Jetzt anhören!

## Erste Pflichten greifen im September

# Der CRA-Countdown läuft

Bild: @MinChu/stock.adobe.com

**Zwar gilt die vollständige Konformität des Cyber Resilience Act (CRA) erst ab dem 11. Dezember 2027 als Voraussetzung, um neue Produkte mit digitalen Elementen in der EU anzubieten. Ab dem 11. September 2026 greifen jedoch schon erste Pflichten. So müssen Hersteller schwere Sicherheitsvorfälle und ausgenutzte Schwachstellen melden.**

Auch wenn neue Maschinen mit digitalen Elementen erst ab Dezember 2027 die vollständigen Produktanforderungen des CRA erfüllen müssen, gelten die Meldepflichten bereits mehr als ein Jahr früher, und zwar unabhängig davon, wann eine Maschine in Verkehr gebracht wurde. Im Vergleich zu NIS-2 und Dora rückt der CRA Maschinen, Steuerungen, Schnittstellen (HMI, Human Machine Interfaces), Edge-Gateways, Remote-Service-Komponenten und zugehörige Software in den Fokus und verlangt belastbare Prozesse über den gesamten Lebenszyklus, von Entwicklung und Dokumentation bis zu Updates und Meldungen. Entscheidend ist, ob das Produkt digitale Elemente enthält und in der EU verfügbar ist.

Moderne Anlagen bestehen aus bis zu 5.000 Bauteilen unterschiedlicher Hersteller. Jede Komponente bringt eigene Software, Releasezyklen und damit auch Schwachstellen mit. Trotzdem trägt der Maschinenbauer die Verantwortung für die Gesamtsicherheit des Produkts, auch wenn er zentrale Komponenten nicht selbst entwickelt und nicht bis in jedes Detail der Zulieferungen hineinschauen kann. Hinzu kommt: Während IT im Rhythmus weniger Jahre erneuert wird, laufen OT-Anlagen oft 15 bis 20 Jahre. Zudem sind Updates häufig riskant, da sie zu Stillständen führen und die Gesamtfunktion beeinflussen können. Dennoch verlangt der CRA, dass Hersteller Schwachstellen dokumentieren, Risiken bewerten und angemessene Gegenmaßnahmen nachweisen. Cybersecurity wird damit zur Ingenieuraufgabe entlang von Konstruktion, Service und Betrieb.

Viele der entlang des Produktlebenszyklus zentral gebündelten CRA-Vorgaben lassen sich jedoch mit solider Produktklassifizierung, technischer Dokumentation und klaren Nutzerinformationen umsetzen. Besonders herausfordernd für Maschinenbauer sind allerdings vier Punkte: das kontinuierliche Schwachstellenmanagement, die Bereitstellung von Patches oder alternativen Schutzmaßnahmen, die fristgerechte Meldung von Vorfällen sowie die nachvollziehbare Steuerung des Produktlebenszyklus.

### Mit Transparenz zur Compliance

Schwachstellenmanagement beginnt mit Transparenz. Hersteller müssen genau wissen, welche Software in welcher Version ihre Maschinen steuert. Ohne eine Software Bill of Materials (SBOM), also eine vollständige Übersicht aller Softwarekomponenten, bleibt das ein Blindflug. Eine stets aktuelle Inventarliste bildet die Grundlage für alle weiteren Schritte.

Bei der Bewertung von Schwachstellen unterstützt zudem ein Product Security Incident Response Team (PSIRT). Diese spezialisierte Arbeitsgruppe innerhalb eines Unternehmens identifiziert Sicherheitslücken in eigenen Produkten, Systemen oder Services und analysiert beziehungsweise behebt diese.

### Updates vs. Betriebsstabilität

Der CRA fordert Sicherheitsupdates, auch wenn viele kritische Bausteine von Dritten stammen. Gleichzeitig darf eine Anlage dadurch nicht destabilisiert werden und muss in einer realen Umgebung funktionieren. Und sobald eine Schwachstelle aktiv ausgenutzt wird oder ein schwerer Vorfall vorliegt, läuft die Uhr: Neben der 24- und 72-Stunden-Meldung verlangt der CRA außerdem einen Abschlussbericht, der spätestens 14 Tage nach Verfügbarkeit einer Korrekturmaßnahme bei aktiv ausgenutzten Schwachstellen und binnen eines Monats bei schweren Sicherheitsvorfällen vorliegen muss. Hier bedarf es einer systematischen Überwachung und einer sauberen Datenbasis, um betroffene Modelle sowie den Status der Ausnutzung belastbar bestimmen zu können. Auch hier bildet die Inventarliste das Fundament. Doch nicht jede Schwachstelle erfordert sofort einen Patch. Die Bewertung muss klären, welche Patches welches Handeln erfordern.

### Automatisierung statt Tabellen

Manuelle Ansätze stoßen aufgrund der Vielzahl an Komponenten in der Praxis schnell an Grenzen. CRA-Fähigkeit basiert deshalb auf drei Faktoren: Transparenz über Assets und Softwarestände, ein belastbarer Pfad für Updates oder alternative Gegenmaßnahmen und Prozesse, die Sicherheitsinformationen so verdichten, dass Meldungen fristgerecht und nachweisbar möglich sind. Die Basis hierfür liefern automatisierte Discovery- und Asset-Management-Ansätze. Sie erfassen kontinuierlich relevante Komponenten, bündeln Informationen zentral und erkennen Veränderungen. Wird eine neue Schwachstelle bekannt, lässt sich prüfen, ob und wo die eigene installierte Basis betroffen ist.

### IEC62443-Schutzschild

Für Endanwender ist es entscheidend, dass Anlagen und Maschinen in ihrer Gesamtheit ein belastbares Sicherheitsniveau nach IEC62443 erreichen. Die Normenreihe beschreibt dafür Security Levels (SL), die sich am zu erwartenden Angreiferprofil orientieren und von Schutz gegen einfache, vorsätzliche Angriffe (SL2) bis zu deutlich anspruchsvolleren Szenarien (SL3) reichen. In der Praxis sind jedoch viele Komponenten nur in begrenztem Umfang in höheren Sicherheitsstufen verfügbar. Häufig bleibt es bei einem niedrigeren Geräteschutz, obwohl die Anlage insgesamt mehr braucht. Hier setzt ein vorgelagertes CRA-Gateway als '62443-Shield' an: Es legt einen Sicherheits-Schirm über die Maschine oder Anlage und kann als kompensierende Maßnahme nach IEC62443 Funktionen bereitstellen, die die Anlage selbst nicht oder nicht durchgängig abdeckt. Dazu zählen etwa das Filtern und Segmentieren von Verkehr, die Härtung von Zugängen bis hin zur Multi-Faktor-Authentifizierung sowie kontrollierter, nachvollziehbarer Remote-Zugriff.

### Virtual Patching

Ein weiteres Dilemma in der OT betrifft Patches und Updates. Wird in einer zentralen Steuerung eine kritische Schwachstelle entdeckt, steht der Betreiber vor der Wahl zwischen Produktionsverlust und Restrisiko. Hier kann Virtual Patching helfen, indem es den Schutz vor die verwundbare Komponente verlagert. Ein vorgelagertes Security-Gateway überwacht dabei den Datenverkehr mit tiefgehender Paketinspektion, prüft Protokolle und Inhalte und blockiert bekannte Angriffsmuster, bevor sie das Ziel erreichen. Voraussetzung ist, dass der relevante Verkehr tatsächlich über diesen Kontrollpunkt läuft und nicht durch Umwege oder vollständige Verschlüsselung unsichtbar wird. Das Prinzip dahinter, das gerade für Legacy-Systeme entscheidend ist, heißt Compensating Controls: Wenn ein System nicht zeitnah aktualisierbar ist, senken Schutzmaßnahmen wie Netzsegmentierung, kontrollierte Zugänge und vorgelagerte technische Barrieren das Risiko. Die Gefahr wird begrenzt und der Sicherheitszustand einer Altkomponente erhöht.

### Schwachstellen priorisieren

Wichtig ist zudem die richtige Priorisierung von Schwachstellen. Moderne Ansätze kombinieren hier Schweregrad (CVSS-Score) und Exploit-Wahrscheinlichkeit (EPSS-Score), um klare Prioritäten zu setzen: Kritische und realistisch ausnutzbare Lücken erfordern sofortiges Handeln, mittlere Risiken zeitnahes Schließen, geringe Relevanz Beobachtung.

### Standardisierung als Hebel

Ein kritischer Faktor bleiben die Kosten. Bei Großanlagen fallen zusätzliche Security-Aufwände oft kaum ins Gewicht, bei kleinen Maschinen können zusätzliche Komponenten und Entwicklungsaufwände das Geschäftsmodell belasten. Der CRA zwingt daher zur Standardisierung und nüchterner Kalkulation. Gleichzeitig ist der wirtschaftliche Druck eindeutig: Denn ohne Konformität gibt es ab Dezember 2027 keinen Marktzugang für neue Produkte im CRA-Geltungsbereich. Wer bis kurz vor den Fristen wartet, droht in Hektik zu verfallen. Besonders die Meldepflichten ab September 2026 verlangen hier eine belastbare Struktur. ■

**www.orangecyberdefense.com**


### Autor

Bild: Orange Cyberdefense

Rainer Baeder ist
Senior Business Development Manager bei der
Orange Cyberdefense Germany GmbH.




Digitales Belegexemplar mit freundlicher Genehmigung des Fachmagazins IT&Production. Dieses Dokument ist ausschließlich zur elektronischen Speicherung durch den Autor sowie zur Weitergabe per E-Mail bestimmt. Abweichende Verwendung nur mit Zustimmung des Verlages.