MVO und CRA: Was Maschinenbauer jetzt wissen und tun müssen

Zwei Fristen, eine Verantwortung

Artikel anhören!

Ab Januar 2027 löst die neue EU-Maschinenverordnung (MVO) die bisherige Maschinenrichtlinie ab – und kurz darauf, im Dezember 2027, greift der Cyber Resilience Act (CRA). Beide Regelwerke verlangen eine CE-Kennzeichnung und stellen Maschinenbauer vor teils erhebliche neue Herausforderungen. Tobias Blickle, Product Marketing Specialist im Bereich Maschinensicherheit bei ABB, und Andreas Schader, global zuständig für Standardisierung und Regulierung im Bereich Motion Drive Products, erklären, worauf es ankommt, wo die größten Fallstricke lauern und warum man besser heute als morgen anfängt.

Sowohl MVO als auch CRA betreffen die CE-Kennzeichnung. Was ändert sich für Maschinenbauer grundlegend?

Andreas Schader: Die Maschinenrichtlinie stammt aus dem Jahr 2006 – sie war also 20 Jahre in Kraft, wenn sie durch die neue Maschinenverordnung abgelöst wird. Das ist keine routinemäßige Revision, das ist ein echter Generationenwechsel. Parallel dazu wird mit dem Cyber Resilience Act erstmals Cybersecurity für Produkte verbindlich geregelt. Beide Rechtsakte sind CE-pflichtig, beide gelten ohne Bestandsschutz: Wer ab Januar 2027 eine Maschine in Verkehr bringt, muss die neue Maschinenverordnung erfüllen – unabhängig davon, wann die verbauten Komponenten entwickelt oder zertifiziert wurden.

Tobias Blickle: Das bedeutet in der Praxis: Konformitätserklärung, technische Dokumentation und alle zugehörigen Nachweise müssen auf die neue Rechtsgrundlage umgestellt werden. Je nach Produkt sind mehrere EU-Rechtsakte zu berücksichtigen: neben der Maschinenverordnung also auch der CRA, die EMV-Richtlinie oder – je nach Einsatzbereich – ATEX. Wer das als reine Verwaltungsaufgabe versteht, unterschätzt den Aufwand.

Was sind die konkreten neuen Anforderungen der Maschinenverordnung gegenüber der alten Richtlinie?

Blickle: Für die meisten Maschinenbauer sind rund 90 Prozent der Anforderungen gleich geblieben – das ist die gute Nachricht. Die entscheidende Neuerung betrifft das Thema 'Protection against Corruption': Ein erfolgreicher Cyberangriff darf nicht zu einer unsicheren Maschinensituation führen. Dieser muss für die Maschinensicherheit rückwirkungsfrei bleiben – das heißt keine Personengefährdung, keine Umweltschäden. Dabei geht es ausdrücklich nicht darum, Angriffe zu verhindern, sondern ihre Auswirkungen zu beherrschen. Das ist ein wichtiger konzeptioneller Unterschied, der in der Risikobeurteilung entsprechend abgebildet werden muss. Das BSI zählt täglich rund 120 IT-OT-Angriffe auf deutsche Unternehmen. Die Anforderungen sind also keine theoretische Vorsichtsmaßnahme – sie reagieren auf eine reale und wachsende Bedrohungslage.

Und der Cyber Resilience Act – was fordert er zusätzlich?

Schader: Der CRA ist konzeptionell neu und verlangt ein anderes Denken. Er verpflichtet Hersteller dazu, ihre Produkte über die gesamte kommunizierte Support-Dauer aktiv auf Schwachstellen zu überwachen, diese zu bewerten und – wenn sie im Produktkontext ausnutzbar sind – zu beheben. Das bedeutet: Schwachstellen-Datenbanken und Patch-Notes der Komponentenlieferanten müssen systematisch verfolgt werden. Für jede bekannte Schwachstelle muss bewertet werden, ob sie unter realistischen Betriebsbedingungen ein Angriffsvektor ist. Ein Beispiel: Eine Schwachstelle betrifft eine Profinet-Schnittstelle. Wenn das Gerät nur über eine digitale Steuerleitung läuft, ist diese Schnittstelle kein Angriffspfad – und es besteht unter Umständen keine Pflicht zur Behebung. Dieses Urteil muss aber intern gefällt und dokumentiert werden. Das setzt einen implementierten Prozess voraus, den nur wenige Maschinenbauer heute haben.

Maschinenverordnung und Cyber Resilience Act bringen Digitalisierung, KI und Security ins Zentrum von Komponentenherstellern, Software-Anbietern, Maschinen- und Anlagenbauern sowie Händlern.

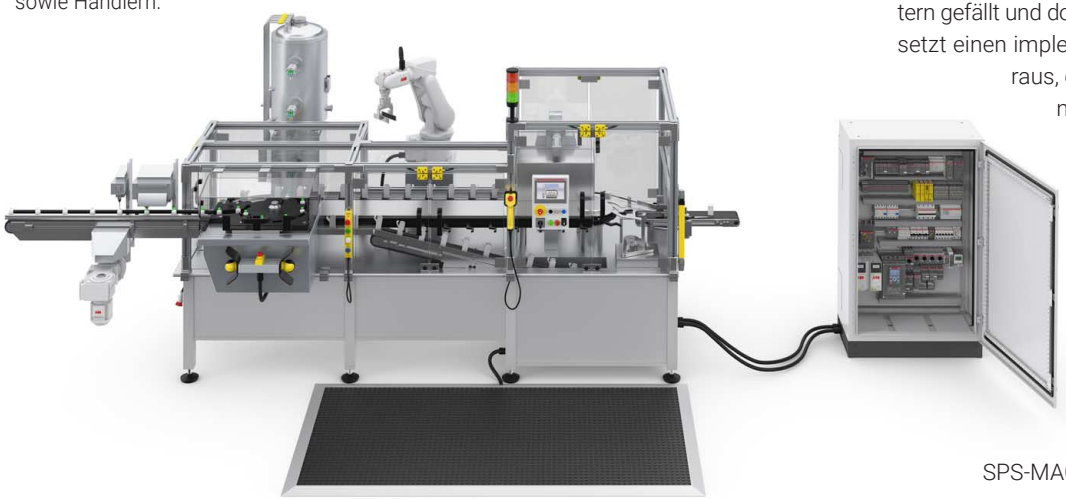

Bild: ABB AG

Bisher kannte man organisatorische Cybersecurity: Asset-Management, Zugriffsregeln, Patch-Management für die IT-Infrastruktur – das regelt NIS 2. Der CRA geht

eine Ebene tiefer und macht die produktspezifische Cybersecurity zur Herstellerpflicht: konkrete Support-Dauern, verpflichtende Sicherheits-Patches, und die Anforderung, ein Produkt so lange zu unterstützen, wie man das kommuniziert hat.

Ab wann gelten welche Pflichten?
Schader: Die Maschinenverordnung gilt ab Januar 2027, der CRA vollständig ab Dezember 2027. Aber bereits ab September 2026 greifen die Meldepflichten des CRA für Bestandsprodukte: Wer davon Kenntnis erhält, dass eine seiner Komponenten aktiv ausgenutzt wird, muss das den Aufsichtsbehörden melden – nicht der Öffentlichkeit, aber den Behörden. Und das gilt für Produkte, die heute schon im Markt sind.

Blickle: Deshalb würde ich sagen: Von den Fristen her hat die Maschinenverordnung Priorität. Wer den Gesamtaufwand betrachtet, muss mit dem CRA jetzt anfangen – nicht erst nach der Maschinenverordnung.

Wird die Deadline noch einmal verschoben? Viele schienen darauf zu spekulieren.
Schader: Das wäre politisch und verfahrenstechnisch extrem aufwändig. Ein neues Gesetzgebungsverfahren auf europäischer Ebene, Parlament, Rat und Kommission müssten zustimmen. Der politische Wille dafür ist nicht erkennbar. Wer darauf setzt, spielt ein gefährliches Spiel.

> Der CRA fordert nicht Resilienz gegen den Cyberangriff selbst, sondern die Beherrschung seiner Auswirkungen.
>
> **Andreas Schader, ABB AG**

Blickle: Hinzu kommt: Wer jetzt noch keinen Notified Body unter Vertrag hat, wird Schwierigkeiten bekommen. Diese Stellen werden überlastet sein. Das ist dann das Problem des Herstellers – niemand sonst.

Wo liegen die größten Unsicherheiten für Maschinenbauer gerade?
Schader: Die größte Herausforderung ist das Fehlen harmonisierter Standards. Für die alte Maschinenrichtlinie gab es davon rund 800 – ein eingespieltes System, das Maschinenbauern eine klare Richtschnur gab. Mit der neuen Maschinenverordnung wurde dieses System zurückgesetzt; alle Standards müssen neu harmonisiert werden. Für die Cybersecurity-Anforderungen gibt es derzeit noch keinen einzigen harmonisierten Standard. Der neue EN50742 befindet sich noch in der Draft-Phase. Das trifft vor allem Unternehmen, die bisher nach dem Muster 'Anforderung plus Standard gleich Umsetzung' gearbeitet haben. Dieses Muster funktioniert gerade nicht.

Blickle: Es ist eine doppelte Unsicherheit: technisch und legislativ zugleich. Der Standardization Request wurde erst ein Jahr nach Veröffentlichung der Regulierung gestellt – so ging ein Jahr Standardisierungszeit verloren. Beim CRA wurde das besser gelöst, aber das ändert nichts daran, dass heute kein fertiger Standard vorliegt.

Wie sollte ein mittelständischer Maschinenbauer konkret vorgehen?
Schader: Zuerst: nicht alles in die IT-Abteilung kippen. Organisatorische IT-Kompetenz ist etwas anderes als produktbezogene Cybersecurity-Kompetenz für Embedded Systems. Diese Fähigkeit muss entweder intern aufgebaut oder extern eingekauft werden – aber die Risikoanalyse-Kompetenz für den CRA sollte man im Haus haben. Denn man muss selbst beurteilen können, ob eine neue Schwachstelle in einer Zulieferkomponente für das eigene Produkt relevant ist. Das kann man nicht vollständig delegieren. Und nicht jede Maschine ist überhaupt CRA-pflichtig: Eine Drehbank ohne jede Außenkommunikation fällt möglicherweise gar nicht in den Geltungsbereich.

Der zweite Schritt ist eine systematische Erfassung aller Kommunikationsschnittstellen: Ethernet, LAN, USB, Funk. Was nicht benötigt wird, wird abgeschaltet oder physisch

Bilder: ABB AG

verschlossen. Das klingt banal, ist aber der Ausgangspunkt jeder Risikobeurteilung. Das Ziel ist dabei nicht maximale, sondern angemessene Sicherheit – Restrisiken sind ausdrücklich erlaubt, müssen aber bewertet und dokumentiert sein.

Blickle: Als Maschinenbauer gilt es, eine ehrliche Istaufnahme zu machen: Wo brauche ich Unterstützung, was kann ich extern vergeben – und was will ich extern vergeben? Am Ende unterschreibt der Hersteller. Er trägt die Verantwortung, auch wenn er Teile der Arbeit delegiert.

Patches und Support über zehn oder fünfzehn Jahre – ist das für Maschinen mit langen Lebensdauern überhaupt realistisch?

Schader: Das ist einer der strukturellen Fehler des CRA. Er kennt nur eine Produktlebensdauer – wie bei einem Smartphone. Aber eine Werkzeugmaschine kann nach zehn Jahren verkauft, generalüberholt und neu in Betrieb genommen werden. Ein Kraftwerk hat eine Laufzeit von vierzig Jahren. Niemand kann ernsthaft vierzig Jahre Cybersecurity-Support versprechen – das wäre wirtschaftlich nicht darstellbar und würde europäische Produkte massiv verteuern. Hier wurde aus meiner Sicht nicht ausreichend an die OT-Realität gedacht.

> Von den Fristen her hat die Maschinenverordnung Priorität, wer aber den Aufwand insgesamt betrachtet, sollte mit dem CRA bereits heute beginnen.
>
> **Tobias Blickle, ABB AG**

Was der Hersteller tun muss: Bereits vor dem Verkauf kommunizieren, wie lange er Support leistet. Die Support-Dauer muss mit dem Supply-Chain-Management abgestimmt sein – denn man kann nur so lange supporten, wie die Kernkomponenten vom Lieferanten unterstützt werden. Danach muss ein Prozess stehen, der Schwachstellen systematisch verfolgt, bewertet und – wenn nötig – behebt. Herstellerverantwortung, nicht Opt-in.

Die Möglichkeit zur digitalen Betriebsanleitung klingt praktisch – aber gibt es auch Risiken?

Blickle: Ja, und die werden oft unterschätzt. Viele Maschinenbauer sehen die Erlaubnis zur digitalen Bereitstellung zunächst als Erleichterung, ohne die Konsequenzen zu durchdenken. Eine Maschine läuft zwanzig, dreißig Jahre. Wenn in dieser Zeit die Domain wechselt oder die Plattform abgeschaltet wird, ist die Dokumentation nicht mehr abrufbar – mit möglichen Haftungsfolgen. Die Papierbeilage ist weiterhin zulässig und für viele Fälle die sicherere Wahl. Digitale Bereitstellung kostet auch Geld und benötigt Infrastruktur – das wird gerne vergessen. ■

Maschinenverordnung (MVO) und Cyber Resilience Act (CRA) – Vergleich der wesentlichen Anforderungen

Thema	Maschinenverordnung (MVO)	Cyber Resilience Act (CRA)
Geltungsbereich	Maschinen, unvollständige Maschinen und verwandte Produkte, die in der EU in Verkehr gebracht werden	Produkte mit digitalen Elementen (Hard- und Software), die in der EU in Verkehr gebracht werden – sofern sie kommunizieren (Netzwerk- oder Datenkommunikation). Rein mechanische Maschinen ohne Außenkommunikation sind ausgenommen.
Inkrafttreten / Stichtag	Veröffentlicht: 2023 Verbindlich ab: 20. Januar 2027	Veröffentlicht: 2024 Meldepflichten ab: September 2026 Vollständig verbindlich ab: 11. Dezember 2027
Wesentliche neue Anforderungen	• Protection against Corruption (verschärft): Ein Cyberangriff darf nicht zu einer unsicheren Maschinensituation führen – keine Personengefährdung, keine Umweltschäden • Rückwirkungsfreiheit der Maschine bei Angriff • Elektronische Betriebsanleitung nun zulässig (mit Bedingungen) • Erweiterte Risikobeurteilung inkl. Cyberbezug	• Produktspezifische Schwachstellenanalyse und -bewertung • Aktive Überwachung von Schwachstellen-Datenbanken • Verpflichtende Sicherheits-Patches während der Support-Dauer • Kommunizierte Support-Dauer muss eingehalten werden • Meldepflicht bei aktiv ausgenutzten Schwachstellen • Software Bill of Materials (SBOM)
Pflichten für Maschinenhersteller	• Risikobeurteilung auf neue Rechtsgrundlage umstellen • Technische Dokumentation aktualisieren • Konformitätserklärung erneuern • Cybersecurity-Aspekte in Risikobeurteilung integrieren	• Alle Außenschnittstellen erfassen und dokumentieren • Nicht benötigte Schnittstellen deaktivieren/verschließen • Support-Dauer festlegen und kommunizieren • Schwachstellen-Management-Prozess implementieren • Meldungen an Aufsichtsbehörden sicherstellen
Lebensdauer & Support (Besondere Herausforderung OT)	Dokumentationspflicht gilt für die Lebensdauer der Maschine (kann Jahrzehnte betragen).Digitale Dokumentation: Verfügbarkeit über gesamte Nutzungsdauer sicherstellen.	CRA kennt nur eine Produktlebensdauer (kein Unterschied zwischen physischer und digitaler Lebenszeit). Für Maschinen mit langen Laufzeiten (10–40 Jahre) und Möglichkeit zur Generalüberholung entsteht ein struktureller Zielkonflikt.
Empfohlene Vorgehensweise	1. Risikobeurteilung auf MVO umstellen 2. Cybersecurity-Anteil (ca. 10 %) an Cybersecurity-Team übergeben 3. Technische Dokumentation aktualisieren 4. Konformitätserklärung erneuern 5. Notified Body frühzeitig einbinden (falls erforderlich)	1. Prüfen, ob Produkt in den CRA-Geltungsbereich fällt 2. Alle Kommunikationsschnittstellen erfassen 3. Schwachstellen-Management-Prozess aufbauen 4. Support-Dauer festlegen und kommunizieren 5. Interne CRA-Kompetenz aufbauen (nicht vollständig delegierbar) 6. Ab September 2026: Meldepflichten einhalten

Quellen: EU-Verordnung 2023/1230 (Maschinenverordnung) | EU-Verordnung 2024/2847 (Cyber Resilience Act) | Experteninterview ABB (Blickle/Schader) | BSI, Bitkom 2024