Der Countdown läuft: Sind Sie bereit für die ersten CRA-Pflichten?

Ab dem 11. September 2026 greifen die ersten verbindlichen Pflichten des Cyber Resilience Act (CRA): Hersteller von Produkten mit digitalen Elementen müssen aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle strukturiert, fristgerecht und über die zentrale EU-Meldeplattform melden. Für viele Unternehmen ist das der erste konkrete Stresstest ihrer CRA-Readiness.

Warum jetzt handeln?

Die Meldepflichten nach Art. 14 CRA erfordern, Sicherheitsereignisse schnell zu erkennen und zu bewerten, Verantwortlichkeiten zu klären sowie belastbare technische Informationen fristgerecht bereitzustellen. Fehlende Zuständigkeiten, Kommunikationswege und Nachweise kosten im Ereignisfall wertvolle Zeit und erhöhen regulatorische, operative und reputative Risiken.

Wer ist betroffen?

Die Meldepflicht gilt für alle Hersteller digitaler Produkte auf dem EU-Markt.

Dazu zählen insbesondere:

- Softwarehersteller
- IoT- und Smart-Device-Hersteller
- Maschinenbauer mit vernetzter Steuerung
- Hersteller von Medizingeräten mit Software (soweit keine vorrangige sektorale Regelung greift)
- Industrie-4.0-Komponenten
- Netzwerkkomponenten und Embedded Systems

Wichtig: Auch Hersteller außerhalb der EU sind betroffen, wenn sie ihre Produkte in der EU anbieten.

Was muss gemeldet werden?

AKTIV AUSGENUTZTE SCHWACHSTELLEN

Eine Meldung ist erforderlich, wenn:

- eine Schwachstelle in einem eigenen Produkt bekannt wird,
- diese aktiv von Angreifern ausgenutzt wird,
- und der Hersteller davon Kenntnis erlangt.

Wichtig: Nicht jede Schwachstelle ist meldepflichtig. Ein CVE-Eintrag oder das Ergebnis eines Penetrationstests allein löst keine Meldepflicht aus.

SCHWERE SICHERHEITSVORFÄLLE

Meldepflichtig können außerdem Sicherheitsvorfälle sein, die die Produktsicherheit betreffen und erhebliche Auswirkungen haben, beispielsweise:

- Lieferkettenangriffe
- kompromittierte Firmware-Updates
- Angriffe auf Update-Server
- Verbreitung von Malware über Produkte

www.tuv.com/c-r-a

TÜV Rheinland

Welche Fristen gelten?

DER CRA SIEHT EINEN MEHRSTUFIGEN MELDEPROZESS VOR:

INNERHALB VON 24 STUNDEN
Frühwarnung (Early Warning):
Erste Informationen zum Sicherheitsvorfall müssen gemeldet werden.

INNERHALB VON 72 STUNDEN
Detaillierte Meldung:
Ergänzung um technische Informationen, Auswirkungen und Gegenmaßnahmen.

NACH ABSCHLUSS DER UNTERSUCHUNG
Abschlussbericht:
Dokumentation von Ursache, Auswirkungen und umgesetzten Maßnahmen.

Wichtig: Die Frist beginnt, sobald der Hersteller Kenntnis von einem meldepflichtigen Ereignis erlangt.

Was sollen Hersteller jetzt prüfen?

Um die Anforderungen erfüllen zu können, sollten Unternehmen frühzeitig sicherstellen, dass:

- Sicherheitsvorfälle erkannt und bewertet werden können
- Verantwortlichkeiten klar definiert sind
- Meldeprozesse dokumentiert sind
- technische Informationen kurzfristig verfügbar sind
- Incident-Response-Prozesse etabliert sind

Sind Sie auf die ersten CRA-Pflichten vorbereitet?

UNSERE CRA-EXPERT*INNEN UNTERSTÜTZEN SIE DABEI,

- ✔ den Handlungsbedarf Ihres Unternehmens zu bewerten
- ✔ CRA-Anforderungen einzuordnen
- ✔ bestehende Prozesse zu überprüfen
- ✔ Melde- und Incident-Response-Prozesse aufzubauen

Häufige Missverständnisse

VIELE UNTERNEHMEN GEHEN ZUNÄCHST VON FALSCHEN ANNAHMEN AUS.

„Jede Schwachstelle muss gemeldet werden."
Nein. Meldepflichtig sind ausschließlich aktiv ausgenutzte Schwachstellen.

„Die Meldepflicht gilt erst ab Dezember 2027."
Nein. Die Anforderungen aus Artikel 14 CRA gelten bereits ab dem 11. September 2026.

„Nur Hersteller kritischer Produkte sind betroffen."
Nein. Grundsätzlich gilt die Meldepflicht für alle Hersteller, deren Produkte unter den Anwendungsbereich des Cyber Resilience Act fallen.

Bereiten Sie Ihr Unternehmen frühzeitig auf die neuen CRA-Anforderungen vor.

Sprechen Sie mit unseren CRA-Expert*innen

Kontaktdaten
TÜV Rheinland i-sec GmbH
Am Grauen Stein · 51105 Köln
Tel. 0800 806 9000 3000
service@i-sec.tuv.com

www.tuv.com/c-r-a

TÜV Rheinland