Cyber Resilience Act

Betroffenheit und notwendige Maßnahmen zur Umsetzung der neuen EU-Verordnung zur Cybersicherheit von Produkten mit digitalen Elementen.

Mit dem Cyber Resilience Act (CRA) werden die Anforderungen an die Cybersicherheit für zahlreiche Produkte deutlich verschärft. Ziel des CRA ist die Schaffung eines einheitlichen Sicherheitsstandards für digitale Produkte auf dem Europäischen Markt. Die Verordnung soll ab dem Jahr 2027 unmittelbar in allen EU-Mitgliedstaaten gelten.

Wer ist betroffen?

Betroffen sind Hersteller, Einführer und Händler von Produkten mit digitalen Elementen. Produkte mit digitalen Elementen sind Software- oder Hardwareprodukte sowie deren Backendsysteme. Dazu gehören u.a.: Vernetzte Maschinen, IoT-Geräte, Apps, Wearables, Softwareprogramme, Festplatten, Firewalls, Passwort-Manager, Mikroprozessoren, uvm. Nur einige wenige Produktarten sind vom CRA ausgenommen.

Was ist umzusetzen?

Der CRA verpflichtet Hersteller von Produkten mit digitalen Elementen, bestimmte Anforderungen an die Cybersicherheit und das Schwachstellenmanagement zu erfüllen. Hersteller müssen Produkte mit digitalen Elementen so konzipieren und entwickeln, dass während des gesamten Produktlebenszyklus ein angemessenes Cybersicherheitsniveau gewährleistet ist.

Auf der Grundlage einer Bewertung der Cybersicherheitsrisiken müssen zahlreiche Maßnahmen ergriffen werden. Unter anderem dürfen die erfassten Produkte nur mit einer sicheren Standardkonfiguration und ohne bekannte ausnutzbare Schwachstellen auf den Markt gebracht werden. Darüber hinaus fordert der CRA zahlreiche technische und organisatorische Maßnahmen zur Resilienz der Produkte.

Hersteller von Produkten mit digitalen Elementen müssen außerdem weitreichende Anforderungen an die Behandlung von Schwachstellen erfüllen. Ausgehend von einer fortlaufenden Überwachung der Produkte müssen Hersteller bekannt gewordene Schwachstellen durch kostenlose Sicherheitsupdates beseitigen. Aktiv ausgenutzte Schwachstellen müssen an die Marktüberwachungsbehörde gemeldet werden.

Was droht bei Verstößen?

Die Marktüberwachungsbehörden verfügen über weitreichende Untersuchungs-, Abhilfe- und Sanktionsbefugnisse. Bei Verstößen gegen den CRA drohen unter anderem Produktwarnungen und Bußgelder bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes.

Unsere Unterstützung

Wir unterstützen Sie bei der Umsetzung der Anforderungen des Cyber Resilience Act u.a. mit folgenden Leistungen:

- Prüfung der Betroffenheit
- Anforderungskatalog und Gap-Analyse
- Vertragsgestaltung mit Lieferanten und Dienstleistern
- Cybersecurity Compliance Management

Next Step: Kontaktaufnahme

Gerne erläutern wir Ihnen unser Vorgehen ausführlich in einem persönlichen Gespräch.

T + 49 30 / 2332 895 0
E info@reuschlaw.de