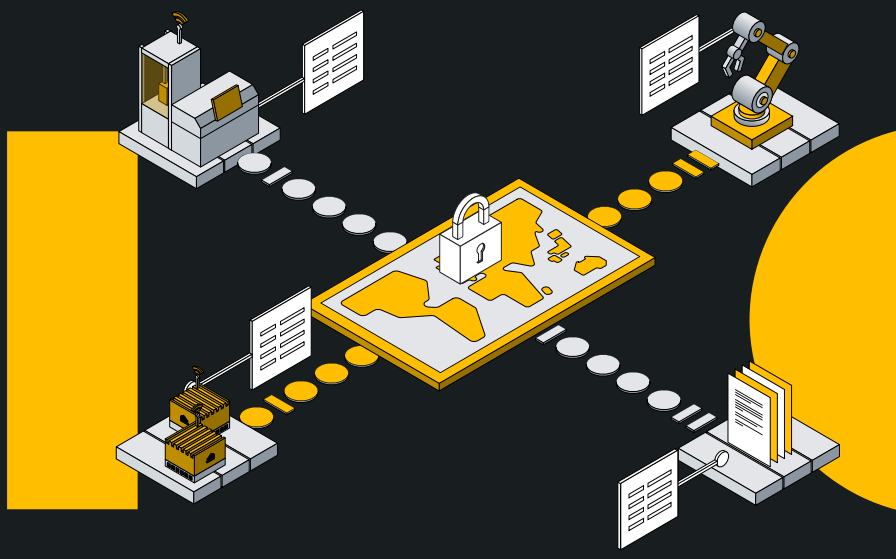
CUMULOCITY

WHITE PAPER

CRA: DIE EU-VERORDNUNG ZUR CYBER-RESILIENZ

Sind die Softwarekomponenten Ihrer Produkte schon konform?



Inhaltsverzeichnis

Zusammenfassung

Das EU-Gesetz zur Cyber-Resilienz (Cyber Resilience Act, CRA) führt verbindliche Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen ein. Es verpflichtet Hersteller dazu, Sicherheit bereits bei der Konzeption zu berücksichtigen, während des gesamten Produktlebenszyklus auf Schwachstellen zu achten und sicherzustellen, dass ihre Produkte bei Bedarf gezielt aktualisiert werden können.

Für Hersteller intelligenter Geräte ist diese Verordnung sowohl eine Herausforderung als auch eine Chance. Die Einhaltung der Vorschriften erfordert sichere Software-Entwicklungspraktiken, die Nachverfolgung von Softwareversionen und die Möglichkeit, auf Schwachstellen effektiv zu reagieren. Bei Nichteinhaltung drohen Geldstrafen von bis zu 15 Millionen Euro oder 2,5 % des weltweiten Umsatzes sowie die mögliche Entfernung vom EU-Markt.

Andererseits können Firmen, die früh ihre Produkte mit dem CRA in Einklang bingen, Wettbewerbsvorteile erlangen. Durch die Entwicklung sicherer und zuverlässiger vernetzter Produkte können Hersteller das Vertrauen ihrer Kunden gewinnen und ihre Position in einem zunehmend sicherheitsbewussten Markt stärken.

Wichtige Meilensteine rücken schnell näher. Der CRA trat am 10. Dezember 2024 in Kraft. Die Meldepflicht für Schwachstellen und Vorfälle gilt ab dem 11. September 2026, und die vollständigen Produktanforderungen gelten ab dem 11. Dezember 2027. Für Hersteller, deren Produktentwicklungs- und Testzyklen sich über Jahre erstrecken, müssen die Vorbereitungen jetzt beginnen.

Einführung

Intelligente Geräte sind mittlerweile stark vernetzt. Industriemaschinen, medizinische Geräte oder Gebäudeautomationssysteme basieren heute auf komplexen Software-Stacks, Cloud-Diensten und Integrationen von Drittanbietern. Während die Vernetzung neue Möglichkeiten eröffnet, vergrößert sie auch die Angriffsfläche für Cyber-Bedrohungen.

Die Europäische Union hat mit dem Cyber Resilience Act (CRA) eine EU-Verordnung geschaffen, um die Mindeststandards für Cybersicherheit anzuheben. Im Gegensatz zu fragmentierten nationalen Vorschriften oder freiwilligen Richtlinien schreibt der CRA einheitliche, harmonisierte Verpflichtungen für den gesamten EU-Markt vor. Die Verordnung verlagert die Verantwortung für die Sicherheit eindeutig auf die Hersteller und stellt sicher, dass vernetzte Geräte von Grund auf sicher sind und während ihres gesamten Lebenszyklus sicher bleiben.

Für Hersteller vernetzter Geräte sind die Auswirkungen klar. Produkte, welche die CRA-Anforderungen nicht erfüllen, können vom Markt genommen werden. Schwachstellen müssen überwacht und behoben werden. Die Einhaltung der Vorschriften erfordert neue Prozesse für die Entwicklung, das Lieferkettenmanagement und den Kundendienst nach der Markteinführung.

Dieses Whitepaper richtet sich an Hersteller intelligenter Geräte, IoT-Führungskräfte, Produktmanager und Compliance-Teams, die die Anforderungen des CRA und deren Bedeutung in der Praxis verstehen müssen.

Worum geht es beim CRA?

Der CRA gilt für alle „Produkte mit digitalen Elementen“ und umfasst alles von IoT-Geräten für Verbraucher bis hin zu Industrieanlagen und integrierter Software. Sein Hauptziel ist es, sicherzustellen, dass Sicherheit kein optionales Merkmal ist, sondern ein integraler Bestandteil der Entwicklung und Wartung vernetzter Produkte.

Geltungsbereich und Verpflichtungen

Gemäß dem CRA müssen Hersteller:

- **Standardmäßig sichere Produkte entwickeln und ausliefern.** Geräte müssen über eine starke Authentifizierung, verschlüsselte Kommunikation, einen sicheren Systemstart und sichere Standardkonfigurationen verfügen.
- **Prozesse zum Schwachstellenmanagement einrichten.** Hersteller müssen Schwachstellen in allen Produktkomponenten überwachen und zeitnah Sicherheitsupdates veröffentlichen, um Risiken zu minimieren, wobei Updates nach Möglichkeit automatisch installiert werden sollten. Darüber hinaus müssen Hersteller eine Richtlinie zur koordinierten Offenlegung von Schwachstellen (CVD) implementieren, die es der Öffentlichkeit ermöglicht, Schwachstellen zu melden, auch wenn diese noch nicht ausgenutzt wurden. Dies unterscheidet sich von der obligatorischen Meldung von Vorfällen an die Behörden und ist für die Förderung von Transparenz und proaktiver Risikominderung von entscheidender Bedeutung.
- **Erkannte Schwachstellen melden.** Wenn eine Schwachstelle erkannt wird, muss sie innerhalb von 24 Stunden an die EU-Agentur für Cybersicherheit (ENISA) gemeldet werden, wobei innerhalb von 72 Stunden eine detaillierte Risikobewertung vorzulegen ist.
- **Die Einhaltung durch Konformitätsprüfung und CE-Kennzeichnung nachweisen.** Bei Standardprodukten können Hersteller in der Regel eine eigene Bewertung vornehmen. Bei „wichtigen“ oder „kritischen“ Produkten ist jedoch eine Bewertung durch eine benannte Stelle erforderlich.

Jeder Hersteller muss einen Wartungszeitraum festlegen, in dem er Schwachstellen behebt. Dieser Zeitraum muss mindestens fünf Jahre betragen, es sei denn, die erwartete Lebensdauer des Produkts ist kürzer.

Fristen und Geldstrafen

Die Verordnung trat im Dezember 2024 in Kraft. Einige Verpflichtungen – wie beispielsweise der Umgang mit Schwachstellen – gelten ab 2026. Die vollständige Einhaltung wird am 11. Dezember 2027 verbindlich.

Die Nichteinhaltung hat erhebliche Konsequenzen. Produkte können vom EU-Markt genommen werden, und Hersteller müssen mit Geldstrafen von bis zu 15 Millionen Euro oder 2,5 % ihres weltweiten Jahresumsatzes rechnen.

Wichtige Aspekte für die Einhaltung der CRA-Vorschriften

Um die Anforderungen des CRA zu erfüllen, müssen Hersteller einen ganzheitlichen, lebenszyklusorientierten Ansatz verfolgen. Sechs Bereiche müssen besonders berücksichtigt werden:

1. Dokumentation und Nachweis der Compliance
Die CRA-Compliance beginnt mit der Dokumentation. Hersteller müssen:

- ein vollständiges Produktinventar führen
- öffentlich zugängliche Dokumentationen bereitstellen, einschließlich Anweisungen für die sichere Außerbetriebnahme (gemäß Artikel 31, Anhang II)
- detaillierte Protokolle über Softwareveränderungen, Updates, Schwachstellenbewertungen und Maßnahmen zur Fehlerbehebung führen.

Diese Dokumentation ist für die erfolgreiche Durchführung von Konformitätsbewertungen und Audits unerlässlich – und oft der Ausgangspunkt für jede CRA-konforme Vorgehensweise.

2. Sichere Entwicklungsprozesse und Risikobewertung
Hersteller müssen sichere Entwicklungsmethoden einführen, die durch produktspezifische Risikobewertungen unterstützt werden. Diese dienen als Leitfaden für die Auswahl und Implementierung von Sicherheitsmaßnahmen wie Gefahrenmodellierung, sichere Codierung und Software-Signierung.

3. Produktsicherheit
Auf Grundlage der Risikobewertung müssen technische Kontrollen implementiert werden, wie:

- Sicherer Startvorgang (Secure Boot)
- Authentifizierte und verschlüsselte Updates
- Verpflichtende sichere Standardeinstellungen
- Manipulationssichere Mechanismen
- Gesicherte Funktion zum Zurücksetzen auf die Werkseinstellungen

Diese sollten bereits in den frühesten Entwicklungsphasen der Produktarchitektur integriert werden.

4. Software-Updates und Schwachstellenmanagement
Hersteller müssen alle Softwarekomponenten – eigene, von Drittanbietern und Open Source – auf Schwachstellen überwachen und sichere Updates bereitstellen, die:

- Verschlüsselt geprüft werden
- Sicherheitspatches von funktionalen Updates trennen,
- nach Möglichkeit eine Versionsrücksetzung unterstützen.

Ein proaktives Schwachstellenmanagement erfordert klare Zuständigkeiten, automatisierte Überwachungstools und schnelle Reaktionsmöglichkeiten.

5. Reaktion auf Vorfälle
Hersteller müssen Sicherheitslücken und schwerwiegende Vorfälle innerhalb der folgenden Fristen an die ENISA und ihr nationales CSIRT melden:

- Erste Meldung innerhalb von 24 Stunden
- Vollständiger technischer Bericht innerhalb von 72 Stunden
- Abschließender Statusbericht innerhalb von 14 Tagen nach Behebung

Dies erfordert einen klar definierten Plan für die Reaktion auf Sicherheitsvorfälle, der technische, rechtliche und kommunikative Teams einbindet.

6. Verantwortlichkeiten in der Lieferkette und Bauteile von Drittanbietern
Der CRA gilt für Open-Source-Komponenten, Commercial Libraries und Integrationen in der Lieferkette. Hersteller müssen:

- Die vollständige Transparenz auf Komponentenebene aufrechterhalten (z. B. SBOMs)
- Kontinuierlich das Risiko offengelegter Schwachstellen bewerten
- Die rechtliche Verantwortung für den in ihren Produkten verwendeten Code von Drittanbietern und Open-Source-Code übernehmen

Importeure und Händler unterliegen ebenfalls den Verpflichtungen des CRA. Wenn sie ein Produkt verändern oder die Marke umbenennen, können sie die volle Verantwortung des Herstellers übernehmen. Hersteller müssen auch „wesentliche Modifikationen“ verwalten – Änderungen, die sich auf die Konformität oder den Verwendungszweck auswirken.

Best Practices für cyber-resiliente intelligente Geräte

Während der CRA die Mindestanforderungen festlegt, können Unternehmen noch mehr tun, um sich Wettbewerbsvorteile zu sichern:

- **Sicherheitsprinzipien anwenden.** Nutzen Sie sichere Standardeinstellungen, Sicherheitsmodelle und eine sichere Programmierung bereits in einer frühen Entwicklungsphase einsetzen.
- **Integrieren Sie Cybersicherheit in DevOps.** Integrieren Sie Sicherheitstests und -scans in CI/CD-Pipelines.
- **Planen Sie einen langfristigen Support.** Definieren Sie klare End-of-Life-Richtlinien, warten Sie die Update-Infrastruktur und kommunizieren Sie Empfehlungen an die Anwender.
- **Risiken kontinuierlich überwachen:** Wiederverwendung von Komponenten nachverfolgen, Bibliotheken und Abhängigkeiten auf Schwachstellen prüfen und eine hohe Update-Bereitschaft sicherstellen.

Die nächsten Schritte für Unternehmen

Um sich auf den CRA vorzubereiten, sollten Sie sich auf diese fünf praktischen Schritte konzentrieren:

1. **Überprüfen Sie Ihr Geräteportfolio auf CRA-Relevanz**
   Identifizieren Sie, welche vernetzten Produkte unter den Geltungsbereich des CRA fallen, und bewerten Sie den aktuellen Sicherheitsreifegrad. Dies schafft eine Grundlage für Risikoabschätzung, Compliance-Planung und potenzielle Plattformunterstützung

2. **Analysieren Sie Ihre Gerätemanagement- und Update-Fähigkeiten**
   Analysieren Sie, wie Updates bereitgestellt, verifiziert und nachverfolgt werden. Moderne Gerätemanagement-Plattformen wie Cumulocity ermöglichen automatisierte OTA-Updates, bieten Transparenz zum Update-Status und stellen revisionssichere Protokolle sicher.

3. **Stellen Sie die SBOM-Verfolgung und Komponenten-Transparenz sicher**
   Der CRA verlangt für jedes Produkt ein vollständiges Software Bill of Materials (SBOM). Stellen Sie sicher, dass Ihre Teams SBOMs erstellen, verwalten und nutzen können, um in Echtzeit auf Bedrohungen zu reagieren.

4. **Nutzen Sie den CRA-Technical Guide von Cumulocity**
   Cumulocity unterstützt die CRA-Konformität durch sichere Updates, vollständige Software-Transparenz in der Geräteflotte und integriertes Risikotracking. Unser Leitfaden „A Practical Reference Architecture for Cyber Resilience Act (CRA) Compliance“ enthält Architekturdiagramme, Compliance-Workflows und praxisnahe Umsetzungshinweise. Fordern Sie Ihr Exemplar an.

5. **Analysieren Sie Ihre CRA-Compliance mit unserem Expertenteam**
   Möchten Sie Ihre aktuelle Ausgangslage mit den CRA-Anforderungen abgleichen? Unsere Produkt- und Compliance-Experten helfen Ihnen, nächste Schritte zu planen und Chancen für Plattformunterstützung zu identifizieren – ohne Vertriebsdruck, mit echtem Mehrwert.

Wie Cumulocity hilft, die CRA-Anforderungen zu erfüllen

Cumulocity bietet eine integrierte Plattform, die Hersteller bei der Erfüllung der CRA-Anforderungen in mehreren zentralen Bereichen unterstützt:

- Flottenweite Gerätetransparenz, einschließlich SBOM-Verfolgung
- Sichere OTA-Update-Bereitstellung, mit Audit-Trails und Rollback-Unterstützung
- Ereignis- und Anomalieüberwachung (z. B. fehlgeschlagene Anmeldungen oder Updates)
- CVE-Korrelation und Schwachstellenverfolgung
- Unterstützung bei Konformitätsbewertungen durch integrierte Dokumentationswerkzeuge

Durch den Einsatz von Cumulocity können Hersteller ihre CRA-Readiness beschleunigen, manuellen Aufwand reduzieren und Unsicherheiten minimieren. Unser Partnernetzwerk umfasst zudem Beratungsunternehmen, die bei Sicherheitsarchitektur und Readiness-Planung unterstützen.

Fazit

Der Cyber Resilience Act (CRA) verändert grundlegend, wie vernetzte Produkte entwickelt, bereitgestellt und unterstützt werden. Die Verordnung bringt zwar neue Komplexität mit sich, zielt am Ende aber auf eine notwendige Verbesserung der Produktsicherheit in einer immer stärker vernetzten Welt. Geschäftsmodelle mit vernetzen Produkten bekommen klare und verlässliche Rahmenbedingungen. Produkte mit klarem Fokus auf den Kundennutzen- und sicherheit werden klar im Vorteil sein, Hersteller, die sich frühzeitig vorbereiten – und mit Plattformen wie Cumulocity zusammenarbei ten – können nicht nur die Compliance sicherstellen, sondern auch ihre Wettbewerbsfähigkeit in einer sicheren und regulierten Zukunft stärken.

Machen Sie den nächsten Schritt

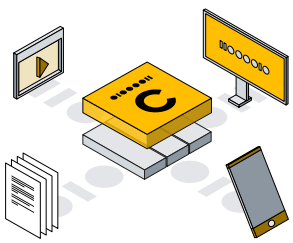
Der Weg zur CRA-Compliance beginnt mit Transparenz und den richtigen Werkzeugen. Warten Sie nicht, bis Fristen bedrohlich näher rücken – handeln Sie jetzt, um Ihre smarten Produkte abzusichern und dem regulatorischen Druck einen Schritt voraus zu sein.

HOLEN SIE SICH EXPERTENHILFE

Möchten Sie wissen, inwieweit Ihre aktuellen Systeme den Anforderungen der CRA entsprechen?

Unser Professional Services Team hilft Ihnen dabei, Ihre Situation zu analysieren und praktische nächste Schritte zu identifizieren.

Talk to an expert



Quellen

Offizielle Referenzen:

- EU Cyber Resilience Act (EU 2024/2847)
- ENISA/JRC CRA Requirements Mapping Document

Glossar

- **SBOM (Software Bill of Materials):** Eine Liste der Softwarekomponenten in einem Produkt.
- **OTA (Over-the-Air):** Fernübertragung von Firmware- oder Software-Updates.
- **Secure Boot:** Prozess zur Sicherstellung der Geräteintegrität beim Start
- **CVE (Common Vulnerabilities & Exposures):** Veröffentlichte Sicherheitslücken