Deloitte.

Cyber Resilience Act (CRA)

Die EU-Verordnung zur Cyber-Sicherheit von Produkten mit digitalen Elementen

Was ist der CRA?

Der Cyber Resilience Act (CRA) ist die EU-Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Hardware und Software wie zum Beispiel vernetzte Geräte, Apps oder eingebettete Software) und deren Remote-Datenverarbeitungslösungen.

Erstmals werden EU-weit verbindliche Anforderungen u. a. an:

- die sichere Entwicklung („security by design"),
- das Schwachstellenmanagement sowie
- die Bereitstellung von Sicherheitsupdates

für Produkte festgelegt, die in der EU in Verkehr gebracht oder bereitgestellt werden.

Während sich bestehende Regelungen primär auf Organisationen (z.B. NIS2) konzentrieren, adressiert der CRA direkt die Cyber-Sicherheit von Produkten selbst über deren gesamten Lebenszyklus hinweg.

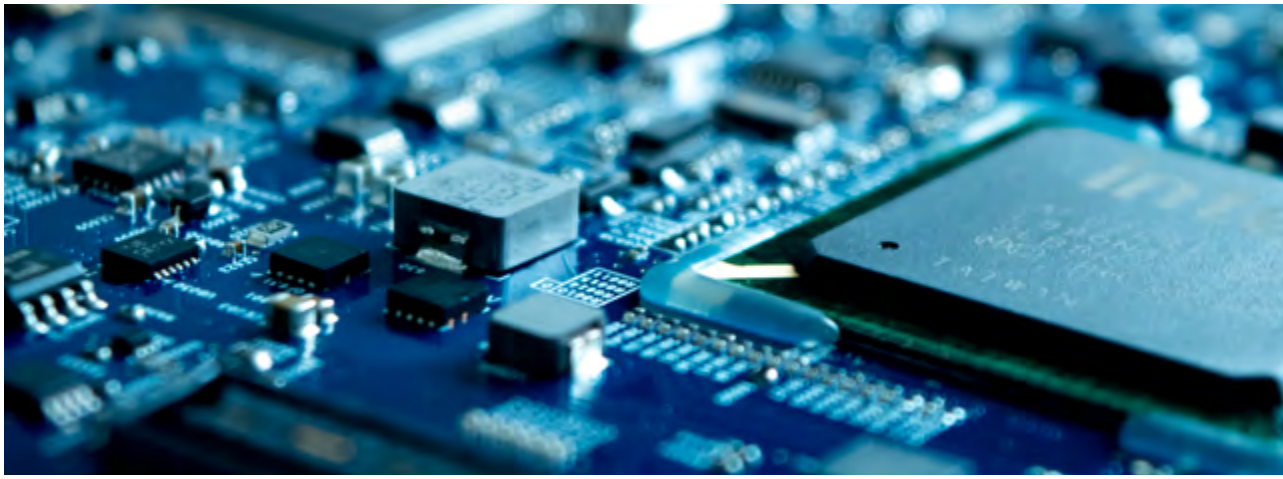
Für Unternehmen bedeutet das:

- verpflichtende Sicherheitsanforderungen bei Entwicklung und Bereitstellung digitaler Produkte,
- formalisierte Meldeprozesse für Schwachstellen und Sicherheitsvorfälle,
- sowie Nachweis- und Konformitätsanforderungen (inkl. CE-Kennzeichnung).

Wer ist betroffen?

Die Verordnung gilt für sogenannte „Produkte mit digitalen Elementen", d.h. Produkte, deren bestimmungsgemäße oder vorhersehbare Nutzung eine direkte oder indirekte Datenverbindung zu Gerät oder Netzwerk umfasst.
Betroffen sind insbesondere:

- Hersteller digitaler Produkte
- Importeure
- Distributoren



Kernpflichten für betroffene Organisationen

Produkt-Governance
Cyber-Sicherheit wird integraler Bestandteil des Produktlebenszyklus, indem Hersteller Sicherheitsanforderungen bereits bei Konzeption, Entwicklung und Wartung berücksichtigen müssen.

Technische und organisatorische Maßnahmen
Hersteller müssen u.a.:

- Sicherheitsrisiken systematisch bewerten,
- Schwachstellen identifizieren und beheben,
- Sicherheitsupdates über einen definierten Supportzeitraum bereitstellen.

Meldepflichten bei Sicherheitsvorfällen
Bei aktiv ausgenutzten Schwachstellen oder schwerwiegenden Sicherheitsvorfällen gelten künftig Meldepflichten gegenüber Behörden über eine zentrale EU-Meldeplattform.

Konformitätsbewertung & Dokumentation
Betroffene Produkte müssen:

- CRA-konform entwickelt werden,
- einer Konformitätsbewertung unterzogen werden,
- sowie mit CE-Kennzeichnung bereitgestellt werden.

Aufsicht & Sanktionen

Die Einhaltung des CRA wird durch nationale **Marktüberwachungs-behörden** überwacht.

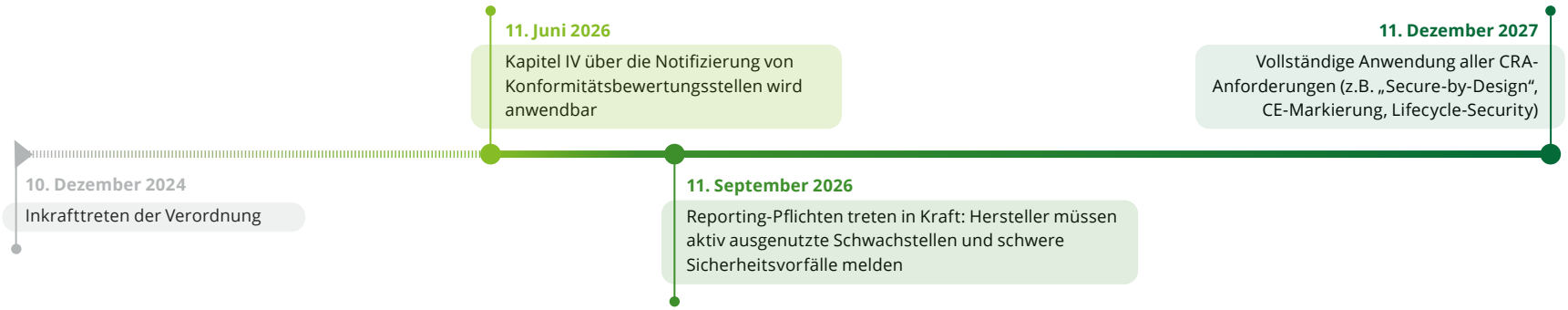
Bei Verstößen können Maßnahmen der Marktüberwachung (z.B. Einschränkung oder Rücknahme vom Markt) angeordnet werden.

Sanktionsregelungen werden von den Mitgliedstaaten festgelegt und im nationalen Vollzug angewandt.

Was Unternehmen jetzt konkret tun sollten

01 Betroffenheitsanalyse für Produkte mit digitalen Elementen durchführen
02 Rollen entlang der Lieferkette (Hersteller / Importeur / Distributor) klären
03 Gap-Analyse gegenüber CRA-Sicherheitsanforderungen durchführen
04 Vulnerability- und Incident-Reporting-Prozesse vorbereiten
05 Konformitätsbewertungs- und Dokumentationsprozesse etablieren
06 Umsetzungs-Roadmap erstellen

Timeline



Deloitte.

Kontakt

Karin Mair
Managing Partner |
Technology & Transformation und
Strategy, Risk & Transactions

+43 1 537 00-4840
kmair@deloitte.at

Georg Schwondra
Partner |
Cyber

+43 1 537 00-3760
gschwondra@deloitte.at