschlägig ist,
- ob das Produkt als Standardprodukt, wichtiges Produkt Klasse I, wichtiges Produkt Klasse II oder kritisches Produkt eingestuft wird,
- welche Folgen sich daraus für die Konformitätsbewertung ergeben,
- welche Normen, Spezifikationen, Zertifikate oder Lieferantennachweise herangezogen werden.

Diese Dokumentation sollte Teil der technischen Dokumentation bzw. der CRA-Konformitätsakte sein.

7.6 Was ist bei Maschinen typischerweise zu erwarten?

Für viele Maschinenbauer wird die typische Einordnung voraussichtlich lauten: Die Maschine ist ein Produkt mit digitalen Elementen und fällt daher grundsätzlich unter den CRA, wird aber als Gesamtmaschine nicht automatisch zu einem wichtigen oder kritischen Produkt. In vielen Fällen wird sie daher als Standardprodukt mit digitalen Elementen behandelt werden können.

Das gilt insbesondere für Maschinen, deren Kernfunktion mechanisch, verfahrenstechnisch, handhabungstechnisch oder produktionstechnisch ist und bei denen digitale Elemente der Steuerung, Bedienung, Diagnose, Kommunikation oder Fernwartung dienen.

Typische Beispiele sind:

- eine Verpackungsmaschine mit SPS, HMI und Fernwartung,
- eine Roboterzelle mit Steuerung, HMI und Netzwerkschnittstelle,
- eine Förderanlage mit vernetzter Steuerung,
- eine Montageanlage mit Industrie-PC und Rezepturverwaltung,
- eine Werkzeugmaschine mit digitaler Parametrierung,
- eine Sondermaschine mit OPC-UA-Schnittstelle,
- eine Maschine mit Cloud-Monitoring oder Remote-Diagnose.

Bei solchen Maschinen ist der CRA dennoch ernst zu nehmen. Auch wenn keine Einstufung als wichtiges oder kritisches Produkt vorliegt, gelten die wesentlichen Cybersicherheitsanforderungen, die Herstellerpflichten, die technische Dokumentation, die Benutzerinformationen, das Schwachstellenmanagement und die CE-Konformitätsbewertung.

Besondere Aufmerksamkeit ist erforderlich, wenn Maschinenbauer eigene digitale Produkte oder digitale Teilprodukte separat bereitstellen. Dazu können zum Beispiel eigene Fernwartungslösungen, HMI-Software, Maschinen-Apps, Edge-Devices, Diagnosegeräte, Steuerungskomponenten, Netzwerkmodule, VPN-Lösungen oder Sicherheitskomponenten gehören. In solchen Fällen kann nicht nur die Gesamtmaschine, sondern auch das separat bereitgestellte digitale Produkt klassifiziert werden müssen.

Ein Maschinenbauer sollte daher nicht pauschal sagen: „Unsere Maschinen sind keine wichtigen Produkte.“ Richtig ist vielmehr eine differenzierte Betrachtung:

Die Maschine als Gesamtprodukt wird häufig ein Standardprodukt mit digitalen Elementen sein. Einzelne digitale Komponenten oder separat bereitgestellte Produkte können jedoch in Klasse I, Klasse II oder in seltenen Fällen als kritisch einzustufen sein. Entscheidend ist immer die Kernfunktionalität des konkret bereitgestellten Produkts.

Für die Praxis empfiehlt sich deshalb ein kurzer Klassifizierungsvermerk für jede Maschinenplattform oder Produktfamilie. Dieser Vermerk sollte die digitale Produktgrenze, die Kernfunktionalität, die enthaltenen digitalen Elemente, die relevanten Anhänge des CRA und das gewählte Konformitätsbewertungsverfahren dokumentieren. So lässt sich gegenüber Kunden, Behörden und internen Projektbeteiligten nachvollziehbar begründen, warum eine Maschine als Standardprodukt, wichtiges Produkt oder kritisches Produkt behandelt wird.

8 Konformitätsbewertung und CE-Kennzeichnung

Der Cyber Resilience Act folgt der bekannten Logik des europäischen Produktsicherheitsrechts: Bevor ein Produkt mit digitalen Elementen auf dem Unionsmarkt bereitgestellt wird, muss der Hersteller bewerten, ob die einschlägigen Anforderungen erfüllt sind. Diese Bewertung ist Teil der Konformitätsbewertung. Am Ende stehen die technische Dokumentation, die EU-Konformitätserklärung und die CE-Kennzeichnung.

Für Maschinenbauer ist dieses Prinzip grundsätzlich vertraut. Auch bei Maschinen muss der Hersteller vor dem Inverkehrbringen prüfen, ob alle anwendbaren Anforderungen erfüllt wurden, die technische Dokumentation erstellen, die Betriebsanleitung bereitstellen, die EU-Konformitätserklärung ausstellen und die CE-Kennzeichnung anbringen. Der CRA erweitert diesen bekannten Prozess um die produktbezogene Cybersecurity.

Neu ist dabei vor allem, dass nicht nur das Produkt selbst, sondern auch bestimmte Herstellerprozesse betrachtet werden. Die Konformitätsbewertung bezieht sich daher nicht nur auf den technischen Zustand der Maschine zum Zeitpunkt der Auslieferung, sondern auch auf Prozesse wie Schwachstellenmanagement, Update- und Patch-Management, Supportzeitraum, Benutzerinformation und technische Dokumentation.

8.1 Interne Fertigungskontrolle / Selbstbewertung

Für viele Produkte mit digitalen Elementen ist die interne Fertigungskontrolle das zentrale Konformitätsbewertungsverfahren. Dieses Verfahren entspricht im Grundsatz einer Selbstbewertung durch den Hersteller. Der Hersteller prüft selbst, ob das Produkt und die von ihm eingerichteten Prozesse die wesentlichen Cybersicherheitsanforderungen des CRA erfüllen.

Die interne Fertigungskontrolle ist insbesondere für sogenannte Standardprodukte mit digitalen Elementen relevant. Damit sind Produkte gemeint, die zwar unter den CRA fallen, aber nicht als wichtige Produkte der Klasse I oder II nach Anhang III und nicht als kritische Produkte nach Anhang IV einzustufen sind.

Für den Maschinenbau dürfte dieses Verfahren in vielen Fällen der Regelfall sein. Eine vernetzte Maschine mit SPS, HMI, Industrie-PC, Robotersteuerung, OPC-UA-Schnittstelle oder Fernwartungszugang kann zwar ein Produkt mit digitalen Elementen sein. Sie wird aber nicht automatisch zu einem wichtigen oder kritischen Produkt, solange ihre Kernfunktionalität nicht einer der besonders geregelten Produktkategorien des CRA entspricht.

Bei der internen Fertigungskontrolle muss der Hersteller unter anderem sicherstellen, dass:

- das Produkt die wesentlichen Cybersicherheitsanforderungen erfüllt,
- eine Cybersecurity-Risikobewertung durchgeführt wurde,
- geeignete Maßnahmen nach dem Stand der Technik umgesetzt wurden,
- die Herstellerprozesse zur Schwachstellenbehandlung eingerichtet sind,
- Sicherheitsupdates und Minderungsmaßnahmen bereitgestellt werden können,
- der Supportzeitraum festgelegt und kommuniziert wurde,
- die Benutzerinformationen vollständig und verständlich sind,
- die technische Dokumentation erstellt wurde,
- die EU-Konformitätserklärung ausgestellt wird,
- die CE-Kennzeichnung korrekt angebracht wird.

Die Selbstbewertung darf nicht mit einer bloßen Selbsterklärung ohne Nachweise verwechselt werden. Der Hersteller muss die Bewertung nachvollziehbar dokumentieren und gegenüber Marktüberwachungsbehörden belegen können, wie die Anforderungen erfüllt wurden. Die interne Fertigungskontrolle setzt daher eine belastbare techn. Dokumentation und nachvollziehbare Entscheidungsgrundlagen voraus.

Für Maschinenbauer bietet dieses Verfahren den Vorteil, dass es gut in bestehende CE-Prozesse integriert werden kann. Die Cybersecurity-Bewertung kann als zusätzlicher Bestandteil der technischen Dokumentation geführt werden. Voraussetzung ist jedoch, dass die eigenen Prozesse, Lieferanteninformationen, Softwarestände, Schnittstellen, Updates und Benutzerinformationen systematisch erfasst und bewertet werden.

8.2 Wann eine notifizierte Stelle erforderlich wird

Eine notifizierte Stelle wird nicht für jedes Produkt mit digitalen Elementen automatisch erforderlich. Ob eine externe Konformitätsbewertungsstelle einzubinden ist, hängt insbesondere von der Produktklassifizierung und vom gewählten Konformitätsbewertungsverfahren ab.

Bei Standardprodukten mit digitalen Elementen kann der Hersteller grundsätzlich die interne Fertigungskontrolle anwenden. Eine notifizierte Stelle ist hier im Regelfall nicht erforderlich.

Bei wichtigen Produkten der Klasse I ist die Situation differenzierter. Eine Selbstbewertung kann möglich sein, wenn einschlägige harmonisierte Normen, gemeinsame Spezifikationen oder geeignete europäische Cybersecurity-Zertifizierungsschemata vollständig angewendet werden. Fehlen solche Grundlagen oder werden sie nur teilweise angewendet, muss der Hersteller auf ein strengeres Verfahren ausweichen. Dann kann die Einbindung einer notifizierten Stelle erforderlich werden, zum Beispiel im Rahmen einer EU-Baumusterprüfung oder eines Verfahrens der umfassenden Qualitätssicherung.

Bei wichtigen Produkten der Klasse II ist eine reine interne Fertigungskontrolle grundsätzlich nicht ausreichend. Hier sind strengere Verfahren vorgesehen. In Betracht kommen insbesondere eine EU-Baumusterprüfung mit anschließender interner Fertigungskontrolle, ein Verfahren der umfassenden Qualitätssicherung oder ein geeignetes europäisches Cybersecurity-Zertifizierungsschema. Wird kein geeignetes Zertifizierungsschema genutzt, ist in der Praxis regelmäßig eine notifizierte Stelle einzubeziehen.

Bei kritischen Produkten kann eine europäische Cybersecurity-Zertifizierung erforderlich werden. Ist ein entsprechendes Zertifizierungsschema vorgesehen, kann dieses den maßgeblichen Nachweis darstellen. Andernfalls kommen ebenfalls die strengeren Verfahren zur Anwendung, wie sie für wichtige Produkte der Klasse II vorgesehen sind.

Für Maschinenbauer ist besonders wichtig: Die Integration einer Klasse-I-, Klasse-II- oder kritischen Komponente in eine Maschine macht die Gesamtmaschine nicht automatisch selbst zu einem Produkt dieser Kategorie. Maßgeblich bleibt die Kernfunktionalität des konkret bereitgestellten Produkts. Wird jedoch eine solche Komponente separat bereitgestellt oder unter eigenem Namen vertrieben, kann für diese Komponente ein eigenes Konformitätsbewertungsverfahren erforderlich sein.

Praktisch bedeutet dies: Maschinenbauer sollten frühzeitig prüfen, ob sie nur Standardmaschinen mit digitalen Elementen bereitstellen oder ob einzelne eigene Produkte, Softwaretools, Fernwartungslösungen, Netzwerkkomponenten oder Sicherheitskomponenten in eine höhere CRA-Kategorie fallen

können. Diese Entscheidung sollte dokumentiert und mit der Konformitätsbewertungsstrategie verknüpft werden.

8.3 Zusammenhang mit harmonisierten Normen

Harmonisierte Normen spielen bei der Konformitätsbewertung eine zentrale Rolle. Sie konkretisieren die gesetzlichen Anforderungen und können eine Vermutungswirkung auslösen. Wenn eine harmonisierte Norm im Amtsblatt der Europäischen Union zum CRA gelistet ist und korrekt angewendet wird, darf der Hersteller grundsätzlich davon ausgehen, dass die von der Norm abgedeckten Anforderungen erfüllt sind.

Diese Vermutungswirkung ist für Maschinenbauer aus anderen CE-Bereichen bekannt. Auch bei der Maschinensicherheit erleichtern harmonisierte Normen den Nachweis, dass grundlegende Anforderungen erfüllt wurden. Beim CRA wird dieses Prinzip auf die wesentlichen Cybersicherheitsanforderungen übertragen.

Für die Konformitätsbewertung hat dies mehrere praktische Auswirkungen. Erstens erleichtern harmonisierte Normen die technische Bewertung, weil sie abstrakte Anforderungen in konkrete Maßnahmen, Prüfungen und Dokumentationspunkte übersetzen. Zweitens können sie den Aufwand für die Nachweisführung reduzieren. Drittens können sie bei wichtigen Produkten der Klasse I entscheidend dafür sein, ob eine Selbstbewertung möglich bleibt oder ob eine notifizierte Stelle erforderlich wird.

Wichtig ist jedoch: Die Anwendung einer Norm ersetzt nicht die Pflicht zur Produktbewertung. Der Hersteller muss weiterhin prüfen, ob die Norm für sein Produkt geeignet ist, welche Anforderungen sie abdeckt und welche Anforderungen zusätzlich zu betrachten sind. Eine Norm kann die Cybersecurity-Risikobewertung unterstützen, aber sie nimmt dem Hersteller nicht die Verantwortung für die konkrete Maschine, ihre Schnittstellen, ihre Software und ihre Einsatzbedingungen ab.

Im Maschinenbau wird voraussichtlich eine Kombination verschiedener Normen relevant sein. Horizontale CRA-Normen können allgemeine Anforderungen an Produkte mit digitalen Elementen abdecken. Die EN IEC 62443-Reihe kann für industrielle Automatisierungs- und Steuerungssysteme herangezogen werden. Für Funkkomponenten können zusätzlich RED-relevante Normen wie EN 18031 von Bedeutung sein. Produktspezifische Normen können für bestimmte digitale Komponenten oder Teilprodukte ergänzend erforderlich werden.

Solange eine Norm jedoch nicht ausdrücklich als harmonisierte Norm zum CRA gelistet ist, erzeugt sie keine formale Vermutungswirkung für den CRA. Sie kann aber dennoch als Stand der Technik, als fachliche Grundlage und als technischer Nachweis in der Konformitätsbewertung genutzt werden.

8.4 Erweiterung der technischen Dokumentation

Der CRA führt zu einer deutlichen Erweiterung der technischen Dokumentation. Neben den klassischen Unterlagen zur Maschine müssen künftig auch cyberbezogene Nachweise aufgenommen werden. Die technische Dokumentation muss zeigen, mit welchen Mitteln der Hersteller sicherstellt, dass das Produkt mit digitalen Elementen und die von ihm eingerichteten Prozesse die wesentlichen Cybersicherheitsanforderungen erfüllen.

Für Maschinenbauer bedeutet dies, dass die technische Dokumentation nicht nur um ein einzelnes zusätzliches Dokument ergänzt werden sollte. Vielmehr muss die CRA-Dokumentation mit der bestehenden CE-Dokumentation verknüpft werden. Die Beschreibung der Maschine, die Steuerungsarchitektur, die Risikobeurteilung, die funktionale Sicherheit, die Betriebsanleitung, die Softwarestände, die Schnittstellen und die Cybersecurity-Bewertung müssen zusammenpassen.

Typische Inhalte der erweiterten technischen Dokumentation sind:

- Beschreibung des Produkts mit digitalen Elementen,
- Abgrenzung der digitalen Produktgrenze,
- Übersicht über digitale Hardware-, Software- und Firmwarebestandteile,
- Beschreibung der Schnittstellen und Datenverbindungen,
- Cybersecurity-Risikobewertung,
- angewandte harmonisierte Normen, Spezifikationen oder technische Regeln,
- Beschreibung der umgesetzten Cybersecurity-Maßnahmen,
- Begründung nicht anwendbarer Anforderungen,
- Nachweise zu Security by Design und Security by Default,
- Beschreibung des Schwachstellenmanagements,
- Update- und Patchkonzept,
- Supportzeitraum und dessen Begründung,
- Benutzerinformationen und sicherheitsrelevante Hinweise,
- Lieferanteninformationen und Software-/Komponentenverzeichnis,
- Nachweise zur Konformitätsbewertung,
- EU-Konformitätserklärung.

Die technische Dokumentation muss vor dem Inverkehrbringen erstellt werden. Gleichzeitig ist sie beim CRA stärker lebenszyklusbezogen als in vielen klassischen CE-Prozessen. Sie muss bei Bedarf während des Supportzeitraums aktualisiert werden, zum Beispiel wenn neue Schwachstellen bekannt werden, Sicherheitsupdates bereitgestellt werden, Komponenten geändert werden oder sich die Bewertung von Cyberrisiken verändert.

Besonders wichtig ist die Dokumentation nicht anwendbarer Anforderungen. Wenn der Hersteller zu dem Ergebnis kommt, dass bestimmte wesentliche Cybersicherheitsanforderungen für das konkrete Produkt nicht relevant sind, sollte dies nicht einfach weggelassen werden. Die Nichtanwendbarkeit sollte nachvollziehbar begründet werden.

Für Maschinenbauer empfiehlt sich daher eine klare Dokumentationsstruktur. Bewährt wäre zum Beispiel ein eigener CRA-Abschnitt innerhalb der technischen Dokumentation, der auf bestehende Dokumente verweist: Risikobeurteilung, Schaltpläne, Softwareliste, Netzwerktopologie, Benutzerverwaltung, Betriebsanleitung, Updateanweisung, Lieferantennachweise und Serviceprozesse. So entsteht kein isolierter IT-Ordner, sondern eine integrierte CE-Dokumentation.

8.5 Einbindung in bestehende CE-Prozesse im Maschinenbau

Der CRA sollte nicht als vollständig separater Zusatzprozess verstanden werden. Für Maschinenbauer ist es wesentlich effizienter, die neuen Anforderungen in bestehende CE-, Entwicklungs- und Qualitätsprozesse einzubinden.

Der klassische CE-Prozess beginnt mit der Klärung des Anwendungsbereichs und der anwendbaren Rechtsakte. Künftig sollte an dieser Stelle zusätzlich geprüft werden, ob die Maschine ein Produkt mit digitalen Elementen ist und ob der CRA anzuwenden ist. Direkt danach sollte die Klassifizierung erfolgen: Standardprodukt, wichtiges Produkt Klasse I, wichtiges Produkt Klasse II oder kritisches Produkt.

In der Risikobeurteilung nach Maschinenverordnung steht weiterhin die Sicherheit von Personen im Mittelpunkt. Die Cybersecurity-Risikobewertung ergänzt diese Betrachtung. Sie betrachtet, welche Cyberbedrohungen die digitalen Elemente der Maschine betreffen können und welche Auswirkungen daraus auf Verfügbarkeit, Integrität, Vertraulichkeit, Prozessfunktion und ggf. Maschinensicherheit entstehen. Wo Cybersecurity Einfluss auf Safety-Funktionen haben kann, müssen beide Bewertungen miteinander verknüpft werden.

In der Konstruktion und Steuerungstechnik sollten Security by Design und Security by Default als zusätzliche Entwicklungsanforderungen aufgenommen werden. Dazu gehören zum Beispiel Netzwerktrennung, abgesicherte Fernwartung, Benutzerrollen, sichere Passwörter, Updatefähigkeit, Protokollierung, Schutz sicherheitsrelevanter Parameter und Begrenzung unnötiger Schnittstellen.

In der Lieferantenauswahl sollten CRA-relevante Informationen abgefragt werden. Dazu gehören Software- und Firmwarestände, Updatefähigkeit, bekannte Schwachstellen, Supportzeiträume, Sicherheitsfunktionen, Schwachstellenmeldewege und Konformitätsnachweise für digitale Komponenten.

In der Inbetriebnahme sollte geprüft werden, ob die cyberrelevanten Einstellungen dem bewerteten Zustand entsprechen. Dazu gehören zum Beispiel geänderte Initialpasswörter, deaktivierte nicht benötigte Dienste, dokumentierte Netzwerkschnittstellen, geregelte Fernwartung, korrekte Benutzerrollen und freigegebene Softwarestände.

In der Betriebsanleitung sollten die cyberrelevanten Informationen für den Betreiber aufgenommen werden. Der Betreiber muss wissen, wie die Maschine sicher in seine IT- bzw. OT-Umgebung integriert wird, wie Fernwartung freigegeben wird, wie Updates durchgeführt werden, welche Passwortrichtlinien gelten und an wen Schwachstellen gemeldet werden können.

Im Service- und Änderungsmanagement muss verhindert werden, dass die Cyberresilienz nachträglich verschlechtert wird. Softwareupdates, Komponentenwechsel, neue Schnittstellen, Fernwartungsänderungen oder Cloud-Erweiterungen sollten deshalb auch unter CRA-Gesichtspunkten bewertet werden.

Damit entsteht ein integrierter Prozess:

1. Anwendungsbereich und CRA-Relevanz prüfen.
2. Produkt klassifizieren.
3. Konformitätsbewertungsverfahren festlegen.
4. Cybersecurity-Risikobewertung durchführen.
5. technische und organisatorische Maßnahmen definieren.
6. Lieferanteninformationen und Softwarestände erfassen.
7. Maßnahmen in Konstruktion, Steuerung und Software umsetzen.

8. Update-, Patch- und Schwachstellenprozesse festlegen.
9. Benutzerinformationen und Betriebsanleitung ergänzen.
10. technische Dokumentation erstellen und verknüpfen.
11. EU-Konformitätserklärung und CE-Kennzeichnung vorbereiten.
12. Änderungen und Schwachstellen während des Supportzeitraums weiterverfolgen.

Für Maschinenbauer liegt der größte Nutzen darin, den CRA nicht als isolierte IT-Compliance-Anforderung zu behandeln. Er sollte als zusätzlicher Baustein des bestehenden CE-Prozesses verstanden werden. So lässt sich Cybersecurity praxisnah mit Maschinensicherheit, funktionaler Sicherheit, Steuerungstechnik, Dokumentation und Service verbinden.

9 Was muss der Maschinenbauer praktisch beachten?

Der Cyber Resilience Act führt nicht nur neue rechtliche Anforderungen ein, sondern verändert auch die praktische Arbeitsweise im Maschinenbau. Cybersecurity muss künftig dort berücksichtigt werden, wo Maschinen geplant, konstruiert, programmiert, beschafft, dokumentiert, ausgeliefert und betreut werden.

Für Maschinenbauer ist dabei entscheidend, das Thema nicht ausschließlich an die IT-Abteilung oder den Betreiber zu delegieren. Der CRA stellt produktbezogene Anforderungen an den Hersteller. Wenn eine Maschine als Produkt mit digitalen Elementen in Verkehr gebracht wird, muss der Hersteller nachweisen können, dass Cybersecurity im Produkt und in den zugehörigen Prozessen angemessen berücksichtigt wurde.

In der Praxis bedeutet dies: Cybersecurity wird zu einem Bestandteil des Entwicklungs-, Konstruktions-, Einkaufs-, Dokumentations- und Serviceprozesses. Viele Anforderungen lassen sich in bestehende CE- und Qualitätsprozesse integrieren. Voraussetzung ist jedoch, dass digitale Elemente, Schnittstellen, Softwarestände, Lieferanteninformationen, Benutzerrollen, Updates und Schwachstellenprozesse systematisch erfasst und bewertet werden.

9.1 Frühe Einbindung der Cybersecurity in die Konstruktion

Cybersecurity sollte bereits zu Beginn eines Maschinenprojekts berücksichtigt werden. Wird das Thema erst kurz vor Auslieferung oder im Rahmen der finalen CE-Dokumentation betrachtet, sind wirksame Maßnahmen häufig nur noch mit erheblichem Aufwand möglich.

Bereits in der Konzept- und Konstruktionsphase sollte daher geklärt werden, welche digitalen Elemente die Maschine enthält, welche Schnittstellen vorgesehen sind und welche Cyberrisiken dadurch entstehen können. Dazu gehören beispielsweise SPS, HMI, Industrie-PC, Robotersteuerung, Safety-Steuerung, Frequenzumrichter mit Netzwerkschnittstelle, Fernwartungsrouter, WLAN- oder Mobilfunkmodule, Kamerasysteme, Sensoren, Cloud-Funktionen, Softwaretools und Updatefunktionen.

Die frühe Einbindung der Cybersecurity hat mehrere Vorteile. Unsichere Architekturentscheidungen können vermieden werden, bevor sie fest im Maschinenkonzept verankert sind. Nicht benötigte Schnittstellen können entfallen. Fernwartung, Benutzerrollen, Passwortkonzept, Netzwerksegmentierung und Updatefähigkeit können konstruktiv mitgedacht werden. Außerdem können Lieferanten bereits frühzeitig nach den erforderlichen Cybersecurity-Informationen gefragt werden.

Für die Praxis empfiehlt es sich, Cybersecurity als festen Punkt in die Projektstart- und Design-Review-Checklisten aufzunehmen. Neben Fragen zur Maschinensicherheit, funktionalen Sicherheit, elektrischen Ausrüstung und Bedienbarkeit sollte daher auch geprüft werden:

- Welche digitalen Elemente sind vorgesehen?
- Welche Datenverbindungen bestehen?
- Welche Schnittstellen sind wirklich erforderlich?
- Welche Fernzugriffe sind geplant?
- Welche Komponenten sind updatefähig?
- Welche Benutzerrollen werden benötigt?
- Welche sicherheitsrelevanten Parameter sind digital zugänglich?
- Welche Lieferanteninformationen werden benötigt?

So wird Cybersecurity nicht zu einem nachträglichen Zusatzthema, sondern Teil des Maschinenkonzepts.

9.2 Festlegung der digitalen Grenzen der Maschine

Ein zentraler praktischer Schritt ist die Festlegung der digitalen Grenzen der Maschine. Im klassischen Maschinenbau werden häufig mechanische, elektrische und sicherheitstechnische Grenzen definiert. Für den CRA muss zusätzlich beschrieben werden, welche digitalen Elemente zur Maschine gehören und wo die Verantwortungsgrenze des Herstellers endet.

Die digitale Grenze beschreibt, welche Hardware, Software, Firmware, Schnittstellen, Kommunikationsverbindungen und ggf. entfernten Datenverarbeitungsfunktionen Bestandteil des Produkts mit digitalen Elementen sind. Diese Abgrenzung ist wichtig für die Cybersecurity-Risikobeurteilung, die technische Dokumentation, die Benutzerinformationen, das Updatekonzept und das Schwachstellenmanagement.

Typische Bestandteile der digitalen Produktgrenze können sein:

- SPS und Steuerungssoftware,
- HMI und Visualisierungssoftware,
- Industrie-PC mit Betriebssystem und Anwendungen,
- Robotersteuerung und Roboterprogramme,
- Safety-Steuerung und sicherheitsrelevante Parametrierung,
- Frequenzumrichter mit Kommunikationsschnittstellen,
- Kamerasysteme und Bildverarbeitungssoftware,
- Fernwartungsrouter und VPN-Zugänge,
- Maschinen-Apps oder Konfigurationstools,
- lokale Datenbanken, Rezepturverwaltung oder Logging-Systeme,
- Cloud- oder Remote-Dienste, soweit sie für Maschinenfunktionen erforderlich sind.

Ebenso wichtig ist die Abgrenzung zur Betreiberumgebung. Das Unternehmensnetzwerk, die IT-Infrastruktur des Betreibers, kundenseitige Firewalls, kundenseitige Benutzerverwaltung oder übergeordnete MES-/ERP-Systeme gehören nicht automatisch zur Maschine. Trotzdem können sie für die sichere Integration der Maschine relevant sein. Der Hersteller sollte daher klar beschreiben, welche Voraussetzungen auf Betreiberseite erforderlich sind.

Eine saubere digitale Grenzdefinition verhindert Missverständnisse. Sie zeigt, welche Bestandteile der Hersteller selbst bewertet und verantwortet, welche Schnittstellen zur Betreiberumgebung bestehen und welche Maßnahmen der Betreiber bei Installation, Betrieb und Wartung beachten muss.

9.3 Schnittstellenanalyse: Ethernet, WLAN, USB, Feldbus, Remote Service

Schnittstellen sind im CRA-Kontext besonders wichtig, weil sie Angriffsflächen eröffnen können. Jede physische oder logische Verbindung zu anderen Geräten, Netzwerken oder Diensten sollte daher systematisch erfasst und bewertet werden.

Im Maschinenbau sind insbesondere folgende Schnittstellen typisch:

- industrielle Feldbusse und Industrial-Ethernet-Systeme,
- Ethernet-Schnittstellen,
- USB-Ports,
- serielle Schnittstellen,
- WLAN,
- Bluetooth,
- Mobilfunk,
- Fernwartungszugänge,
- VPN-Verbindungen,
- OPC UA,
- MQTT,
- Webserver oder Web-HMI,
- Cloud- oder Edge-Anbindungen,
- Service-Tools und Engineering-Schnittstellen,
- Speichermedien und Update-Schnittstellen.

Physische Verbindung: Eine tatsächlich vorhandene technische Verbindung über ein Medium oder eine Schnittstelle. Entscheidend ist, dass über diese Verbindung Daten zwischen der Maschine und einem anderen Gerät, Netzwerk oder Dienst übertragen werden können.

Logische Verbindung: Liegt vor, wenn eine Kommunikation nicht allein durch das Vorhandensein eines Kabels oder Funkmoduls beschrieben wird, sondern durch eine softwarebasierte oder protokollbasierte Verbindung ermöglicht wird. Auch wenn die physische Übertragung zum Beispiel über Ethernet erfolgt, entsteht die eigentliche Angriffsfläche häufig erst durch die darüber laufende logische Verbindung.

Für jede Schnittstelle sollte geklärt werden, wofür sie benötigt wird, wer sie nutzen darf, ob sie im Normalbetrieb aktiv sein muss und welche Schutzmaßnahmen vorgesehen sind. Nicht benötigte Schnittstellen sollten deaktiviert, entfernt oder logisch gesperrt werden. Benötigte Schnittstellen sollten angemessen abgesichert und dokumentiert werden.

Besonders kritisch sind Fernwartungs- und Service-Schnittstellen. Sie ermöglichen häufig einen tiefen Zugriff auf Steuerung, HMI, Programme, Parameter oder Diagnosedaten. Daher sollte klar geregelt sein, ob Fernwartung standardmäßig deaktiviert ist, wie sie freigegeben wird, wer Zugriff erhält, wie die Authentifizierung erfolgt, ob Zugriffe protokolliert werden und wie der Betreiber den Zugriff kontrollieren kann.

Auch USB-Schnittstellen sollten nicht unterschätzt werden. Sie werden häufig für Updates, Rezepturen, Datensicherung oder Servicezwecke verwendet. Ohne geeignete Vorgaben können darüber Schadsoftware, unautorisierte Softwarestände oder manipulierte Konfigurationsdateien eingebracht werden.

Die Schnittstellenanalyse sollte Teil der technischen Dokumentation sein. Sie kann beispielsweise in Form einer Schnittstellenmatrix, eines Netzwerkplans oder einer digitalen Produktübersicht erfolgen.

9.4 Rollenklärung: Hersteller, Integrator, Importeur, Betreiber

Im Maschinenbau sind häufig mehrere Akteure an einer Maschine oder Anlage beteiligt. Neben dem ursprünglichen Maschinenhersteller können Integratoren, Systemlieferanten, Softwareanbieter, Händler, Importeure, Betreiber und externe Serviceunternehmen beteiligt sein. Für die CRA-Umsetzung ist daher eine klare Rollenklärung erforderlich.

Der Hersteller ist grundsätzlich dafür verantwortlich, dass das von ihm bereitgestellte Produkt mit digitalen Elementen die Anforderungen des CRA erfüllt. Dazu gehört auch, dass digitale Komponenten angemessen ausgewählt, bewertet und dokumentiert werden. Wenn der Maschinenhersteller die Maschine unter eigenem Namen oder eigener Marke in Verkehr bringt, trägt er die entsprechende Herstellerverantwortung.

Ein Integrator kann ebenfalls Herstellerpflichten auslösen, wenn er aus mehreren Komponenten eine neue Maschine oder ein neues Produkt mit digitalen Elementen erstellt und dieses unter eigener Verantwortung bereitstellt. Besonders relevant ist dies bei Sondermaschinen, Roboterzellen, Retrofit-Projekten, Linienintegration oder bei der Kombination mehrerer digitaler Komponenten zu einem neuen Gesamtsystem.

Importeure und Händler haben eigene Pflichten, wenn sie Produkte mit digitalen Elementen aus Drittstaaten auf dem EU-Markt bereitstellen oder vertreiben. Für Maschinenbauer ist dies insbesondere dann relevant, wenn Maschinen, Steuerungen, Fernwartungsrouter oder Softwareprodukte aus Nicht-EU-Ländern bezogen und in der EU bereitgestellt werden.

Der Betreiber ist nicht Adressat der Herstellerpflichten des CRA, hat aber eine wichtige Rolle beim sicheren Betrieb. Er muss die Maschine entsprechend den Benutzerinformationen, Netzwerkanforderungen, Passwortvorgaben, Updatehinweisen und organisatorischen Vorgaben betreiben. Der Hersteller muss daher die notwendigen Informationen bereitstellen, damit der Betreiber diese Rolle erfüllen kann.

In Projekten mit mehreren Beteiligten sollte frühzeitig geregelt werden:

- Wer bringt welches Produkt mit digitalen Elementen in Verkehr?
- Wer ist Hersteller der Gesamtmaschine?
- Wer verantwortet Software, Fernwartung und Cloud-Funktionen?
- Wer pflegt Updates und Schwachstelleninformationen?
- Wer informiert den Betreiber bei Sicherheitsproblemen?
- Wer bewertet Änderungen nach der Auslieferung?
- Wer ist Ansprechpartner für Schwachstellenmeldungen?

Ohne klare Rollenklärung besteht das Risiko, dass wichtige CRA-Pflichten zwischen Hersteller, Integrator, Lieferant und Betreiber ungeklärt bleiben.

9.5 Umgang mit Zukaufkomponenten

Maschinenbauer entwickeln digitale Komponenten meist nicht vollständig selbst. SPS, HMI, Industrie-PCs, Robotersteuerungen, Frequenzumrichter, Fernwartungsrouter, Betriebssysteme, Softwarebibliotheken, Kamerasysteme und Kommunikationsmodule stammen häufig von externen Lieferanten. Trotzdem muss der Hersteller der Gesamtmaschine bewerten, ob diese Komponenten die Cybersecurity der Maschine beeinflussen.

Der Umgang mit Zukaufkomponenten wird daher zu einem zentralen Bestandteil der CRA-Umsetzung. Der Maschinenbauer sollte nicht nur technische Datenblätter und elektrische Schnittstellen betrachten, sondern auch Cybersecurity-Informationen vom Lieferanten einholen.

Wichtige Lieferanteninformationen sind zum Beispiel:

- Produkt- und Softwareversionen,
- Firmwarestände,
- Betriebssysteme und relevante Softwarebestandteile,
- bekannte Schwachstellen,
- Update- und Patchmöglichkeiten,
- Supportzeitraum des Lieferanten,
- sichere Standardkonfiguration,
- Passwort- und Benutzerkonzept,
- Kommunikationsschnittstellen und Protokolle,
- Dokumentation zu Sicherheitsfunktionen,
- Kontaktstelle für Schwachstellenmeldungen,
- vorhandene Konformitätsnachweise oder Zertifikate.



Abb. 12: Information, die ein Integrator von seinen Lieferanten einholen sollte

Für die Praxis empfiehlt sich ein digitales Komponentenverzeichnis. Dieses sollte nicht nur die Hardware aufführen, sondern auch Software, Firmware, Betriebssysteme, Versionen und Lieferanteninformationen enthalten. Nur so kann der Maschinenbauer später prüfen, ob eine bekannte Schwachstelle eine von ihm gelieferte Maschine oder Maschinenserie betrifft.

Cybersecurity sollte außerdem Bestandteil der Lieferantenbewertung werden. Ein Lieferant, der keine Informationen zu Updates, Schwachstellen, sicheren Standardkonfigurationen oder Supportzeiträumen bereitstellen kann, kann für CRA-relevante Produkte ein erhebliches Risiko darstellen.

9.6 Anforderungen an Passwörter, Benutzerrollen und Zugriffsschutz

Passwörter, Benutzerrollen und Zugriffsschutz gehören zu den grundlegenden Cybersecurity-Maßnahmen. Im Maschinenbau werden diese Themen jedoch häufig uneinheitlich behandelt. Teilweise existieren allgemeine Standardpasswörter, gemeinsame Servicekonten, unklare Rollen oder dauerhaft aktive Fernzugänge. Solche Praktiken passen nicht zu Security by Design und Security by Default.

Für Maschinenbauer sollte daher ein klares Zugriffskonzept erstellt werden. Dieses Konzept beschreibt, welche Benutzerrollen es gibt, welche Rechte diese Rollen besitzen und wie unbefugter Zugriff verhindert wird.

Typische Rollen können sein:

- Bediener,
- Einrichter,
- Instandhaltung,
- Service,
- Administrator,
- Hersteller-Service,
- externer Fernwartungszugang.

Nicht jede Rolle darf auf alle Funktionen zugreifen. Bediener benötigen beispielsweise keine Rechte zur Änderung sicherheitsrelevanter Parameter oder zur Installation von Software. Servicepersonal benötigt ggf. erweiterte Rechte, diese sollten jedoch kontrolliert, nachvollziehbar und möglichst zeitlich begrenzt sein.

Für Passwörter und Zugangsdaten sollten mindestens folgende Grundsätze gelten:

- keine universellen Standardpasswörter im Auslieferungszustand,
- Änderung initialer Passwörter bei Inbetriebnahme,
- individuelle Zugangsdaten statt gemeinsamer Konten, soweit praktikabel,
- angemessene Passwortkomplexität,
- Schutz von Service- und Administratorkonten,
- sichere Verwaltung von Zugangsdaten,
- Sperrung oder Deaktivierung nicht benötigter Konten,
- dokumentierter Prozess für Passwortverlust oder Rollenänderung.

Bei Fernwartung sollte der Zugriff nur nach Freigabe durch den Betreiber oder autorisiertes Personal möglich sein. Außerdem sollte der Betreiber erkennen können, wann ein Fernzugriff aktiv ist und wie dieser beendet werden kann.

9.7 Logging, Backup, Wiederherstellung und sichere Konfiguration

Cyberresilienz bedeutet nicht nur, Angriffe zu verhindern. Es muss auch möglich sein, sicherheitsrelevante Ereignisse zu erkennen, nachzuvollziehen und nach einem Vorfall einen sicheren Zustand wiederherzustellen. Deshalb sind Logging, Backup, Wiederherstellung und sichere Konfiguration wichtige Praxisbausteine.

Logging dient dazu, relevante Ereignisse zu protokollieren. Im Maschinenbau können dazu beispielsweise gehören:

- fehlgeschlagene und erfolgreiche Anmeldeversuche,
- Änderungen an Benutzerrollen,
- Änderungen an sicherheitsrelevanten Parametern,
- Aktivierung von Fernwartung,
- Software- oder Firmwareupdates,
- Änderung von Netzwerkeinstellungen,
- Einspielen von Rezepturen oder Programmen,
- sicherheitsrelevante Störungen oder Manipulationshinweise.

Nicht jedes Ereignis muss dauerhaft oder detailliert gespeichert werden. Entscheidend ist, dass sicherheitsrelevante Änderungen nachvollziehbar bleiben. Die Protokollierung sollte außerdem so gestaltet sein, dass sie nicht ohne Weiteres durch unbefugte Personen gelöscht oder manipuliert werden kann.

Backups sind wichtig, um nach Fehlkonfigurationen, Datenverlust, Schadsoftware oder Systemausfällen einen funktionsfähigen Zustand wiederherstellen zu können. Für Maschinenbauer sollte festgelegt werden, welche Daten gesichert werden müssen. Dazu können gehören:

- SPS-Programme,
- HMI-Projekte,
- Roboterprogramme,
- Sicherheitsparameter,
- Rezepturen,
- Konfigurationsdateien,
- Netzwerkeinstellungen,
- Benutzer- und Rolleninformationen,
- Lizenz- oder Aktivierungsdaten,
- Prüf- und Produktionsdaten, soweit relevant.

Ebenso wichtig ist die Wiederherstellung. Ein Backup ist nur dann wertvoll, wenn der Wiederherstellungsprozess beschrieben, getestet und für den Betreiber nachvollziehbar ist. Besonders bei sicherheitsrelevanten Parametern muss sichergestellt werden, dass nach einer Wiederherstellung keine unvalidierten oder unsicheren Zustände entstehen.

Die sichere Konfiguration beschreibt den bewerteten und freigegebenen Sollzustand der Maschine. Dieser Zustand sollte dokumentiert werden. Dazu gehören aktive Dienste, offene Ports, Benutzerrollen, Fernwartungseinstellungen, Softwarestände, Netzwerkkonfigurationen und Updatezustand.

9.8 Patchfähigkeit und Update-Konzept

Ein Produkt mit digitalen Elementen muss während des Supportzeitraums angemessen betreut werden können. Dazu gehört ein Konzept, wie Sicherheitsupdates, Patches oder andere Minderungsmaßnahmen bereitgestellt werden. Für Maschinenbauer ist dies besonders anspruchsvoll, weil Updates den Maschinenbetrieb, die Prozessqualität und ggf. sicherheitsbezogene Funktionen beeinflussen können.

Ein Update-Konzept sollte daher nicht nur festlegen, dass Updates möglich sind. Es muss beschreiben, wie Updates kontrolliert, getestet, freigegeben, verteilt, dokumentiert und bei Bedarf rückgängig gemacht werden können.

Wichtige Punkte eines Update-Konzepts sind:

- Welche Komponenten sind updatefähig?
- Welche Updates sind sicherheitsrelevant?
- Wer stellt Updates bereit?
- Wer darf Updates installieren?
- Erfolgt die Installation lokal, remote oder durch Servicepersonal?
- Wie wird die Echtheit und Integrität eines Updates geprüft?
- Wie wird verhindert, dass nicht freigegebene Software installiert wird?
- Wie werden Updates vor der Auslieferung getestet?
- Gibt es einen Rollback- oder Wiederherstellungsprozess?
- Wie werden Betreiber über verfügbare Updates informiert?
- Wie wird dokumentiert, welche Maschine welchen Stand besitzt?

Bei sicherheitsbezogenen Steuerungen ist besondere Vorsicht erforderlich. Änderungen an Firmware, Parametrierung oder Steuerungslogik können Auswirkungen auf validierte Sicherheitsfunktionen haben. In solchen Fällen muss geprüft werden, ob eine erneute Validierung oder eine Aktualisierung der technischen Dokumentation erforderlich ist.

Nicht jede Maschine benötigt automatische Online-Updates. In vielen industriellen Anwendungen können manuell freigegebene Updates, Serviceeinsätze oder kontrollierte Offline-Updates sinnvoller sein. Entscheidend ist, dass der Hersteller ein realistisches und wirksames Verfahren hat, um Schwachstellen während des Supportzeitraums zu behandeln.

9.9 Informationspflichten gegenüber dem Betreiber

Der Betreiber benötigt klare Informationen, um die Maschine sicher und cyberresilient betreiben zu können. Deshalb muss die Betriebsanleitung bzw. Benutzerinformation um cyberrelevante Inhalte ergänzt werden.

Diese Informationen sollten praxisnah und auf die konkrete Maschine zugeschnitten sein. Allgemeine Hinweise wie „Sorgen Sie für IT-Sicherheit“ reichen nicht aus. Der Betreiber muss verstehen, welche

Schnittstellen vorhanden sind, welche Einstellungen sicherheitsrelevant sind, wie Fernwartung genutzt wird, wie Updates durchgeführt werden und welche organisatorischen Maßnahmen erforderlich sind.

Typische Inhalte der Benutzerinformation sind:

- Beschreibung der digitalen Schnittstellen,
- Anforderungen an die Netzwerkintegration,
- Vorgaben zu Benutzerrollen und Passwörtern,
- Hinweise zur sicheren Konfiguration,
- Umgang mit Fernwartung und Remote Service,
- Freigabe und Beendigung von Fernzugriffen,
- Durchführung von Updates und Patches,
- Backup- und Wiederherstellungshinweise,
- Verhalten bei Verdacht auf Cyberangriff oder Manipulation,
- Kontaktstelle für Schwachstellenmeldungen,
- Supportzeitraum und Ende des Supports,
- Hinweise zur sicheren Außerbetriebnahme,
- Hinweise zur Datenlöschung bei Weitergabe oder Entsorgung.

Für Maschinenbauer ist besonders wichtig, die Grenze zwischen Hersteller- und Betreiberverantwortung klar zu beschreiben. Der Hersteller muss die Maschine sicher auslegen und die erforderlichen Informationen bereitstellen. Der Betreiber muss die Maschine entsprechend diesen Vorgaben betreiben, Zugangsdaten schützen, Updates berücksichtigen und die Maschine sicher in seine IT- bzw. OT-Umgebung integrieren.

9.10 Interne Prozesse: Schwachstellenmonitoring, Incident Handling

Der CRA verlangt nicht nur technische Maßnahmen am Produkt, sondern auch interne Herstellerprozesse. Maschinenbauer müssen während des Supportzeitraums in der Lage sein, Schwachstellen zu erkennen, zu bewerten, zu behandeln und ggf. zu melden.

Ein Schwachstellenmonitoring sollte relevante Informationsquellen berücksichtigen. Dazu gehören Lieferantenmeldungen, CERT-Informationen, Schwachstellendatenbanken, Kundenmeldungen, Serviceberichte, interne Tests und externe Sicherheitsmeldungen. Der Hersteller muss bewerten können, ob eine bekannte Schwachstelle eigene Produkte betrifft.

Incident Handling beschreibt den Umgang mit konkreten Sicherheitsvorfällen. Dazu gehört die interne Bewertung, ob eine aktiv ausgenutzte Schwachstelle oder ein schwerwiegender Sicherheitsvorfall vorliegt, welche Sofortmaßnahmen erforderlich sind, ob eine Meldung an zuständige Stellen erforderlich ist und welche Informationen an betroffene Betreiber weiterzugeben sind.

Für die Praxis sollten folgende Punkte festgelegt werden:

- Wer nimmt Schwachstellenmeldungen entgegen?
- Wer bewertet technische Betroffenheit?
- Wer entscheidet über Maßnahmen?
- Wer koordiniert Lieferanteninformationen?
- Wer kommuniziert mit Kunden und Betreibern?

- Wer ist für gesetzliche Meldungen zuständig?
- Wie werden Fristen überwacht?
- Wie werden Entscheidungen dokumentiert?
- Wie werden Updates oder Minderungsmaßnahmen bereitgestellt?

Auch das Supportende muss geplant und kommuniziert werden. Der Hersteller muss festlegen, wie lange Sicherheitsupdates und Schwachstellenbehandlung bereitgestellt werden. Das Ende des Supports sollte dem Betreiber klar mitgeteilt werden, damit dieser rechtzeitig entscheiden kann, ob eine Maschine weiterbetrieben, modernisiert, vom Netzwerk getrennt oder ersetzt werden muss.

Für Maschinenbauer ist das Supportende besonders sensibel, weil Maschinen oft lange genutzt werden. Ein Steuerungssystem kann technisch noch funktionieren, obwohl Betriebssysteme, HMI-Software oder Kommunikationsmodule keinen Sicherheits-Support mehr erhalten. In solchen Fällen muss der Hersteller klar beschreiben, welche Konsequenzen sich daraus ergeben und welche Maßnahmen der Betreiber ergreifen sollte.

Insgesamt zeigt sich: Die praktische Umsetzung des CRA ist kein einmaliges Dokumentationsprojekt. Sie erfordert einen dauerhaften Produktprozess. Dieser Prozess beginnt bei der Konstruktion, umfasst Lieferanten, Software, Schnittstellen, Benutzerinformationen und Service und endet erst mit dem Ende des definierten Supportzeitraums.

10 Schnittstelle zwischen Safety und Security

Im klassischen Maschinenbau wurden Safety und Security lange Zeit getrennt betrachtet. Safety bezieht sich auf den Schutz von Personen vor Gefährdungen, die von einer Maschine ausgehen können. Security bezieht sich dagegen auf den Schutz vor unbefugtem Zugriff, Manipulation, Missbrauch, Schadsoftware, Datenverlust oder Angriffen auf digitale Systeme.

Mit der zunehmenden Vernetzung von Maschinen lässt sich diese Trennung in der Praxis jedoch nicht mehr vollständig aufrechterhalten. Wenn sicherheitsrelevante Steuerungen, Parameter, Programme, Betriebsarten, Fernwartungszugänge oder Diagnosesysteme digital erreichbar sind, kann ein Cyberangriff mittelbar oder unmittelbar Einfluss auf die Maschinensicherheit haben.

Der Cyber Resilience Act adressiert diese Entwicklung aus Sicht der produktbezogenen Cybersecurity. Die Maschinenverordnung betrachtet Cybersecurity dagegen dort, wo sie Auswirkungen auf die Sicherheit von Maschinen haben kann, insbesondere im Zusammenhang mit dem Schutz gegen Manipulation und der Sicherheit und Zuverlässigkeit von Steuerungssystemen. Für Maschinenbauer entsteht damit eine wichtige Schnittstelle: Cybersecurity-Maßnahmen können notwendig sein, um die Integrität sicherheitsrelevanter Maschinenfunktionen zu erhalten.

10.1 Warum Cybersecurity für Maschinensicherheit relevant wird

Maschinen werden zunehmend über digitale Systeme gesteuert, parametriert, überwacht und gewartet. Steuerungen kommunizieren mit HMI-Systemen, Industrie-PCs, Robotersteuerungen, Frequenzumrichtern, Sicherheitssteuerungen, Kamerasystemen, Cloud-Diensten oder übergeordneten Produktionsnetz-

werken. Gleichzeitig werden Fernwartung, Remote-Diagnose, Softwareupdates und digitale Servicefunktionen immer häufiger eingesetzt.

Dadurch entstehen neue Angriffsmöglichkeiten. Ein unbefugter Zugriff auf eine Maschine kann nicht nur Daten oder Verfügbarkeit betreffen, sondern auch Maschinenfunktionen verändern. Werden beispielsweise Bewegungsparameter, Geschwindigkeiten, Sicherheitsgrenzen, Betriebsarten, Programme oder Verriegelungslogiken manipuliert, kann daraus eine sicherheitsrelevante Gefährdung entstehen.

Beispiele für mögliche Safety-Auswirkungen von Security-Problemen sind:

- Veränderung sicherheitsrelevanter Parameter,
- Manipulation von Roboterprogrammen oder Bewegungsbereichen,
- Deaktivierung oder Umgehung von Schutzfunktionen,
- Veränderung von Grenzwerten für Geschwindigkeit, Kraft oder Position,
- unbefugte Aktivierung eines Fernwartungszugangs,
- Installation manipulierter Software oder Firmware,
- Wiederherstellung eines alten, nicht mehr validierten Softwarestands,
- Veränderung von Benutzerrollen oder Zugriffsrechten,
- Manipulation von Diagnose- oder Fehlermeldungen,
- Beeinträchtigung der Verfügbarkeit sicherheitsrelevanter Steuerungskomponenten.

Damit wird Cybersecurity zu einem Bestandteil der technischen Integrität der Maschine. Eine Sicherheitsfunktion kann noch so sorgfältig nach EN ISO 13849-1 ausgelegt und validiert sein: Wenn ihre Parameter, Software oder Schnittstellen ungeschützt verändert werden können, ist ihre praktische Wirksamkeit gefährdet.

Für Maschinenbauer bedeutet dies, dass Cybersecurity nicht nur als Schutz des Betreibernetzwerks verstanden werden darf. Sie ist auch eine Voraussetzung dafür, dass sicherheitsrelevante Funktionen der Maschine während des Betriebs, der Wartung und der späteren Änderung zuverlässig erhalten bleiben.

10.2 Manipulation sicherheitsbezogener Steuerungen

Sicherheitsbezogene Steuerungen spielen im Maschinenbau eine zentrale Rolle. Sie überwachen Not-Halt-Funktionen, Schutztüren, Lichtgitter, Scanner, Zustimmtaster, sichere Geschwindigkeiten, sichere Positionen, sichere Stillstände, sichere Bremsfunktionen oder sicherheitsgerichtete Raumbegrenzungen. Ihre Auslegung, Validierung und Dokumentation erfolgt typischerweise auf Grundlage der funktionalen Sicherheit.

Gleichzeitig sind moderne Sicherheitssteuerungen häufig digital parametrierbar, updatefähig, vernetzbar und über Engineering-Tools zugänglich. Genau dadurch entsteht die Schnittstelle zur Cybersecurity. Wenn sicherheitsrelevante Parameter, Programme oder Konfigurationen unbefugt verändert werden können, kann die Sicherheitsfunktion ihre Wirkung verlieren oder nur noch eingeschränkt erfüllen.

Typische sicherheitsrelevante Manipulationsrisiken sind zum Beispiel:

- Änderung von Sicherheitsparametern,
- Veränderung von Abschaltgrenzen,
- Deaktivierung einzelner Sicherheitsfunktionen,

- Änderung sicherer Geschwindigkeiten oder Positionen,
- Manipulation von Schutztür- oder Lichtgitterlogik,
- Einspielen nicht freigegebener Sicherheitsprogramme,
- Veränderung sicherer Kommunikationsverbindungen,
- Rücksetzen auf alte oder nicht validierte Softwarestände,
- unbefugte Änderung von Quittier- oder Reset-Logiken.

Ein besonderes Risiko besteht darin, dass Manipulationen nicht sofort sichtbar sein müssen. Eine Maschine kann im Normalbetrieb scheinbar funktionieren, obwohl eine sicherheitsrelevante Parametrierung verändert wurde. Die Gefährdung zeigt sich dann erst in einer konkreten Situation, beispielsweise beim Öffnen einer Schutztür, beim Eingriff in einen Arbeitsbereich oder bei einem Fehlerfall.

Deshalb müssen sicherheitsbezogene Steuerungen gegen unbefugte Änderung geschützt werden. Dazu gehören unter anderem rollenbasierte Zugriffsrechte, Schutz von Engineering-Schnittstellen, sichere Verwaltung von Projektdateien, Integritätsprüfung von Programmen, dokumentierte Freigabeprozesse, Protokollierung sicherheitsrelevanter Änderungen und klare Vorgaben für Updates oder Parametrieränderungen.

Für Maschinenbauer ist wichtig: Die funktionale Sicherheit bewertet, ob eine Sicherheitsfunktion bei bestimmungsgemäßer Auslegung und Umsetzung ausreichend zuverlässig wirkt. Cybersecurity muss zusätzlich sicherstellen, dass diese Auslegung nicht unbefugt verändert, manipuliert oder umgangen werden kann.

10.3 Fernwartung und Zugriff auf sicherheitsrelevante Parameter

Fernwartung ist im Maschinenbau weit verbreitet. Sie ermöglicht schnelle Diagnose, Unterstützung bei Störungen, Softwareanpassungen, Parametrierung und Service ohne Vor-Ort-Einsatz. Aus Sicht des CRA ist Fernwartung jedoch eine besonders relevante Schnittstelle, weil sie bewusst einen Zugriff von außen auf die Maschine ermöglicht.

Besonders kritisch wird Fernwartung, wenn über den Remote-Zugang nicht nur Diagnosedaten gelesen, sondern auch Programme, Parameter, Benutzerrechte, Softwarestände oder sicherheitsrelevante Einstellungen verändert werden können. In solchen Fällen kann ein kompromittierter Fernwartungszugang unmittelbare Auswirkungen auf Maschinenfunktion, Verfügbarkeit und Maschinensicherheit haben.

Für Maschinenbauer sollten daher klare Grundsätze gelten:

- Fernwartung sollte nicht dauerhaft und unkontrolliert aktiv sein.
- Der Betreiber sollte Fernzugriffe freigeben und beenden können.
- Fernzugriffe sollten eindeutig authentifiziert und autorisiert werden.
- Zugriffe sollten protokolliert und nachvollziehbar sein.
- Servicezugänge sollten nicht auf gemeinsamen Standardpasswörtern beruhen.
- Zugriff auf sicherheitsrelevante Parameter sollte besonders geschützt sein.
- Änderungen an Sicherheitsprogrammen oder Sicherheitsparametern sollten nur nach definiertem Freigabeprozess erfolgen.
- Nach Änderungen sicherheitsrelevanter Funktionen sollte geprüft werden, ob eine erneute Validierung erforderlich ist.

Eine sinnvolle technische Lösung kann darin bestehen, Fernwartungszugänge funktional zu begrenzen. Nicht jeder Remote-Zugriff muss automatisch Zugriff auf alle Maschinenfunktionen bieten. Es kann unterschiedliche Berechtigungen für Diagnose, Bedienunterstützung, Softwareupdate, Parametrierung und sicherheitsrelevante Konfiguration geben.

Besonders bei sicherheitsbezogenen Steuerungen sollte der Hersteller festlegen, ob und in welchem Umfang eine Fernänderung überhaupt zulässig ist. In vielen Fällen kann es sinnvoll sein, sicherheitsrelevante Änderungen nur lokal, durch autorisierte Personen und mit anschließender Validierung zuzulassen.

Die Betriebsanleitung sollte den Umgang mit Fernwartung klar beschreiben. Der Betreiber muss wissen, wann ein Fernzugriff möglich ist, wer ihn freigeben darf, woran ein aktiver Fernzugriff erkennbar ist, wie er beendet wird und welche Änderungen nur durch qualifiziertes Personal vorgenommen werden dürfen.

10.4 Security als Voraussetzung für die Integrität von Safety-Funktionen

Safety-Funktionen setzen voraus, dass ihre technische Umsetzung unverändert, wirksam und nachvollziehbar bleibt. Genau hier leisten Security-Maßnahmen einen wichtigen Beitrag. Sie schützen nicht nur Daten, sondern auch die Integrität der sicherheitsrelevanten Maschinenkonfiguration.

Eine Sicherheitsfunktion besteht häufig aus Sensorik, Logik, Aktorik, Parametern, Software, Kommunikation und Validierungsnachweisen. Wenn eine dieser Ebenen unbefugt verändert wird, kann die Funktion beeinträchtigt werden. Security-Maßnahmen sollen verhindern, dass solche Veränderungen unkontrolliert erfolgen.

Beispiele für Security-Maßnahmen zur Absicherung von Safety-Funktionen sind:

- Schutz der Engineering-Schnittstellen,
- rollenbasierte Zugriffsbeschränkung für sicherheitsrelevante Parameter,
- Trennung von Bedien-, Service- und Administrationsrechten,
- Integritätsprüfung von Sicherheitsprogrammen,
- Versionsverwaltung von Sicherheitssoftware und Parametrierung,
- Protokollierung sicherheitsrelevanter Änderungen,
- Schutz vor unautorisierten Updates,
- Freigabeprozess für Änderungen an Safety-Funktionen,
- sichere Speicherung von Validierungsständen,
- Netzwerktrennung zwischen Betreiber-IT, Maschinensteuerung und Sicherheitsfunktionen,
- abgesicherte Remote-Service-Prozesse,
- Backup und kontrollierte Wiederherstellung freigegebener Konfigurationen.

Dabei ist wichtig: Security-Maßnahmen ersetzen keine funktionale Sicherheitsbewertung. Eine abgesicherte Sicherheitssteuerung ist nicht automatisch funktional sicher. Umgekehrt ist eine funktional sichere Steuerung nicht automatisch ausreichend gegen Cyberangriffe geschützt. Beide Betrachtungen müssen zusammengeführt werden.

In der technischen Dokumentation sollte daher beschrieben werden, welche sicherheitsrelevanten digitalen Elemente vorhanden sind und wie ihre Integrität geschützt wird. Dazu gehören insbesondere sicher-

heitsbezogene Steuerungsprogramme, Parameter, Kommunikationsverbindungen, Zugriffsrechte, Updatewege und Validierungsstände.

Für Maschinenbauer ist dies ein wichtiger Paradigmenwechsel. Früher wurde häufig angenommen, dass eine validierte Sicherheitsfunktion dauerhaft gültig bleibt, solange keine bewusste technische Änderung vorgenommen wird. Bei vernetzten und updatefähigen Maschinen muss zusätzlich betrachtet werden, ob unbefugte oder unbeabsichtigte digitale Änderungen möglich sind und wie diese verhindert oder erkannt werden.

10.5 Risikobeurteilung nach MVO vs. Cybersecurity Risk Assessment nach CRA

Die Risikobeurteilung nach Maschinenverordnung und das Cybersecurity Risk Assessment nach CRA verfolgen unterschiedliche Ziele. Beide Bewertungen können sich überschneiden, sind aber nicht identisch.

Die Risikobeurteilung nach Maschinenverordnung betrachtet Gefährdungen für Personen, die von der Maschine ausgehen können. Sie fragt zum Beispiel: Welche mechanischen, elektrischen, thermischen, ergonomischen oder steuerungstechnischen Gefährdungen bestehen? Welche Verletzungsschwere ist möglich? Wie häufig sind Personen der Gefährdung ausgesetzt? Können sie die Gefährdung vermeiden? Welche Schutzmaßnahmen sind erforderlich?

Das Cybersecurity Risk Assessment nach CRA betrachtet dagegen Cyberrisiken für ein Produkt mit digitalen Elementen. Es fragt zum Beispiel: Welche digitalen Elemente und Schnittstellen sind vorhanden? Welche Bedrohungen können auf diese wirken? Welche Auswirkungen hätte ein unbefugter Zugriff, eine Manipulation, ein Ausfall, ein Datenverlust oder eine Schwachstelle? Welche Maßnahmen sind erforderlich, um Cyberrisiken zu minimieren, Sicherheitsvorfälle zu verhindern und deren Auswirkungen zu begrenzen?

Die Schnittstelle entsteht dort, wo Cybersecurity-Ereignisse Safety-Auswirkungen haben können. Ein Cyberangriff ist zunächst kein klassischer mechanischer Gefährdungsfaktor. Wenn der Angriff jedoch dazu führen kann, dass eine sicherheitsrelevante Funktion deaktiviert, manipuliert oder unwirksam wird, muss dieser Zusammenhang auch in der Maschinensicherheitsbetrachtung berücksichtigt werden.

Praktisch kann folgende Abgrenzung helfen:

Die Risikobeurteilung nach Maschinenverordnung beantwortet die Frage:
„Welche Gefährdungen können durch die Maschine für Personen entstehen und welche Schutzmaßnahmen sind erforderlich?“

Das Cybersecurity Risk Assessment nach CRA beantwortet die Frage:
„Welche Cyberrisiken bestehen für die digitalen Elemente des Produkts und welche Maßnahmen sind erforderlich, um diese Risiken über den Produktlebenszyklus zu beherrschen?“

Die gemeinsame Schnittstellenfrage lautet:
„Kann ein Cybersecurity-Ereignis dazu führen, dass eine sicherheitsrelevante Maschinenfunktion verändert, beeinträchtigt, deaktiviert oder umgangen wird?“

Wenn diese Frage bejaht wird, müssen Safety und Security gemeinsam betrachtet werden. Die Cybersecurity-Maßnahme dient dann nicht nur dem Schutz digitaler Systeme, sondern auch der Aufrechterhaltung der Wirksamkeit von Safety-Funktionen.

Für Maschinenbauer empfiehlt sich daher ein integrierter Dokumentationsansatz. Die klassische Risikobeurteilung bleibt das zentrale Dokument zur Maschinensicherheit. Das CRA-Cybersecurity Risk Assessment ergänzt diese Bewertung um digitale Bedrohungen, Schnittstellen und Herstellerprozesse. Wo sich beide Bereiche berühren, sollten Verweise hergestellt werden, zum Beispiel bei sicherheitsbezogenen Steuerungen, Fernwartung, Softwareupdates, Sicherheitsparametern, Netzwerkanbindungen und Zugriffsschutz.

Damit entsteht kein doppelter oder widersprüchlicher Prozess. Vielmehr wird die bestehende Safety-Betrachtung um die Frage ergänzt, ob Cybersecurity-Ereignisse die Wirksamkeit sicherheitsrelevanter Maßnahmen beeinflussen können.

11 Lösungsansatz am Beispiel einer einfachen Maschine

Die Anforderungen des Cyber Resilience Act wirken auf den ersten Blick abstrakt. Für Maschinenbauer ist jedoch entscheidend, die Vorgaben in konkrete Arbeitsschritte zu übersetzen. Das folgende Beispiel zeigt, wie eine einfache automatisierte Maschine mit digitalen Elementen pragmatisch bewertet und dokumentiert werden kann.

Das Beispiel erhebt keinen Anspruch auf Vollständigkeit für jede Maschinenart. Es soll vielmehr zeigen, wie Maschinenbauer die CRA-Anforderungen strukturiert in ihre bestehenden Entwicklungs-, CE- und Dokumentationsprozesse integrieren können.

11.1 Beschreibung der Beispielmaschine

Als Beispiel dient eine einfache automatisierte Maschine zur Bearbeitung oder Prüfung von Werkstücken. Die Maschine verfügt über eine SPS zur Ablaufsteuerung, ein HMI zur Bedienung und Parametrierung, eine Ethernet-Schnittstelle zur Einbindung in ein Produktionsnetzwerk, einen USB-Serviceport für Datensicherung und Softwareupdates sowie einen optionalen Fernwartungszugang.

Die Maschine wird als vollständige Maschine durch einen Maschinenbauer auf dem europäischen Markt bereitgestellt. Sie enthält digitale Hardware, Software und Firmware. Außerdem sind Datenverbindungen zu anderen Geräten oder Netzwerken vorgesehen bzw. vernünftigerweise vorhersehbar. Damit ist eine Prüfung des CRA-Anwendungsbereichs erforderlich.

Die Kernfunktion der Maschine besteht jedoch nicht in der Bereitstellung von Cybersecurity-Funktionen, Netzwerkmanagement, VPN-Diensten, Betriebssystemen, Firewalls oder vergleichbaren digitalen Produkten. Die digitale Technik dient vielmehr der Steuerung, Bedienung, Diagnose, Parametrierung und Wartung der Maschine. Die Maschine ist daher in diesem Beispiel als Standardprodukt mit digitalen Elementen zu betrachten, sofern keine besonderen Produktkategorien nach Anhang III oder IV des CRA einschlägig sind.



Abb. 13: Bildlische Darstellung des Maschinenbeispiels

11.2 Digitale Elemente und Schnittstellen der Maschine

Im ersten Schritt werden die digitalen Elemente und Schnittstellen der Maschine erfasst. Diese Übersicht bildet die Grundlage für die weitere Cybersecurity-Risikobewertung und für die technische Dokumentation.

Zur Maschine gehören in diesem Beispiel folgende digitale Elemente:

- SPS mit Steuerungsprogramm,
- HMI mit Bedienoberfläche und Parametrierfunktionen,
- Engineering-Zugang für Service- und Inbetriebnahmetätigkeiten,
- Ethernet-Schnittstelle zur Kommunikation mit dem Produktionsnetzwerk,
- USB-Serviceport für Datensicherung, Rezepturimport oder Softwareupdate,
- optionaler Fernwartungsrouter bzw. VPN-Zugang,
- Rezeptur- oder Parameterspeicher,
- Software- und Firmwarestände der eingesetzten Komponenten,
- Benutzer- und Rollenverwaltung,
- ggf. Diagnose- oder Logging-Funktionen.

Zusätzlich wird festgelegt, welche Schnittstellen vorhanden sind und welchem Zweck sie dienen:

- Ethernet: Maschinenkommunikation, Diagnose, Datenaustausch mit übergeordneten Systemen,
- USB: Service, Backup, Rezepturimport oder Update,
- HMI: Bedienung, Parametrierung, Benutzerverwaltung,
- Engineering-Schnittstelle: Programmierung, Inbetriebnahme, Service,
- Fernwartung: optionaler Zugriff durch autorisiertes Servicepersonal,
- interne Steuerungskommunikation: Kommunikation zwischen SPS, HMI, Antriebstechnik und ggf. weiteren Komponenten.

Diese Übersicht sollte nicht nur in der Konstruktion bekannt sein, sondern als dokumentierte Schnittstellen- und Komponentenliste in die CRA-Dokumentation übernommen werden. Nur wenn bekannt ist, welche digitalen Elemente vorhanden sind, kann später bewertet werden, ob eine Schwachstelle oder ein Update die Maschine betrifft.

11.3 Erste CRA-Einstufung

Die CRA-Einstufung erfolgt in mehreren Schritten.

Zunächst wird geprüft, ob die Maschine ein Produkt mit digitalen Elementen ist. Dies ist im Beispiel zu bejahen, da die Maschine digitale Hardware, Software und Firmware enthält. Außerdem verfügt sie über physische und logische Datenverbindungen, insbesondere Ethernet, USB und optional Fernwartung.

Anschließend wird geprüft, ob die bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte Datenverbindung zu einem Gerät oder Netzwerk umfasst. Auch dies ist zu bejahen. Die Ethernet-Schnittstelle ist für die Einbindung in eine Produktionsumgebung vorgesehen. Der USB-Port wird für Servicezwecke genutzt. Der optionale Fernwartungszugang ermöglicht eine Verbindung von außen.

Im dritten Schritt wird geprüft, ob die Maschine in eine der Kategorien wichtiger Produkte der Klasse I oder Klasse II nach Anhang III oder kritischer Produkte nach Anhang IV fällt. Maßgeblich ist hierbei die Kernfunktionalität des bereitgestellten Produkts. Die Kernfunktion der Maschine liegt in der Bearbeitung, Prüfung oder Handhabung von Werkstücken, nicht in der Bereitstellung einer der genannten Cybersecurity- oder Netzwerkfunktionen.

Die Beispielmaschine wird daher wie folgt eingestuft:

- CRA-Anwendungsbereich: ja,
- Produkt mit digitalen Elementen: ja,
- wichtiges Produkt Klasse I: nein, sofern keine entsprechende Kernfunktion vorliegt,
- wichtiges Produkt Klasse II: nein, sofern keine entsprechende Kernfunktion vorliegt,
- kritisches Produkt: nein,
- Konformitätsbewertungsverfahren: interne Fertigungskontrolle / Selbstbewertung.

Diese Einstufung sollte als kurzer Klassifizierungsvermerk dokumentiert werden. Dabei sollte ausdrücklich festgehalten werden, dass einzelne Komponenten wie Fernwartungsrouter, Betriebssysteme oder Netzwerkschnittstellen relevant sein können, die Gesamtmaschine dadurch aber nicht automatisch zu einem wichtigen oder kritischen Produkt wird. Maßgeblich bleibt die Kernfunktionalität der bereitgestellten Maschine.

11.4 Beispielhafte Cybersecurity-Risikobewertung

Im nächsten Schritt wird eine einfache Cybersecurity-Risikobewertung durchgeführt. Dabei werden typische Bedrohungen betrachtet und geeignete Maßnahmen abgeleitet. Die Bewertung muss zur Maschine, ihren Schnittstellen und ihrem vorgesehenen Einsatz passen.

Für die Beispielmaschine können unter anderem folgende Cyberrisiken betrachtet werden:

Unbefugter Zugriff über das Netzwerk
Über die Ethernet-Schnittstelle könnte ein unbefugter Zugriff auf HMI, SPS oder Diagnosedienste erfolgen. Dadurch könnten Parameter verändert, Daten ausgelesen, Maschinenfunktionen beeinflusst oder die Verfügbarkeit der Maschine beeinträchtigt werden.

Mögliche Maßnahmen:

- Netzwerkzugriff auf erforderliche Dienste begrenzen,
- nicht benötigte Dienste deaktivieren,
- Benutzerrollen und Passwörter verwenden,
- Netzwerkintegration in der Betriebsanleitung beschreiben,
- Fernwartung getrennt und kontrolliert freigeben.

Missbrauch des Fernwartungszugangs
Ein kompromittierter Fernwartungszugang könnte einen weitreichenden Zugriff auf die Maschine ermöglichen. Besonders kritisch wäre dies, wenn Programme, Parameter oder sicherheitsrelevante Einstellungen verändert werden können.

Mögliche Maßnahmen:

- Fernwartung standardmäßig deaktiviert oder nur nach Betreiberfreigabe aktivieren,
- Zugriff nur für autorisiertes Servicepersonal,
- starke Authentifizierung,
- Protokollierung von Fernzugriffen,
- klare Trennung von Diagnosezugriff und Änderungsrechten,
- organisatorischer Freigabeprozess für sicherheitsrelevante Änderungen.

Manipulation über USB-Serviceport
Über USB könnten manipulierte Dateien, nicht freigegebene Updates oder Schadsoftware eingebracht werden. Außerdem könnten Rezepturen oder Parameter unkontrolliert verändert werden.

Mögliche Maßnahmen:

- USB-Funktion auf erforderliche Anwendungsfälle beschränken,
- nur freigegebene Datenträger und Dateien zulassen,
- Updatepakete prüfen,
- Bedien- und Serviceanweisung für USB-Nutzung erstellen,
- nicht benötigte USB-Funktionen deaktivieren,
- Zugriff auf USB-Funktionen rollenbasiert begrenzen.

Unbefugte Änderung von Maschinenparametern

Über HMI, Engineering-Tool oder Fernwartung könnten Parameter verändert werden, die Einfluss auf Maschinenfunktion, Qualität, Prozesssicherheit oder ggf. Maschinensicherheit haben.

Mögliche Maßnahmen:

- rollenbasiertes Berechtigungskonzept,
- Trennung von Bedien-, Einricht-, Service- und Administratorrechten,
- Schutz kritischer Parameter gegen unbefugte Änderung,
- Protokollierung relevanter Parameteränderungen,
- Freigabeprozess für sicherheitsrelevante Änderungen,
- Validierungsprüfung nach Änderungen an sicherheitsrelevanten Funktionen.

Veraltete Software- oder Firmwarestände

Veraltete Softwarestände können bekannte Schwachstellen enthalten. Ohne Übersicht über die verwendeten Versionen kann der Hersteller später nicht bewerten, ob eine Schwachstelle die Maschine betrifft.

Mögliche Maßnahmen:

- Software- und Firmwareliste erstellen,
- Lieferanteninformationen zu Updates und Schwachstellen einholen,
- Updateprozess definieren,
- Supportzeitraum festlegen,
- betroffene Maschinen anhand von Seriennummern oder Softwareständen nachvollziehbar machen.

Verlust oder Beschädigung von Konfigurationen

Durch Fehlbedienung, Schadsoftware, Hardwarefehler oder fehlerhafte Updates könnten Programme, Rezepturen, Parameter oder Konfigurationen verloren gehen.

Mögliche Maßnahmen:

- Backupkonzept erstellen,
- Wiederherstellungsprozess beschreiben,
- freigegebene Software- und Parameterstände dokumentieren,
- Wiederherstellung nur durch autorisierte Personen,
- Prüfung nach Wiederherstellung sicherheitsrelevanter Einstellungen.

Die Cybersecurity-Risikobewertung sollte nicht nur Risiken beschreiben, sondern jeweils nachvollziehbar dokumentieren, welche Maßnahmen getroffen wurden und welche Restrisiken verbleiben. Sie kann als eigenständiges Dokument oder als CRA-Abschnitt innerhalb der technischen Dokumentation geführt werden.

11.5 Technische Maßnahmen

Aus der Risikobewertung werden technische Maßnahmen abgeleitet. Für die Beispielmaschine können folgende Maßnahmen vorgesehen werden:

- sicheres Rollen- und Rechtekonzept im HMI,
- Änderung initialer Passwörter bei Inbetriebnahme,
- keine universellen Standardpasswörter im Auslieferungszustand,
- Deaktivierung nicht benötigter Dienste und Schnittstellen,
- Begrenzung der Ethernet-Kommunikation auf erforderliche Funktionen,
- kontrollierte Freigabe des Fernwartungszugangs,
- Protokollierung relevanter Fernzugriffe und Parameteränderungen,
- Schutz von Service- und Engineering-Zugängen,
- eindeutige Verwaltung von Software- und Firmwareständen,
- kontrolliertes Updateverfahren,
- Backup- und Wiederherstellungsmöglichkeit,
- Dokumentation der sicheren Standardkonfiguration.

Bei sicherheitsrelevanten Parametern ist zusätzlich zu prüfen, ob Änderungen Auswirkungen auf validierte Sicherheitsfunktionen haben können. Änderungen an Sicherheitsprogrammen, sicheren Geschwindigkeiten, sicheren Positionen, Schutztürlogiken oder anderen sicherheitsbezogenen Funktionen dürfen nicht unkontrolliert erfolgen. Hier muss gegebenenfalls eine erneute Validierung durchgeführt und dokumentiert werden.

Technische Maßnahmen sollten möglichst so umgesetzt werden, dass die Maschine bereits im Auslieferungszustand sicher vorkonfiguriert ist. Der Betreiber soll nicht erst durch umfangreiche Nacharbeiten einen cyberresilienten Grundzustand herstellen müssen.

11.6 Organisatorische Maßnahmen beim Hersteller

Neben technischen Maßnahmen benötigt der Maschinenbauer interne Prozesse. Diese Prozesse stellen sicher, dass Cybersecurity nicht nur einmalig bei der Auslieferung betrachtet wird, sondern während des Supportzeitraums aufrechterhalten werden kann.

Für die Beispielmaschine sollte der Hersteller insbesondere folgende organisatorische Maßnahmen einführen:

- Zuständigkeit für Cybersecurity im Produktentwicklungsprozess festlegen,
- CRA-Relevanz und Produktklassifizierung dokumentieren,
- Cybersecurity-Risikobewertung durchführen und aktuell halten,
- Lieferanteninformationen zu digitalen Komponenten einholen,
- Software- und Komponentenverzeichnis führen,
- Supportzeitraum für die Maschine festlegen,
- Kontaktstelle für Schwachstellenmeldungen benennen,
- Prozess zur Bewertung gemeldeter Schwachstellen einrichten,
- Prozess zur Bereitstellung von Updates oder Minderungsmaßnahmen definieren,
- Meldeprozess für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle festlegen,
- Änderungsmanagement für Software, Firmware und digitale Schnittstellen einführen,
- Servicepersonal zu cyberrelevanten Vorgaben unterweisen.

Diese organisatorischen Maßnahmen müssen nicht zwingend ein eigenständiges Managementsystem bilden. Sie können in bestehende Prozesse wie Entwicklungsfreigabe, Lieferantenbewertung, Änderungsmanagement, Serviceprozess, Reklamationsbearbeitung und technische Dokumentation integriert werden.

Entscheidend ist, dass der Hersteller im Ernstfall handlungsfähig ist. Wenn eine Schwachstelle bekannt wird, muss nachvollziehbar sein, welche Maschinen betroffen sind, wie die Schwachstelle bewertet wird, wer Maßnahmen festlegt, wie Betreiber informiert werden und wie die Umsetzung dokumentiert wird.

11.7 Anforderungen an die Betriebsanleitung

Die Betriebsanleitung muss den Betreiber in die Lage versetzen, die Maschine sicher und cyberresilient zu betreiben. Für die Beispielmaschine sollte daher ein eigener Abschnitt zu Cybersecurity, IT-Sicherheit oder digitalen Schnittstellen aufgenommen werden.

Dieser Abschnitt sollte mindestens folgende Punkte enthalten:

- Beschreibung der vorhandenen digitalen Schnittstellen,
- Hinweise zur sicheren Netzwerkintegration,
- Vorgaben zur Änderung initialer Passwörter,
- Beschreibung der Benutzerrollen und Zugriffsrechte,
- Hinweise zur sicheren Verwendung des USB-Serviceports,
- Beschreibung der Fernwartungsfunktion,
- Verfahren zur Freigabe und Beendigung des Fernzugriffs,
- Hinweis, dass Fernwartung nur durch autorisierte Personen erfolgen darf,
- Hinweise zu Updates und freigegebenen Softwareständen,
- Backup- und Wiederherstellungshinweise,
- Verhalten bei Verdacht auf Manipulation oder Cyberangriff,
- Kontaktstelle für Schwachstellenmeldungen,
- Angabe des Supportzeitraums,
- Hinweise zum Ende des Supports,
- Hinweise zur sicheren Außerbetriebnahme und Datenlöschung.

Ein möglicher Textbaustein für die Betriebsanleitung kann lauten:

Cybersecurity und digitale Schnittstellen
Die Maschine verfügt über digitale Schnittstellen zur Bedienung, Diagnose, Datensicherung, Wartung und optionalen Fernwartung. Diese Schnittstellen dürfen nur durch autorisierte und entsprechend unterwiesene Personen genutzt werden. Zugangsdaten sind vertraulich zu behandeln und gegen unbefugte Weitergabe zu schützen.

Initiale Passwörter sind bei der Inbetriebnahme zu ändern. Nicht benötigte Schnittstellen und Dienste sind deaktiviert zu halten. Der Fernwartungszugang darf nur für konkrete Servicefälle freigegeben werden und ist nach Abschluss der Arbeiten wieder zu deaktivieren. Änderungen an Maschinenparametern, Softwareständen oder sicherheitsrelevanten Einstellungen dürfen nur durch autorisierte Personen und entsprechend den Vorgaben des Herstellers durchgeführt werden.

Vor dem Einspielen von Updates, Backups oder Konfigurationsdateien ist sicherzustellen, dass die Dateien aus einer freigegebenen und vertrauenswürdigen Quelle stammen. Nach Änderungen an sicherheitsrelevanten Funktionen ist zu prüfen, ob eine erneute Validierung oder Funktionsprüfung erforderlich ist.

Bei Verdacht auf unbefugten Zugriff, Manipulation, Schadsoftware oder eine bekannte Schwachstelle ist die Maschine in einen sicheren Zustand zu versetzen und der Hersteller bzw. die angegebene Kontaktstelle zu informieren.

11.8 Technische Dokumentation

Die CRA-relevanten Nachweise werden in die technische Dokumentation aufgenommen. Für die Beispielmaschine sollte die Dokumentation mindestens folgende Bestandteile enthalten:

- Beschreibung der Maschine und ihrer digitalen Funktionen,
- Abgrenzung der digitalen Produktgrenze,
- Übersicht der digitalen Komponenten,
- Software- und Firmwareliste,
- Netzwerktopologie bzw. Kommunikationsübersicht,
- CRA-Einstufung und Klassifizierungsvermerk,
- Cybersecurity-Risikobewertung,
- Beschreibung der technischen Maßnahmen,
- Beschreibung der organisatorischen Maßnahmen,
- Lieferanteninformationen zu digitalen Komponenten,
- Supportzeitraum und Begründung,
- Update- und Patchkonzept,
- Schwachstellenmanagementprozess,
- Benutzerinformationen bzw. Betriebsanleitung,
- Nachweise zur Konformitätsbewertung,
- EU-Konformitätserklärung.

Die technische Dokumentation sollte so aufgebaut sein, dass sie später aktualisiert werden kann. Wenn sich Softwarestände ändern, Updates bereitgestellt werden, neue Schwachstellen bekannt werden oder digitale Schnittstellen geändert werden, muss die Dokumentation entsprechend gepflegt werden.

Für Maschinenbauer ist eine klare Verweisstruktur sinnvoll. Nicht alle Informationen müssen in einem einzigen Dokument stehen. Es kann zweckmäßig sein, eine CRA-Konformitätsakte zu erstellen, die auf bestehende Dokumente verweist, zum Beispiel auf Schaltpläne, Netzwerktopologie, Softwareliste, Risikobeurteilung, Betriebsanleitung, Serviceanweisung, Lieferantendokumentation und Änderungsprotokolle.

11.9 Update- und Schwachstellenprozess

Für die Beispielmaschine wird ein einfacher, aber nachvollziehbarer Update- und Schwachstellenprozess festgelegt.

Der Hersteller benennt eine Kontaktstelle für Schwachstellenmeldungen. Meldungen können von Betreibern, Servicepersonal, Lieferanten, Sicherheitsforschern oder internen Stellen kommen. Jede Meldung wird erfasst, technisch bewertet und einem Produkt bzw. einer Maschinenvariante zugeordnet.

Der Prozess kann in folgenden Schritten ablaufen:

1. Eingang der Schwachstellenmeldung.
2. Erfassung der betroffenen Komponente, Softwareversion und Maschinenvariante.
3. Bewertung, ob die Schwachstelle die Beispielmaschine betrifft.
4. Bewertung der möglichen Auswirkungen auf Verfügbarkeit, Integrität, Vertraulichkeit und ggf. Maschinensicherheit.
5. Entscheidung, ob eine aktiv ausgenutzte Schwachstelle oder ein schwerwiegender Sicherheitsvorfall vorliegt.
6. Festlegung von Korrektur- oder Minderungsmaßnahmen.
7. Bereitstellung eines Sicherheitsupdates, einer Konfigurationsänderung oder einer Betreiberanweisung.
8. Information betroffener Betreiber.
9. Dokumentation der Entscheidung und der getroffenen Maßnahmen.
10. Prüfung, ob gesetzliche Meldepflichten ausgelöst werden.

Für Updates wird festgelegt, welche Komponenten aktualisiert werden können und wie Updates freigegeben werden. Updates müssen aus vertrauenswürdiger Quelle stammen und vor Freigabe geprüft werden. Bei Änderungen an sicherheitsrelevanten Funktionen ist zu bewerten, ob zusätzliche Prüfungen oder Validierungen erforderlich sind.

Der Hersteller sollte außerdem dokumentieren können, welche Maschine welchen Software- und Firmwarestand besitzt. Nur so lässt sich im Fall einer Schwachstelle feststellen, welche ausgelieferten Maschinen betroffen sind.

11.10 Ergebnis: pragmatischer CRA-konformer Umgang

Das Beispiel zeigt, dass ein pragmatischer CRA-konformer Umgang mit einer einfachen Maschine möglich ist, wenn die Anforderungen strukturiert in den bestehenden Maschinenbauprozess integriert werden.

Der entscheidende Schritt besteht nicht darin, jede Maschine wie ein komplexes IT-System zu behandeln. Entscheidend ist vielmehr, die digitalen Elemente und Schnittstellen bewusst zu erfassen, die daraus entstehenden Cyberrisiken zu bewerten, angemessene Maßnahmen festzulegen und diese nachvollziehbar zu dokumentieren.

Für die Beispielmaschine ergibt sich folgender pragmatischer Lösungsansatz:

- Die Maschine wird als Produkt mit digitalen Elementen identifiziert.
- Die digitale Produktgrenze wird beschrieben.

- Die Maschine wird als Standardprodukt mit digitalen Elementen eingestuft.
- Das Verfahren der internen Fertigungskontrolle wird gewählt.
- Digitale Komponenten, Schnittstellen und Softwarestände werden dokumentiert.
- Cybersecurity-Risiken werden bewertet.
- Technische Maßnahmen wie Rollen, Passwörter, Schnittstellenschutz, Fernwartungsfreigabe, Logging, Backup und Updatekontrolle werden umgesetzt.
- Organisatorische Prozesse für Lieferanteninformationen, Schwachstellen, Updates, Supportzeitraum und Incident Handling werden eingerichtet.
- Die Betriebsanleitung wird um cyberrelevante Informationen ergänzt.
- Die technische Dokumentation wird um CRA-relevante Nachweise erweitert.
- Die EU-Konformitätserklärung und CE-Dokumentation werden entsprechend angepasst.

Damit wird der CRA nicht zu einem isolierten Zusatzprojekt, sondern zu einem weiteren Baustein des bestehenden CE-Prozesses. Für Maschinenbauer liegt genau darin der praktikable Weg: Cybersecurity wird frühzeitig in Konstruktion, Steuerungstechnik, Software, Einkauf, Dokumentation und Service integriert.

12 Marktaufsicht, Sanktionen und Umsetzungshilfen

Der Cyber Resilience Act ist nicht nur eine technische Orientierungshilfe, sondern eine verbindliche europäische Produktverordnung. Die Einhaltung der Anforderungen kann durch Marktüberwachungsbehörden überprüft werden. Für Hersteller bedeutet dies, dass Cybersecurity-Anforderungen künftig ähnlich wie auch andere CE-Anforderungen nachweisbar dokumentiert und gegenüber Behörden begründet werden müssen.

12.1 Sanktionsrahmen nach Artikel 64 CRA

Artikel 64 CRA sieht einen gestaffelten Sanktionsrahmen vor. Verstöße gegen die wesentlichen Cybersicherheitsanforderungen nach Anhang I sowie gegen zentrale Herstellerpflichten, insbesondere nach den Artikeln 13 und 14, können mit Geldbußen von bis zu 15 Mio. EUR oder, bei Unternehmen, bis zu 2,5 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden, je nachdem, welcher Betrag höher ist.

Für weitere Verstöße, beispielsweise gegen bestimmte Pflichten von Wirtschaftsakteuren, Vorgaben zur technischen Dokumentation oder Konformitätsbewertung, sieht der CRA Geldbußen von bis zu 10 Mio. EUR oder bis zu 2 % des weltweiten Jahresumsatzes vor. Werden gegenüber notifizierten Stellen oder Marktüberwachungsbehörden falsche, unvollständige oder irreführende Informationen bereitgestellt, können Geldbußen von bis zu 5 Mio. EUR oder bis zu 1 % des weltweiten Jahresumsatzes verhängt werden.

Die Höhe einer Geldbuße richtet sich nach den Umständen des Einzelfalls. Zu berücksichtigen sind unter anderem Art, Schwere und Dauer des Verstoßes, die Folgen des Verstoßes, frühere einschlägige Verstöße sowie Größe und Marktanteil des betroffenen Wirtschaftsakteurs. Geldbußen können außerdem zusätzlich zu anderen korrektiven oder beschränkenden Maßnahmen der Marktüberwachungsbehörde verhängt werden.

Für Maschinenbauer ist damit klar: Die CRA-Konformität sollte nicht nur als technische Zusatzanforderung verstanden werden. Sie ist Teil der Produktkonformität und kann im Marktüberwachungsfall unmittelbare wirtschaftliche Konsequenzen haben.

12.2 Marktüberwachung in Deutschland

In Deutschland kommt dem Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, eine zentrale Rolle bei der Umsetzung des CRA zu. Das BSI wird als marktüberwachende Behörde für den Cyber Resilience Act tätig und kann Produkte mit digitalen Elementen stichprobenartig oder anlassbezogen auf ihre Cybersicherheit überprüfen.

Für Hersteller bedeutet dies, dass CRA-relevante Nachweise strukturiert verfügbar sein müssen. Dazu gehören insbesondere die Cybersecurity-Risikobewertung, die technische Dokumentation, die Produktklassifizierung, die Konformitätsbewertung, Benutzerinformationen, Angaben zum Supportzeitraum, Nachweise zum Schwachstellenmanagement sowie Informationen zu Updates und Korrekturmaßnahmen.

Die Marktaufsicht kann dabei nicht nur formale Dokumente prüfen. Sie kann auch untersuchen, ob ein Produkt ein erhebliches Cybersicherheitsrisiko aufweist, ob Nichtkonformitäten bestehen und ob Korrekturmaßnahmen erforderlich sind. Für Maschinenbauer ist daher eine nachvollziehbare, konsistente und aktuelle CRA-Dokumentation besonders wichtig.

12.3 BSI TR-03183 als Umsetzungshilfe

Als praktische Umsetzungshilfe kann die Technische Richtlinie BSI TR-03183 herangezogen werden. Die Richtlinie beschreibt Cyber-Resilienz-Anforderungen an Hersteller und Produkte aus Sicht des BSI und dient der Vorbereitung auf die Anforderungen des CRA.

Die BSI TR-03183 ist keine harmonisierte Norm im Sinne des CRA und ersetzt keine formale Konformitätsbewertung. Sie kann jedoch als hilfreiche Orientierung dienen, insbesondere beim Aufbau von Prozessen und Nachweisen. Relevant sind insbesondere die Teile zu allgemeinen Anforderungen, Software Bill of Materials, Schwachstellenberichten und Meldungen.

Für Maschinenbauer kann die TR-03183 insbesondere bei folgenden Themen unterstützen:

- Strukturierung der Cybersecurity-Anforderungen,
- Aufbau eines Software- und Komponentenverzeichnisses,
- Umgang mit Software Bill of Materials,
- Schwachstellenmanagement,
- Meldung und Dokumentation von Schwachstellen,
- Vorbereitung technischer Dokumentation,
- Orientierung an der Sichtweise der deutschen Marktaufsicht.

Die TR-03183 sollte daher als ergänzende Umsetzungshilfe betrachtet werden. Sie ersetzt nicht die Prüfung des CRA, der harmonisierten Normen oder der produktspezifischen Anforderungen. Sie kann aber helfen, die internen Herstellerprozesse frühzeitig in eine Richtung zu entwickeln, die mit den Erwartungen der deutschen Marktüberwachung kompatibel ist.

12.4 Praktische Bedeutung für Maschinenbauer

Für Maschinenbauer ergibt sich aus Marktüberwachung und Sanktionsrahmen eine klare Handlungsempfehlung: CRA-Konformität sollte frühzeitig, nachvollziehbar und prüfbar aufgebaut werden. Im Falle einer behördlichen Anfrage muss der Hersteller nicht nur behaupten können, dass Cybersecurity berücksichtigt wurde. Er muss zeigen können, wie digitale Elemente identifiziert, Risiken bewertet, Maßnahmen umgesetzt, Benutzer informiert und Schwachstellen während des Supportzeitraums behandelt werden.

Besonders wichtig sind daher:

- eine dokumentierte CRA-Anwendungsbereichsprüfung,
- eine begründete Produktklassifizierung,
- eine Cybersecurity-Risikobewertung,
- eine Schnittstellen- und Komponentenübersicht,
- ein Software- und Firmwareverzeichnis,
- Lieferanteninformationen zu digitalen Komponenten,
- ein Update- und Patchkonzept,
- ein Schwachstellenmanagementprozess,
- Benutzerinformationen zur sicheren Nutzung,
- eine aktuelle technische Dokumentation,
- eine angepasste EU-Konformitätserklärung.

Der Sanktionsrahmen des CRA sollte nicht als Drohkulisse verstanden werden, sondern als Hinweis auf die Bedeutung des Themas. Cybersecurity wird zu einem überprüfbaren Bestandteil der Produktverantwortung. Wer die Anforderungen frühzeitig in seine bestehenden CE-, Entwicklungs-, Einkaufs-, Dokumentations- und Serviceprozesse integriert, reduziert nicht nur rechtliche Risiken, sondern verbessert auch die langfristige Qualität und Robustheit seiner Maschinen.

13 Fazit

Der Cyber Resilience Act erweitert den klassischen CE-Prozess im Maschinenbau um eine neue, produktbezogene Dimension: die Cyberresilienz von Maschinen und digitalen Komponenten. Für Maschinenbauer bedeutet dies nicht, dass bewährte Prozesse zur Maschinensicherheit, Risikobeurteilung, funktionalen Sicherheit und technischen Dokumentation ersetzt werden. Vielmehr müssen diese Prozesse künftig um Cybersecurity-Aspekte ergänzt und über den gesamten Produktlebenszyklus hinweg weitergedacht werden.

Moderne Maschinen enthalten häufig SPS-Steuerungen, HMI-Systeme, Industrie-PCs, Robotersteuerungen, Frequenzumrichter, Fernwartungszugänge, Netzwerkschnittstellen, Software, Firmware und Cloud- oder Servicefunktionen. Damit können sie Produkte mit digitalen Elementen im Sinne des CRA sein. Entscheidend ist daher nicht mehr nur, ob eine Maschine mechanisch, elektrisch und funktional sicher ist. Zusätzlich muss der Hersteller prüfen, ob digitale Elemente angemessen gegen unbefugten Zugriff, Manipulation, Schwachstellen und Sicherheitsvorfälle geschützt sind.

Für viele Maschinenbauer wird die typische Maschine voraussichtlich als Standardprodukt mit digitalen Elementen einzuordnen sein. Das bedeutet jedoch nicht, dass der CRA vernachlässigt werden darf. Auch für solche Produkte sind eine Cybersecurity-Risikobewertung, geeignete technische und organisatorische

Maßnahmen, Benutzerinformationen, technische Dokumentation, Schwachstellenmanagement, Updateprozesse und eine angepasste EU-Konformitätserklärung erforderlich.

Besonders wichtig ist die frühe Einbindung der Cybersecurity in die Konstruktion. Wer digitale Schnittstellen, Fernwartung, Benutzerrollen, Updatefähigkeit, Lieferanteninformationen und sichere Standardkonfigurationen erst kurz vor der Auslieferung betrachtet, wird häufig mit nachträglichen und aufwendigen Anpassungen konfrontiert. Wird Cybersecurity dagegen bereits in der Konzept- und Entwicklungsphase berücksichtigt, kann sie mit vertretbarem Aufwand in bestehende Maschinenbauprozesse integriert werden.

Der CRA macht außerdem deutlich, dass die Verantwortung des Herstellers nicht mit der Auslieferung der Maschine endet. Während des festgelegten Supportzeitraums müssen Schwachstellen beobachtet, bewertet und behandelt werden. Sicherheitsupdates, Korrekturmaßnahmen, Betreiberinformationen und gegebenenfalls gesetzliche Meldungen werden damit zu einem festen Bestandteil der Produktverantwortung.

Für den Maschinenbau ist auch die Schnittstelle zwischen Safety und Security von zentraler Bedeutung. Cybersecurity ersetzt keine funktionale Sicherheit und keine Risikobeurteilung nach Maschinenverordnung. Sie kann aber eine Voraussetzung dafür sein, dass sicherheitsrelevante Funktionen dauerhaft wirksam bleiben. Wenn Sicherheitsparameter, Programme, Fernwartungszugänge oder Steuerungssysteme digital manipulierbar sind, kann ein Cybersecurity-Problem unmittelbar zu einem Safety-Problem werden.

Die größte Herausforderung des CRA liegt daher nicht in einer einzelnen technischen Maßnahme, sondern in der systematischen Integration in den Produktprozess. Maschinenbauer sollten digitale Produktgrenzen definieren, Schnittstellen erfassen, Lieferanteninformationen einholen, Software- und Firmwarestände dokumentieren, Cyberrisiken bewerten, sichere Konfigurationen festlegen, Update- und Schwachstellenprozesse aufbauen und die Betriebsanleitung entsprechend erweitern.

Gleichzeitig sollte der CRA nicht als unbeherrschbares IT-Regelwerk verstanden werden. Viele Grundprinzipien sind dem Maschinenbau aus der CE-Welt vertraut: systematische Bewertung, risikobasierte Maßnahmen, technische Dokumentation, klare Benutzerinformationen, Konformitätsbewertung und Lebenszyklusverantwortung. Neu ist vor allem der Gegenstand der Betrachtung: digitale Elemente, Datenverbindungen, Software, Schwachstellen und Cybersecurity-Prozesse.

Wer den CRA frühzeitig in bestehende CE-, Entwicklungs-, Einkaufs-, Dokumentations- und Serviceprozesse integriert, kann die Anforderungen pragmatisch und nachvollziehbar erfüllen. Entscheidend ist, Cybersecurity nicht als nachträgliche Zusatzfunktion zu behandeln, sondern als festen Bestandteil moderner Maschinenentwicklung.

Der CRA ist dabei nicht nur als technische Empfehlung zu verstehen, sondern als verbindliche Produktverordnung mit Marktüberwachung und Sanktionsrahmen. Hersteller müssen daher im Fall einer behördlichen Prüfung nachvollziehbar darlegen können, wie sie den Anwendungsbereich bewertet, das Produkt klassifiziert, Cyberrisiken analysiert, Maßnahmen umgesetzt, Benutzer informiert und Schwachstellen während des Supportzeitraums behandelt haben. Eine lückenhafte oder nur informelle Betrachtung reicht künftig nicht mehr aus.

Der Cyber Resilience Act wird den Maschinenbau damit nicht grundlegend neu erfinden. Er macht jedoch verbindlich, was durch Vernetzung, Fernwartung und digitale Steuerungstechnik ohnehin immer wichtiger

wird: Maschinen müssen künftig nicht nur sicher konstruiert, sondern auch cyberresilient entwickelt, dokumentiert, ausgeliefert und über ihren Supportzeitraum betreut werden.

Dieses Whitepaper wurde erstellt von

Andreas Schunkert
Geschäftsführer Cobot Safety

Kontakt:

Web: www.cobot-safety.de
Mail: Andreas.Schunkert@cobot-safety.de
Tel.: 0162 - 87 999 76