TÜV AUSTRIA

CLOCKWORKX

FACT SHEET

Cyber Resilience Act

Was Sie wirklich über den CRA wissen müssen

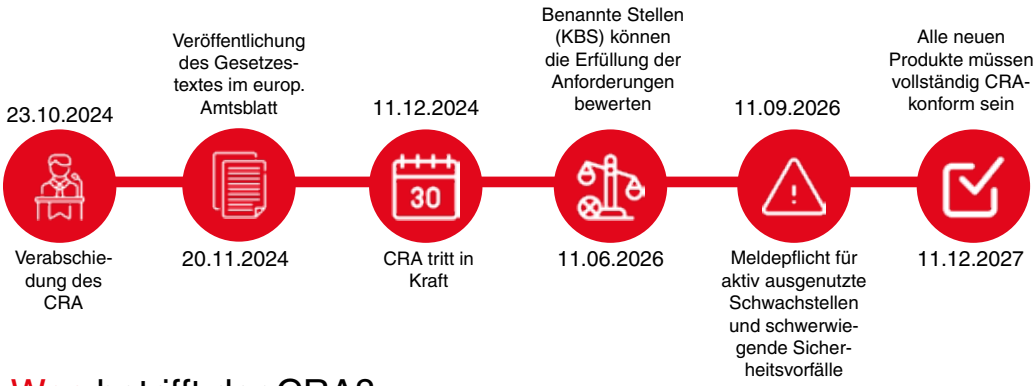
Fakten im Überblick

Was ist der CRA und warum ist er wichtig?

Der Cyber Resilience Act ist eine EU-Verordnung, die erstmals verbindliche Mindeststandards für die Cybersicherheit von Produkten mit digitalen Elementen festlegt. Dazu gehören Hardware, Software und vernetzte Geräte. Ziel ist es, Sicherheitslücken zu reduzieren, die Resilienz gegenüber Cyberangriffen zu erhöhen und die Transparenz für Hersteller und Nutzer zu verbessern. Unternehmen müssen künftig nachweisen, dass ihre Produkte sicher entwickelt, gewartet und aktualisiert werden.

Ab wann gelten die neuen Regularien

Die Umsetzung erfolgt schrittweise:



Wen betrifft der CRA?

- Hersteller von Produkten mit digitalen Elementen (Hardware, Software, IoT-Geräte).
- Importeure und Händler, die solche Produkte in der EU bereitstellen.
- Anbieter von Remote-Datenverarbeitungssystemen (z. B. Cloud-Dienste, SaaS).
- Unternehmen weltweit, sofern ihre Produkte in der EU vermarktet werden.

Ausnahmen:

- Medizinprodukte, Fahrzeuge, zivile Luftfahrt, nationale Sicherheit.
- Kostenlose Open-Source-Software ohne Gewinnerzielungsabsicht.

Welche Anforderungen müssen erfüllt werden?

Security by Design & Default:

Sicherheit von Anfang an in Entwicklung und Produktion integrieren.

Risikobewertung:

Bedrohungen analysieren und dokumentieren.

SBOM (Software Bill of Materials):

Alle verwendeten Software-Komponenten transparent machen.

Schwachstellenmanagement & Meldepflicht:

Prozesse für die Erkennung, Behebung und Meldung von Schwachstellen etablieren.

Updates bereitstellen:

Kostenlose Sicherheitsupdates für mindestens fünf Jahre.

CE-Kennzeichnung & EU-Konformität:

Nachweis der Erfüllung aller Anforderungen.

Welche Maßnahmen müssen Hersteller und Händler nun umsetzen?

- Integration der CRA-Anforderungen in die Produktentwicklung: Sicherheitsprinzipien (Security by Design & Default) von Beginn an berücksichtigen.
- Risikobewertung durchführen: Bedrohungen identifizieren und dokumentieren.
- SBOM-Tools einführen: Transparenz über alle Software-Komponenten sicherstellen.
- Prozesse für Schwachstellenmanagement etablieren: Meldung und Behebung von Sicherheitslücken gemäß den Meldefristen.
- Update-Strategie definieren: Kostenlose Sicherheitsupdates für mindestens fünf Jahre bereitstellen

TÜV AUSTRIA

CLOCKWORKX

TÜV AUSTRIA clockworkX

Wir bei clockworkx GmbH sind überzeugt: Die digitale Transformation gelingt nur, wenn Sicherheit und Zuverlässigkeit von Anfang an mitgedacht werden. Als Teil der TÜV AUSTRIA Gruppe verbinden wir technologische Expertise mit einem ganzheitlichen Ansatz, um Unternehmen dabei zu unterstützen, ihre Systeme sicher, resilient und zukunftsfähig zu gestalten. Unser Ziel ist es, Risiken zu minimieren, Compliance sicherzustellen und nachhaltige Lösungen für eine vernetzte Welt zu schaffen.

TÜV AUSTRIA clockworkX GmbH
Alte Landstr.23, 85521 Ottobrunn
info@tuvaustria.com
www.clockworkx.de | www.tuv.at

Jetzt Quick-Check buchen