EU Cyber Resilience Act

Neue Cybersecurity-Standards für digitale Produkte

Executive Whitepaper

Ralf Platvoet
Remscheid
Februar 2026

Executive Summary

Der EU Cyber Resilience Act (CRA) ist die erste EU-Verordnung, die ein Mindestniveau an Cybersecurity für alle vernetzten Produkte auf dem EU-Markt festlegt. Die Verordnung trat am 10. Dezember 2024 in Kraft und wird schrittweise bis Dezember 2027 vollständig anwendbar.

Kernpunkte:

- **Betrifft alle digitalen Produkte** – von Smartphones über Smart-Home-Geräte bis zu industriellen Steuerungssystemen
- **Lebenszyklus-Ansatz** – Hersteller müssen Sicherheit von Design bis End-of-Life gewährleisten
- **Strenge Bußgelder** – bis zu 15 Mio. EUR oder 2,5% des weltweiten Jahresumsatzes
- **Meldepflichten** – aktiv ausgenutzte Schwachstellen müssen binnen 24 Stunden gemeldet werden

Hersteller, Importeure und Händler digitaler Produkte müssen jetzt handeln, um ihre Produkte CRA-konform zu gestalten und rechtzeitig auf dem EU-Markt halten zu können.

Was ist der EU Cyber Resilience Act?

Der Cyber Resilience Act (Regulation (EU) 2024/2847) ist eine EU-Verordnung, die horizontale Cybersecurity-Anforderungen für Produkte mit digitalen Elementen festlegt. Anders als eine Richtlinie gilt die Verordnung direkt in allen EU-Mitgliedstaaten, ohne dass sie in nationales Recht umgesetzt werden muss.

Ziel ist es, Verbraucher und Unternehmen vor unsicheren digitalen Produkten zu schützen und ein einheitliches Sicherheitsniveau im EU-Binnenmarkt zu schaffen.

Welche Produkte sind betroffen?

Der CRA gilt für alle **Produkte mit digitalen Elementen** (Products with Digital Elements, PDE), deren bestimmungsgemäßer oder vorhersehbarer Gebrauch eine direkte oder indirekte Datenverbindung zu einem Gerät oder Netzwerk umfasst.

Beispiele für betroffene Produkte

Consumer-Produkte:

- Smartphones, Tablets, Laptops
- Smart-Home-Geräte (Thermostaten, Kameras, Babyphones)
- Wearables (Smartwatches, Fitness-Tracker)

- Vernetztes Spielzeug

Software & Cloud-Services:

- Mobile Apps und Desktop-Anwendungen
- Betriebssysteme und Firmware
- SaaS-Lösungen mit Fernverarbeitung

Industrielle & kritische Produkte:

- Industrielle Steuerungssysteme (ICS/SCADA)
- Netzwerkkomponenten (Router, Switches, Firewalls)
- Mikrocontroller und Mikroprozessoren
- Smart Meter Gateways

Ausnahmen

Der CRA gilt nicht für:

- Medizinprodukte (unterliegen eigenen EU-Vorschriften)
- Fahrzeuge (unterliegen spezieller Regulierung)
- Luftfahrtprodukte
- Nicht-kommerzielle Open-Source-Software (kommerzielle Varianten unterliegen dem CRA)

Produktkategorien und Konformitätsbewertung

Der CRA unterscheidet zwischen drei Produktkategorien mit unterschiedlichen Compliance-Anforderungen:

Kategorie	Konformitätsbewertung
Standard-Produkte	**Selbstbewertung durch Hersteller** Beispiele: Haushaltsgeräte, Computerspiele, Mobile Apps
Wichtige Produkte (Class I)	**Externe Prüfung durch benannte Stelle** Beispiele: Browser, Passwort-Manager, VPN-Software
Kritische Produkte (Class II)	**Externe Prüfung + zusätzliche Zertifizierung** Beispiele: Betriebssysteme, Mikroprozessoren, Smart Cards, Firewalls

CE-Kennzeichnung: Nach erfolgreicher Konformitätsbewertung müssen Hersteller die CE-Kennzeichnung anbringen und eine EU-Konformitätserklärung ausstellen.

Wesentliche Cybersecurity-Anforderungen

Der CRA definiert in Annex I zwei Kategorien wesentlicher Anforderungen, die Hersteller erfüllen müssen:

1. Produkt-Cybersecurity-Anforderungen

Produkte müssen so konzipiert, entwickelt und hergestellt werden, dass sie:

- **Frei von bekannten Schwachstellen** sind (beim Inverkehrbringen)
- **Sichere Standardkonfiguration** aufweisen (Secure by Default)
- **Vertraulichkeit, Integrität und Verfügbarkeit** von Daten schützen
- **Angriffsfläche minimieren** (nur notwendige Funktionen und Schnittstellen)
- **Robuste Zugriffskontrolle** implementieren
- **Sicherheitslogs** zur Vorfallserkennung bereitstellen
- **Widerstandsfähig gegen Cyberangriffe** sind
- **Automatische Sicherheitsupdates** ermöglichen

2. Anforderungen an Schwachstellen-Management

Hersteller müssen über den gesamten Produktlebenszyklus:

- **Schwachstellen identifizieren und dokumentieren**
- **Sicherheitsupdates zeitnah bereitstellen** (für mindestens 5 Jahre oder erwartete Produktlebensdauer)
- **Koordinierte Offenlegung** von Schwachstellen ermöglichen
- **Nutzer über Sicherheitsrisiken informieren**

Meldepflichten

Ab dem 11. September 2026 müssen Hersteller aktiv ausgenutzte Schwachstellen und erhebliche Sicherheitsvorfälle über eine zentrale EU-Meldeplattform melden.

Frist	Anforderung
24 Stunden	Meldung an ENISA und zuständige CSIRT bei aktiv ausgenutzten Schwachstellen
Unverzüglich	Information betroffener Nutzer über Sicherheitsrisiken und Schutzmaßnahmen

Wichtig: Diese Meldepflichten gelten für alle Produkte auf dem EU-Markt, auch für solche, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden.

Sanktionen bei Nichteinhaltung

Der CRA sieht erhebliche Bußgelder bei Verstößen vor:

- **Bis zu 15 Mio. EUR oder 2,5% des weltweiten Jahresumsatzes** (je nachdem, welcher Betrag höher ist)

Verstöße umfassen unter anderem:

- Inverkehrbringen nicht-konformer Produkte
- Verletzung der Meldepflichten
- Fehlende oder mangelhafte technische Dokumentation
- Falsche oder irreführende CE-Kennzeichnung

Ausnahme: Bußgelder gelten nicht für nicht-kommerzielle Open-Source-Entwickler.

Zeitplan und Umsetzung

- **10. Dezember 2024:** CRA tritt in Kraft
- **11. Juni 2026:** Benannte Prüfstellen müssen eingerichtet sein
- **11. September 2026:** Meldepflichten für Schwachstellen und Vorfälle greifen
- **11. Dezember 2027: Alle CRA-Anforderungen sind vollständig anwendbar**

Wichtig: Produkte, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden, sind nur bei wesentlichen Änderungen CRA-pflichtig. Meldepflichten gelten jedoch für alle Produkte auf dem Markt.

Handlungsempfehlungen für Hersteller

Kurzfristig (0-6 Monate)

- **Scoping:** Identifizieren Sie alle betroffenen Produkte in Ihrem Portfolio
- **Klassifizierung:** Prüfen Sie, ob Ihre Produkte als Standard, Wichtig oder Kritisch eingestuft werden
- **Gap-Assessment:** Vergleichen Sie bestehende Sicherheitsmaßnahmen mit CRA-Anforderungen
- **Risikoanalyse:** Führen Sie Cybersecurity-Risikobewertungen für Ihre Produkte durch

Mittelfristig (6-18 Monate)

- **Secure by Design:** Integrieren Sie Sicherheitsanforderungen in Produktentwicklung und -design
- **Schwachstellen-Management:** Etablieren Sie Prozesse für Vulnerability Disclosure und Patch Management
- **Lieferkette:** Stellen Sie sicher, dass Zulieferer und Komponenten CRA-konform sind
- **Dokumentation:** Erstellen Sie umfassende technische Dokumentation für Konformitätsbewertung

- **Update-Strategie:** Planen Sie automatische Sicherheitsupdates über den Produktlebenszyklus

Langfristig (18-36 Monate)

- **Konformitätsbewertung:** Führen Sie die erforderliche Konformitätsbewertung durch (intern oder extern)
- **CE-Kennzeichnung:** Bringen Sie CE-Kennzeichnung an und erstellen Sie EU-Konformitätserklärung
- **Incident Response:** Richten Sie Prozesse für 24-Stunden-Meldepflicht ein
- **Kontinuierliche Überwachung:** Etablieren Sie Monitoring für Schwachstellen und Bedrohungen

Besonderheiten für Open-Source-Software

Der CRA enthält spezielle Regelungen für Open-Source-Software (FOSS):

- **Nicht-kommerzielle FOSS:** Von CRA-Anforderungen ausgenommen
- **Kommerzielle FOSS-Nutzung:** Unterliegt dem CRA, wenn sie kommerziell vertrieben wird
- **Open Source Steward:** Neue Rolle für Organisationen, die FOSS-Projekte verwalten
- **Freiwillige Sicherheitszertifizierung:** Artikel 25 ermöglicht freiwillige Security Attestation Programme für FOSS

Fazit

Der EU Cyber Resilience Act ist ein Meilenstein für Produktsicherheit in der digitalen Wirtschaft. Er schafft einheitliche Standards für Cybersecurity über den gesamten Produktlebenszyklus hinweg – von der Entwicklung über die Markteinführung bis zum End-of-Life.

Für Hersteller, Importeure und Händler bedeutet der CRA erhebliche Compliance-Anforderungen, aber auch eine Chance, Vertrauen bei Kunden aufzubauen und Wettbewerbsvorteile durch sichere Produkte zu erzielen.

Handeln Sie jetzt: Mit dem Stichtag 11. Dezember 2027 bleibt wenig Zeit. Unternehmen sollten frühzeitig Gap-Assessments durchführen, Produktentwicklungsprozesse anpassen und Konformitätsbewertungen vorbereiten.

Weiterführende Informationen

- **Offizielle EU-Seite zum CRA:** https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

- **CRA-Verordnung (Volltext):** Regulation (EU) 2024/2847
- **ENISA Standards Mapping:** Cyber Resilience Act Requirements Standards Mapping
- **BSI-Informationen (Deutschland):** https://www.bsi.bund.de/EN/Themen/Cyber_Resilience_Act/

Dieses Whitepaper dient ausschließlich Informationszwecken und stellt keine Rechtsberatung dar.