Cyber Resilience Act: Was Unternehmen jetzt wissen müssen

Sicherheit. Mit dem Cyber Resilience Act (CRA) hat die EU einen weiteren Digitalisierung-Rechtsakt erlassen. Er verpflichtet Unternehmen, digitale Schwachstellen in vernetzten Produkten zu beseitigen und damit deren Sicherheit zu erhöhen. Vernetzte Produkte bieten nämlich oft ein Einfallstor für Cyberangriffe, die weitreichende Folgen nicht nur für die betroffenen Unternehmen, sondern auch für die gesamte Wirtschaft haben können. So hat etwa in der Vergangenheit ein Cyberangriff, unter anderem auf die Schifffahrt, 20 % des Welthandels betroffen. Mehr über den CRA erfahren Sie im folgenden Artikel von RA Georg Huber.

© Frank H. - stock.adobe.com

Mit dem Cyber Resilience Act (CRA) werden Maßnahmen für mehr Cybersicherheit zur gesetzlichen Plicht und zum Wettbewerbsfaktor.

Der Cyber Resilience Act (CRA) ist eine EU-Verordnung, die erstmals verbindliche Mindeststandards für die Cybersicherheit von digitalen Produkten und Software festlegt. Seit Dezember 2024 gilt der CRA. Ab Dezember 2027 dürfen nur noch CRA-konforme Produkte auf dem EU-Markt bereitgestellt werden.

Wer ist betroffen?

Betroffen sind alle Unternehmen, die Produkte mit digitalen Elementen oder Software herstellen, vertreiben, importieren oder als Bestandteil eigener Lösungen ausliefern. Dazu zählen etwa:

- Hersteller und Entwickler von Elektronik und Software
- Handelsunternehmen, die vernetzte Geräte verkaufen
- Serviceanbieter, die digitale Lösungen vertreiben
- Unternehmen, die Produkte aus Nicht-EU-Ländern importieren (z.B. chinesische IoT-Geräte)

Nicht-kommerzielle Open-Source-Software und einige bereits speziell regulierte Produkte (z.B. Medizinprodukte) sind ausgenommen.

Was ist ein „Produkt mit digitalen Elementen“?

Darunter fallen alle Geräte und Software, die mit Netzwerken kommunizieren („Connected Products“), z.B.:

- Smarte Kaffeemaschinen, Smart-Home-Komponenten, vernetzte Maschinen
- Branchensoftware, die ans Internet angebunden ist
- Industrieanlagen mit Fernwartung, Gebäudetechnik oder IoT-Sensoren

Grundlegende CRA-Pflichten

Für alle betroffenen Unternehmen gelten folgende grundlegenden Pflichten:

- Security by Design: Cybersicherheit muss von Anfang an bei der Produktentwicklung mitgedacht werden, entsprechende Standardeinstellungen vorsehen
- Schwachstellenmanagement: proaktive Identifizierung, Klassifizierung, Dokumentation von Sicherheitslücken
- Meldepflicht: Sicherheitsvorfälle spätestens 24 Stunden nach Bekanntwerden melden
- Regelmäßige Sicherheitsupdates: für mindestens 5 Jahre nach Markteinführung bereitstellen
- Datenschutz und Vertraulichkeit: Gewährleistung von Vertraulichkeit und Datenintegrität
- Ereignisreaktion und Resilienz: Erkennung von Sicherheitsvorfällen und deren Abwehr

Beispiel: Ein Softwarehaus muss für die gesamte Lebensdauer seines Programms, mindestens jedoch 5 Jahre, Sicherheitsaktualisierungen bereitstellen und dokumentieren, welche Drittanbieter-Komponenten verwendet werden (Software Bill of Materials, SBOM).

Produktklassen

Der CRA teilt Produkte mit digitalen Elementen in verschiedene Risikokategorien ein, für die unterschiedliche Anforderungen gelten:

- Standardprodukte: Sie umfassen alltägliche Hardware- und Software-Produkte, von denen nur ein geringes Cybersicherheitsrisiko ausgeht. Beispiele sind etwa Programme zur Bildbearbeitung, Büro- und Standardsoftware, Videospiele, einfache IoT-Geräte ohne kritische Funktionen.
- Wichtige Produkte sind Produkte mit digitalen Elementen, bei denen ein erhöhtes Risiko für Nutzer, Unternehmen oder Gesellschaft besteht. Die Kategorie „wichtige Produkte“ wird weiter unterteilt in:
  - Klasse I: Produkte mit grundlegenden Cybersicherheitsfunktionen wie Passwortmanager, Identitäts- und Netzwerkmanager, Wearables, internetfähige Spielzeuge, Smart-Home-Komponenten, eigenständige und eingebettete Browser.
  - Klasse II: Produkte mit erweiterten oder besonders sicherheitsrelevanten Funktionen wie Firewalls, Angriffserkennungs- und Präventionssysteme, manipulationssichere Mikrocontroller, Hypervisors, Container-Runtime-Systeme, Smart Meter Gateways.
  - Kritische Produkte: Das sind Produkte, von denen gravierende Auswirkungen auf grundlegende gesellschaftliche oder wirtschaftliche Funktionen – häufig in kritischen Infrastrukturen – ausgehen können. Beispiele: Smart-Cards, Security-Hardware mit Schutzfunktionen.

Ersatzteile sind vom CRA ausgenommen, sofern sie keine neuen Funktionen zu bestehenden Produkten hinzufügen und ausschließlich der Reparatur dienen.

CE-Kennzeichnung und Konformitätsbewertung

Die zentrale Rolle für den Marktzugang übernimmt künftig die CE-Kennzeichnung. Jedes Produkt mit digitalen Elementen muss also den CRA-Anforderungen entsprechen, damit es mit einem CE-Kennzeichen versehen und damit in der EU verkauft werden darf.

Ob und in welchem Verfahren ein Produkt das CE-Kennzeichen erhält, hängt von seiner Risikoklasse ab: Bei Standardprodukten reicht idR eine interne Prüfung durch den Hersteller („Selbstdeklaration“). Für wichtige und kritische Produkte ist ein Prüfverfahren durch anerkannte „notifizierte Stellen“ vorgesehen.

Spezifische Pflichten im Überblick:

Neben den oben erwähnten grundlegenden Pflichten schreibt der CRA spezifische Pflichten insbesondere im Zusammenhang mit der Risiko- und Konformitätsbewertung vor. Das sind Folgende:

- Technische Dokumentation: Detailbeschreibung von Entwicklung, Architektur, Komponenten, Risikobewertung und Wartungskonzept – die Dokumentation ist mindestens 10 Jahre vorzuhalten.
- EU-Konformitätserklärung: Offizielle Zusicherung, dass sämtliche CRA-Anforderungen und harmonisierte Normen eingehalten sind.
- CE-Kennzeichnung: Sichtbares Zeichen der Compliance. Ohne korrekte Konformitätsbewertung kein Marktzugang, Verstöße führen zum Vertriebsverbot.
- Qualitätssicherung und Überwachung: Bei wichtigen und kritischen Produkten sind regelmäßige externe Audits und eine kontinuierliche Überwachung vorgeschrieben (Schwachstellenmanagement), um die Compliance im Produktlebenszyklus zu sichern.

Transparenz gegenüber Verbrauchern

Hersteller müssen Verbraucher online oder in einer Gebrauchsanleitung klar, verständlich und transparent über die Cybersicherheitsmerkmale, bekannte Schwachstellen, verfügbare Updates sowie empfohlene Sicherheitsmaßnahmen für jedes Produkt mit digitalen Elementen informieren.

Pflicht der Händler, Importeure und Lieferkette

Nicht nur Hersteller, sondern auch Händler und Importeure müssen vor dem Vertrieb prüfen, ob die Produkte eine gültige CE-Kennzeichnung sowie vollständige technische Dokumentation aufweisen. Damit wird die Cybersicherheit entlang der gesamten Lieferkette abgesichert und kontrolliert.

Meldepflichten & Fristen

Bereits ab September 2026 gelten strenge Meldepflichten: Unternehmen müssen Sicherheitsvorfälle binnen 24 Stunden den zuständigen Behörden melden. Bis Dezember 2027 sind sämtliche CRA-Pflichten verpflichtend umzusetzen.

Sanktionen

Bei Verstößen drohen empfindliche Geldbußen:

- Grundlegende Verstöße: bis 15 Millionen Euro oder 2,5 % des weltweiten Umsatzes
- Spezifische Pflichtverletzungen: bis 10 Millionen Euro oder 2 % des weltweiten Umsatzes
- Unvollständige Angaben: bis 5 Millionen Euro oder 1 % des weltweiten Umsatzes

Außerdem drohen weitere Sanktionen, die gravierender als die Geldbußen sein können, nämlich:

- Verkaufsverbote,
- Rückrufaktionen,
- öffentliche Warnungen,
- zivilrechtliche Schadenersatzansprüche.

Schnittstellen und Synergien

Unternehmen, die bereits nach NIS2, DSGVO oder ISO 27001 arbeiten, können Synergien bei Melde- und Dokumentationspflichten nutzen, sollten aber prüfen, wo strengere Vorgaben des CRA greifen.

Handlungsempfehlungen

Betroffene Unternehmen sollten sich schon jetzt auf den CRA vorbereiten. Die frühzeitige Vorbereitung ist deshalb wichtig, weil ab Dezember 2027 nur mehr CRA-konforme Produkte auf den Markt gebracht werden dürfen. Bis dahin müssen daher die die Anforderungen des CRA erfüllt sein, sonst ist der Vertrieb der eigenen Produkte in der EU nicht mehr zulässig. Ein Vertriebsverbot hat naturgemäß verheerende Folgen für das Unternehmen. Folgende Maßnahmen empfehlen sich:

- Alle Produkte mit digitalen Elementen systematisch erfassen und den einzelnen Produktklassen zuordnen
- Verantwortung und Prozesse für Security by Design festlegen
- Frühzeitig Konformitätsbewertung (CE-Kennzeichnung) einleiten
- Risikoanalyse durchführen und technische Dokumentation erstellen
- Lieferketten absichern (vertraglich und technisch)
- Personal schulen, Prozesse testen, Audits einführen
- Im Zweifel frühzeitig externe Experten einbinden
- Laufende Compliance und Überwachung sicherstellen

Fazit

Cybersicherheit wird zur gesetzlichen Pflicht und zum Wettbewerbsfaktor. Rechtzeitige Vorbereitung sichert den Marktzugang und minimiert Geschäftsrisiken – unabhängig von Branche und Unternehmensgröße. ▲

Zum Autor

Dr. Georg Huber, LL.M., CIPP/E.
ist Rechtsanwalt bei
GPK Pegger Kofler &Partner
Rechtsanwälte.

Nähere Infos unter www.lawfirm.at