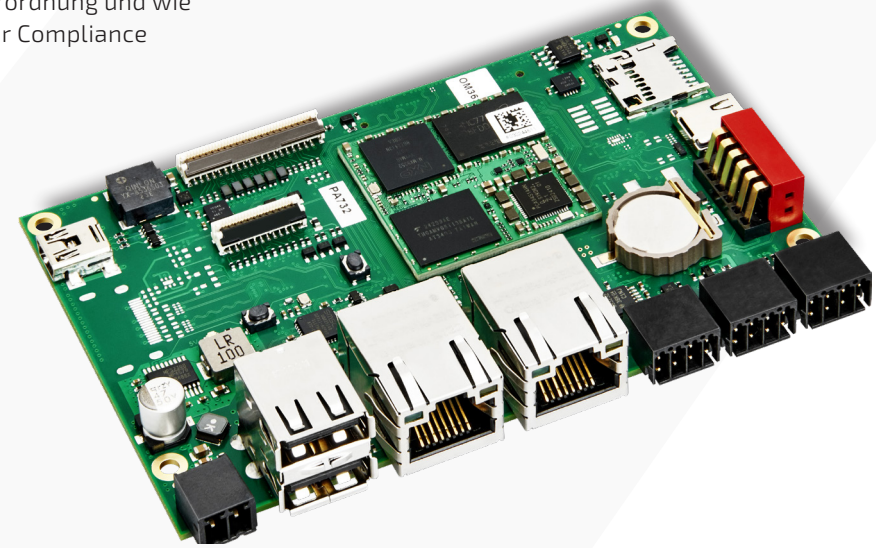
Whitepaper

Cyber Resilience Act (CRA)

Was Unternehmen jetzt wissen und tun sollten

Ihr Leitfaden zur EU-Cybersicherheitsverordnung und wie wir als IoT-Spezialist Sie auf dem Weg zur Compliance begleiten.



15 MIO. EUR

› max. Bußgeld bei Verstößen

DEZ. 2027

› Volle Anwendbarkeit

> 90%

› aller digitalen Produkte betroffen

kontron

The Power of IoT

Executive Summary

Der Cyber Resilience Act (CRA) ist die erste EU-weite Verordnung, die verbindliche Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen festlegt. Sie betrifft Hersteller, Importeure und Händler gleichermaßen.

Auf einen Blick: Das Wichtigste zum CRA

- Gilt für alle Produkte mit digitalen Elementen, die in der EU in Verkehr gebracht werden
- Hersteller müssen Cybersicherheit über den gesamten Produktlebenszyklus sicherstellen
- Bußgelder bis zu 15 Mio. EUR oder 2,5 % des weltweiten Jahresumsatzes des Vorjahres
- Volle Anwendbarkeit ab Dezember 2027
- Jetzt ist der richtige Zeitpunkt zu handeln!

1. Hintergrund: Warum der CRA?

Ransomware, Lieferkettenangriffe und Schwachstellen in vernetzten Geräten verursachen jährlich Schäden in Milliardenhöhe. Gleichzeitig fehlte bislang ein einheitlicher EU-weiter Standard, der sicherstellt, dass Produkte bereits beim Inverkehrbringen sicher sind.

Der CRA schließt diese Lücke. Er ergänzt bestehende Regelwerke wie die NIS-2-Richtlinie und schafft einen verbindlichen Rahmen für die Produktsicherheit.

1.1 Was ist der Cyber Resilience Act?

Der Cyber Resilience Act wurde im Oktober 2024 im Amtsblatt der EU veröffentlicht und ist im Dezember 2024 in Kraft getreten. Er etabliert erstmals harmonisierte Cybersicherheitsanforderungen für Produkte mit digitalen Elementen. Darunter sind Smart-Home-Geräte über Industriesteuerungen bis hin zu Software.

1.2 Wen betrifft der CRA?

Der CRA gilt grundsätzlich für alle wirtschaftlichen Akteure in der Lieferkette:

HERSTELLER	Trägt die Hauptverantwortung: Konformitätsbewertung, CE-Kennzeichnung, technische Dokumentation, Schwachstellen-Management.
IMPORTEURE	Stellen sicher, dass nur konforme Produkte in die EU eingebracht werden.
HÄNDLER	Prüfen, ob Produkte die CRA-Anforderungen erfüllen, bevor sie vertrieben werden.
OPEN-SOURCE-ENTWICKLER	Weitgehend ausgenommen, sofern keine kommerzielle Tätigkeit vorliegt.

2. Zeitplan & Fristen

Unternehmen sollten jetzt mit der Umsetzung beginnen, da die Konformitätsbewertung und technische Dokumentation erhebliche Vorlaufzeit erfordern.

DATUM	MEILENSTEIN	BESCHREIBUNG
DEZ. 2024	Inkrafttreten	CRA tritt offiziell in Kraft
SEP. 2026	Reporting-Pflichten	Meldepflichten bei aktiv ausgenutzten Schwachstellen gelten
DEZ. 2027	Vollständige Anwendung	Alle Anforderungen vollständig anwendbar

Obwohl die volle Anwendbarkeit erst ab Dezember 2027 gilt, sollten Unternehmen spätestens Mitte 2026 mit der Implementierung beginnen, da Konformitätsbewertungsverfahren mehrere Monate in Anspruch nehmen können.

Produkte, die vor Dezember 2027 in Verkehr gebracht wurden, können unter bestimmten Bedingungen übergangsgemäß behandelt werden.

3. Die wichtigsten Anforderungen im Überblick

Der CRA definiert grundlegende Anforderungen an die Cybersicherheit in Anhang I und Anhängen II-IV. Diese lassen sich in drei Hauptbereiche gliedern:

3.1 Sicherheit durch Design (Security by Design)

Hersteller müssen sicherstellen, dass Produkte mit einem angemessenen Cybersicherheitsniveau ausgeliefert werden. Dazu gehören:

- Reduzierung der Angriffsoberfläche (Attack Surface Reduction)
- Schutz vor unbefugtem Zugriff, inkl. Authentifizierungsmechanismen
- Verschlüsselung sensibler Daten im Übertragungsweg und im Ruhezustand
- Sichere Standardkonfigurationen (Secure by Default)
- Keine bekannten ausnutzbaren Schwachstellen bei Markteinführung
- Minimierung der Abhängigkeiten von Drittkomponenten (inkl. Open-Source)

3.2 Schwachstellen-Management über den Lebenszyklus

Hersteller sind verpflichtet, Sicherheitsupdates für mindestens 5 Jahre (oder die erwartete Nutzungsdauer) bereitzustellen. Konkret bedeutet das:

- Meldung aktiv ausgenutzter Schwachstellen innerhalb von 24 Stunden an ENISA und nationale Behörden
- Weitergabe relevanter Informationen an betroffene Nutzer
- Bereitstellung von Sicherheitsupdates

3.3 Transparenz & Dokumentation

Hersteller müssen umfassende technische Dokumentation erstellen und eine Software Bill of Materials (SBOM) führen:

- Software-Stückliste (SBOM) aller Komponenten, Bibliotheken und Abhängigkeiten
- Technische Dokumentation gemäß Anhang VII des CRA
- EU-Konformitätserklärung und CE-Kennzeichnung
- Klare Nutzerinformationen zu Cybersicherheitseigenschaften und Updates

4. Produktkategorien & Risikoeinstufung

Der CRA unterscheidet zwischen Standard-Produkten und kritischen Produkten. Je höher die Risikoklasse, desto strenger die Konformitätsbewertung:

KATEGORIE	BEISPIELE	BEWERTUNGSVERFAHREN
STANDARD-PRODUKTE (DEFAULT)	Smart-TVs, Drucker, Smart-Home-Geräte	Selbstbewertung durch Hersteller
KRITISCH KLASSE I	Passwortmanager, Firewalls, Router	Harmonisierte Standards oder Drittprüfung
KRITISCH KLASSE II	Industrie-SCADA, PKI, Hardware-Sicherheitsmodule (HSM)	Zertifizierung durch akkreditierte Stelle

5. Bußgelder & Konsequenzen bei Verstößen

Der CRA sieht empfindliche Sanktionen vor. Marktaufsichtsbehörden können nicht-konforme Produkte vom Markt nehmen und erhebliche Bußgelder verhängen:

VERSTOSS	MAX. BUSSGELD
Verstöße gegen wesentliche Sicherheitsanforderungen	15 MIO. EUR ODER 2,5 % DES WELTWEITEN JAHRESUMSATZES
Verstöße gegen sonstige Pflichten (z.B. Meldepflichten)	10 MIO. EUR ODER 2 % DES WELTWEITEN JAHRESUMSATZES
Falsche oder irreführende Informationen gegenüber Behörden	5 MIO. EUR ODER 1 % DES WELTWEITEN JAHRESUMSATZES

6. Was Unternehmen jetzt tun müssen

Die CRA-Compliance ist kein einmaliges Projekt, sondern ein fortlaufender Prozess. Wir empfehlen folgende strukturierte Vorgehensweise:

Schritt 1: Bestandsaufnahme & Gap-Analyse (jetzt sofort)

- Alle digitalen Produkte und Komponenten erfassen
- CRA-Risikoklasse für jedes Produkt bestimmen
- Bestehende Sicherheitsmaßnahmen gegen CRA-Anforderungen abgleichen
- Fehlende Dokumentation identifizieren (SBOM, technische Dokumentation)

Schritt 2: Organisatorische Maßnahmen

- Interne Meldeprozesse für Schwachstellen einrichten (24h-Meldekette)
- Verantwortlichkeiten für Produktsicherheit klar definieren
- Schulungen für Entwicklungs- und Compliance-Teams durchführen

Schritt 3: Technische Umsetzung

- Security by Design in Entwicklungsprozesse integrieren
- SBOM-Tooling einführen und Bestandsaufnahme aller Softwareabhängigkeiten
- Patch- und Update-Management-Prozesse aufbauen
- Penetrationstests und Sicherheitsprüfungen durchführen

Schritt 4: Konformitätsbewertung & Zertifizierung (Ab Q3 2026)

- Technische Dokumentation gemäß Anhang VII erstellen
- EU-Konformitätserklärung ausstellen
- CE-Kennzeichnung anbringen
- Ggf. externe Zertifizierungsstelle beauftragen (für Klasse I/II)

7. Wie wir als IoT-Spezialist unterstützen

Wir bieten unseren Kunden und Partnern ein umfassendes Portfolio an Unterstützungsleistungen.

LEISTUNG	DETAILS
SICHERE HARDWARE BY DESIGN	Tamper-Resistant-Module, Secure Boot, HSM-Integration
PATCH & UPDATE MANAGEMENT	Signierte Firmware-Updates, Remote-Management-Fähigkeit
TRANSPARENZ & DOKUMENTATION	SBOM-Unterstützung, CE-Dokumentation, technische Unterlagen
SCHWACHSTELLEN-MANAGEMENT	Koordinierte Offenlegung, 24h Melde-Support, Hotfix-Prozesse
ZERTIFIZIERUNG & COMPLIANCE	Vorbereitung auf EU-Konformitätsbewertung, Prüflaborunterstützung
SCHULUNG & BERATUNG	CRA-Readiness-Workshops, Gap-Analysen, Roadmap-Erstellung

7.1 Sichere Hardware als Fundament Ihrer Compliance

Cybersicherheit beginnt bei der Hardware. Unsere Produkte sind von Grund auf nach dem Prinzip „Security by Design“ entwickelt und bieten folgende sicherheitsrelevanten Eigenschaften:

Hardware-Sicherheitsfunktionen

- Secure Boot & Trusted Platform Module (TPM)
- Hardware Security Module (HSM) Integration
- Tamper Detection & Physical Protection
- Isolierte Sicherheitszonen (TrustZone)
- Kryptographische Beschleunigeranwendungen

Software & Update-Infrastruktur

- Signierte Firmware & Over-the-Air Updates
- Rollback-Schutz & Versionsverwaltung
- Remote Device Management
- Sichere Speicherung von Schlüsseln
- Automatisierte Sicherheitsprüfung im Build

7.2 Transparenz & SBOM-Unterstützung

Die Software Bill of Materials (SBOM) ist eine der zentralen Anforderungen des CRA. Wir helfen Ihnen, eine vollständige und aktuelle SBOM aufzubauen:

- Lieferung unserer Produkte mit vollständiger Komponenten-SBOM im SPDX- oder CycloneDX-Format
- Reguläre Updates der SBOM bei Änderungen an Firmware oder Software
- Unterstützung beim Aufbau eigener SBOM-Prozesse in Ihrer Lieferkette

7.3 Schwachstellen-Management & Meldeprozesse

Unser Schwachstellen-Management unterstützt Sie bei der Einhaltung der strikten Meldepflichten des CRA:

- Proaktive Benachrichtigung bei neu entdeckten Schwachstellen in unseren Produkten
- Priorisierte Bereitstellung von Sicherheitspatches für kritische Schwachstellen
- Unterstützung bei der Kommunikation mit ENISA und nationalen Behörden

Über Kontron

Die Kontron AG ist ein führendes IoT-Technologieunternehmen. Seit mehr als 20 Jahren unterstützt Kontron Unternehmen aus den unterschiedlichsten Branchen dabei, mit intelligenten Lösungen wirtschaftliche Ziele zu erreichen. Von automatisierten industriellen Abläufen, intelligenterem und sicherem Transportwesen bis hin zu fortschrittlichen Kommunikations-, Konnektivitäts-, Medizin- und Energielösungen bietet das Unternehmen seinen Kunden wertschöpfende Technologien. Mit der Übernahme der Katek SE Anfang 2024 stärkt Kontron das Portfolio durch die neue Division GreenTec mit den Bereichen Solarenergie und eMobility maßgeblich und beschäftigt rund 8.000 Mitarbeiterinnen und Mitarbeiter in mehr als 20 Ländern weltweit. Kontron ist im SDAX® sowie TecDAX® der Deutschen Börse gelistet.

Weitere Informationen finden Sie unter: **www.kontron.de**

Über Kontron Electronics

Kontron Electronics GmbH ist ein Full-Service-Dienstleister in der Elektronikbranche und bietet umfassende Leistungen in Entwicklung, Rapid Prototyping und Fertigung. Das Unternehmens-Portfolio umfasst firmeneigene und kundenspezifische Produkte, Entwicklungs- und Konstruktionsdienstleistungen komplexer Elektronik-Komponenten, -Module und -Systeme sowie Produktions- und Montagedienstleistungen für komplette Baugruppen. Das Unternehmen ist Teil des Technologiekonzerns Kontron AG.

Für weitere Informationen besuchen Sie bitte: **www.kontron-electronics.de**

Ihr Kontakt

Kontron Electronics GmbH

Max-Planck-Straße 6
72636 Frickenhausen, Germany
Tel.: +49 7022 4057-0
info@kontron-electronics.de

www.kontron-electronics.de

Global Headquarters

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: +49 821 4086-0
info@kontron.com

www.kontron.com

kontron
The Power of IoT