

Mehr Sicherheit in der industriellen Automation

Technologiebericht

Neue Cyber Resilience Act Verordnung (CRA (EU) 2024/2847)



Neue Anforderungen an digitale, vernetzte Produkte stehen im Fokus des Cyber Resilience Acts. Wie Leuze Sensorlösungen fit für die Zukunft macht und was Kunden wissen sollten.

Die EU hat 2024 mit dem Cyber Resilience Act (CRA (EU) 2024/2847) eine Verordnung zur Cybersicherheit erlassen, die stufenweise in Kraft tritt:

**09
26**

Ab dem 11. September 2026 sind Hersteller von Produkten mit digitalen Elementen verpflichtet, schwerwiegende Sicherheitsvorfälle und aktiv ausgenutzte Schwachstellen an eine zentrale Plattform der EU (Single Reporting Platform) zu melden.

**01
27**

Im Januar 2027 tritt die neue Maschinenverordnung (EU) 2023/1230 in Kraft, die konkrete Anforderungen an Cybersicherheit und digitale Sicherheitsbauteile stellt.

**12
27**

Ab Dezember 2027 müssen alle neu in Verkehr gebrachten digitalen Produkte CRA-konform sein. Das bedeutet für die Hersteller: Sie müssen Cyberrisiken bewerten und dokumentieren, einen „Secure Development Life Cycle“ verankern, und sie dürfen nur Produkte in die Märkte bringen, die nach dem jeweils aktuellen Stand der Technik gegen Cyberattacken gesichert sind.

Cybersicherheit für vernetzte Industrieanlagen

Speziell für die industrielle Automation ist das von großer Bedeutung: In vielen industriellen Umgebungen arbeiten Altanlagen in Kombination mit modernen digitalen Systemen. Weil Maschinen und Steuerungen meist viele Jahre im Einsatz bleiben, können Schwachstellen lange bestehen. Zugleich wächst mit zunehmender Vernetzung auch die Angriffsfläche. Schon kleine Sicherheitslücken können Produktionsausfälle oder den Verlust sensibler Betriebsdaten zur Folge haben. Genau hier setzt der CRA an: Er soll die Sicherheit von Geräten mit digitalen Elementen – dazu zählen auch viele Sensoren von Leuze – in der Entwicklung, im Betrieb und während des ganzen Produktlebens gewährleisten. Ein wichtiger Faktor dabei ist die Update-Fähigkeit. Der CRA fordert, dass Sicherheits-Updates technisch möglich sind und Hersteller sie bei Bedarf zur Verfügung stellen. Anwender profitieren damit von Produkten, die nach den neuesten Sicherheitsstandards entwickelt, betrieben und unterstützt werden.

Für welche Anlagenkomponenten der CRA relevant ist

Der CRA betrifft alle Produkte mit digital vernetzten Elementen, die auf dem EU-Markt erhältlich sind. Dazu gehören vernetzte Hardware wie Sensoren und Steuerungen sowie Softwarelösungen in den Netzwerken automatisierter Anlagen. Die Verordnung fordert von Herstellern wie Leuze eine systematische Risikobewertung, ob Produkte potenziell von Cyberattacken bedroht sind. Bei erkannten Risiken werden Gegenmaßnahmen ergriffen. Der Nachweis der CRA-Erfüllung ist künftig Bestandteil der EU-Konformitätserklärung.

Für neu entwickelte Sensoren gewährleistet der Hersteller mit der EU-Konformitätserklärung, dass sie gegen Cyberangriffe geschützt sind. Bei der Integration von Sensoren müssen Maschinenbauer analog zu Safety-Prozessen die Gefährdung der Gesamtanlage bewerten und gegebenenfalls ihre bestehenden Sicherheitskonzepte anpassen. Betreiber und Integratoren definieren ein Sicherheitsniveau und die entsprechenden technischen Voraussetzungen wie beispielsweise Netzwerksegmentierungen mit Firewalls, User-Management oder Logging-Systeme. Die Sensoren unterstützen diese Architektur, um das definierte Sicherheitsniveau der Anlage zu erreichen. Damit erhalten Endkunden langfristig zuverlässige Maschinen, die robust gegen Angriffe, Produktionsausfälle und den Verlust sensibler Daten sind. Für Bestandsprodukte, die bereits in Anlagen verbaut oder eingelagert sind, gilt: Sie müssen nicht zwingend angepasst werden.

Der CRA schafft die Grundlage für sichere, vernetzte Industrieanlagen – von der Entwicklung bis über den gesamten Produktlebenszyklus.

Wie Hersteller die Vorgaben umsetzen

Leuze hat frühzeitig begonnen, die Anforderungen des CRA in die Entwicklungs- und Produktionsprozesse zu integrieren. Die langjährige Expertise im Bereich Safety – also Arbeitssicherheit und Personenschutz – erleichtert die Erweiterung auf Security-Prozesse, die den Schutz von Systemen und Netzwerken gegen externe Angriffsszenarien gewährleisten. Beide Felder erfordern vergleichbare Strategien und Prozesse. Eckpfeiler der Umsetzung sind:

- **Security-by-Design** – digitale Produkte werden auf dem jeweils aktuellen Stand der Cybersicherheit entwickelt. Bezogen auf Sensoren bedeutet das konkret, dass ihre Architektur für Security erweitert wurde und unter anderem mit sicheren Boot- und Dateisystemen versehen ist: Beim Start wird die geladene Software validiert und mit Sicherheitsmerkmalen auf der Gerätehardware überprüft. Daten auf den Sensoren sind gegen Manipulation geschützt, und die Systemarchitektur ermöglicht eine verschlüsselte Datenübertragung auf den Kommunikationskanälen der Sensoren.
- **Security-by-Default** – die Werkseinstellungen sind grundsätzlich cybersicher ausgelegt, alle optionalen Schnittstellen sind deaktiviert. Jeder Benutzerzugriff erfordert eine Authentifizierung. Sensoren können jederzeit auf die Werkseinstellungen zurückgesetzt und kundenspezifische Daten wieder gelöscht werden.
- **Update-Fähigkeit** – digitale Produkte im Betrieb lassen sich mit Updates auf den neuesten Sicherheitsstandard bringen. Wo sinnvoll, werden Updates über die Prozessschnittstelle ermöglicht. Schlägt ein Update fehl, setzt das System sich auf den vorherigen, sicheren Stand zurück.

Wie der CRA die Produktentwicklung verändert

Im Entwicklungsprozess neuer Sensoren werden alle Phasen um Security-Aspekte ergänzt. Dazu gehören:

- **Systematische Bedrohungsanalyse:** Leuze erstellt eine Risikomatrix, die mögliche Angriffsszenarien prüft und bewertet.
- **Minimierung von Angriffsflächen:** Bereits bei der Produktentwicklung werden strenge Sicherheitsanforderungen integriert.
- **Bereitstellen von Sicherheitsupdates:** Für die Nutzungsdauer ihrer Sensoren definiert Leuze Lebenszyklen. Sie legen die Supportdauer fest und regeln die Produktnachfolge. Leuze sorgt dafür, dass Kunden während der geplanten Nutzungsdauer der Produkte regelmäßig Updates erhalten. Diese sichern die Funktionalität und schließen erkannte Schwachstellen. Außerdem werden Mechanismen entwickelt, um alle Leuze-Produkte innerhalb einer Anlage gesammelt updaten zu können.
- **Dokumentation:** Für jedes Produkt werden umfassende Dokumentationen erstellt, die Kunden bei der sicheren Anwendung unterstützen.
- **Schwachstellenmanagement und Schwachstellenmeldung:** Leuze hat Prozesse etabliert, um Schwachstellen zu identifizieren, zu verwalten und im Ernstfall innerhalb der im CRA formulierten Fristen schnell zu melden.

So unterstützt Leuze bei der CRA-Umsetzung

Als Partner für sichere Sensorlösungen begleitet Leuze die Anwender der Produkte durch die Übergangszeit bis zur vollständigen Umsetzung des CRA. Der Sensorhersteller informiert über die Anforderungen und vermittelt Best-Practice-Ansätze. Kunden erhalten Beratung zu ihren Fragen rund um den CRA – von der Auswahl geeigneter Produkte bis zur sicheren Integration in bestehende Anlagen. Das Informationsangebot umfasst:

- **Individuelle Beratung:** Experten stehen bereit, um Kunden bei der Bewertung ihrer Anlagen und Komponenten zu unterstützen.
- **Anwendungsempfehlungen:** Leuze gibt konkrete Hinweise, wie Sensoren und Steuerungen sicher betrieben werden können.
- **Unterstützung bei der Dokumentation:** Kunden erhalten Hilfe bei der Erstellung der notwendigen technischen Dokumentationen.
- **Informationen zu Meldeprozessen:** Leuze erklärt, wie Sicherheitsvorfälle gemeldet werden und welche Schritte im Ernstfall zu beachten sind.



Herbert Köbel

**Senior Expert –
R&D Software**

Leuze electronic GmbH + Co. KG

In der Braike 1, 73277 Owen
T +49 7021 573-0
F +49 7021 573-199
info@leuze.com
www.leuze.de