ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Der Cyber Resilience Act

Kurzüberblick

Der CRA regelt Anforderungen für die IT-Sicherheit von vernetzten Hardware- und Softwareprodukten, die auf dem den EU-Markt vertrieben werden. Die Anforderungen gelten über den gesamten Lebenszyklus des Produkts. Der Hintergrund: Produkte in der EU sollen ein einheitliches Sicherheitsniveau haben. Damit wird es für Nutzende einfacher, Cybersicherheitseigenschaften von Produkten zu berücksichtigen.

Ausführliche Informationen zum CRA sind in unserem Whitepaper „Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht“ zusammengefasst, es steht kostenlos zum Download bereit unter www.sit.fraunhofer.de/cra

Welche Produkte fallen unter den CRA?

Software und Hardware, die Datenverbindungen mit einem Gerät oder einem Netz aufbauen können, einschließlich einzelner Soft- und Hardwarekomponenten. Das sind beispielsweise

- **Mobile Geräte**
  (z. B. Smartphones, Laptops, vernetztes Spielzeug)
- **Smart-Home-Geräte**
  (z. B. Thermostate, Stromzähler, vernetzte Kameras)
- **Software, die lokal auf elektronischen Geräten installiert wird**
  (z. B. Treiber, Office-Programme, Apps)
- **Vernetzte industrielle Steueranlagen**
  (z. B. fernsteuerbare Maschinen, Roboter, Förderanlagen)
- **Netzwerk-Geräte**
  (z. B. Router, Switches, Gateways)

Siehe Whitepaper Seite 8

Welche Sicherheitsstufe?

Alle unter den CRA fallenden Produkte müssen Sicherheitskriterien erfüllen. Der Nachweis hierüber kann in der Basiskategorie vom Hersteller selbst erbracht werden. Es gibt aber Produkte, die hierfür strengere Kriterien erfüllen müssen, nämlich „wichtige Produkte“ Klasse I und II und „kritische Produkte“, die als Vertrauensanker für andere Produkte dienen.

Kritische Produkte	Art. 8 Anhang IV CRA	z.B. Produkte wie Sicherheitsboxen oder Smartcards, also Produkte, die im Kern Vertrauensanker für andere Produkte sind
Wichtige Produkte Klasse II	Art. 7 Anhang III CRA	z.B. Betriebssysteme für Server, Desktops und mobile Geräte, Mikroprozessoren, Sicherheitshardware und spezialisierte industrielle Systeme und Geräte
Wichtige Produkte Klasse I	Art. 7 Anhang III CRA	z.B. allgemeine Netzwerk- und Systemverwaltungssoftware und grundlegende Hardwarekomponenten
Basiskategorie Produkte mit digitalen Elementen	Art. 3 Nr.1 CRA	z.B. Smartwatches, intelligente Stromzähler, Drucker, Bildbearbeitungssoftware

Welche Konsequenzen hat ein Verstoß gegen den CRA?

Hier drohen erhebliche finanzielle Sanktionen, die je nach Schwere bis zu 15 Mio. € oder 2,5 % des Jahresumsatzes betragen können. Die Sanktionen sind in Art. 64 Abs. 1-4 CRA geregelt.

Bei u.a. falschen oder unvollständigen Informationen - bis zu 5 Mio. € oder 1 % des Jahresumsatzes

Bei Verstoß gegen u.a. Einführer- oder Händlerpflichten - bis zu 10 Mio. € oder 2 % des Jahresumsatzes

Bei Verstoß gegen u.a. die Herstellerpflichten - bis zu 15 Mio. € oder 2,5 % des Jahresumsatzes

Siehe Whitepaper Seite 26

Wen betrifft der CRA?

In erster Linie:

Hersteller

Sie müssen unter anderem:

+ eine Risikobewertung ihres Produkts über den gesamten Lebenszyklus durchführen und dies dokumentieren
+ die Behandlung von Schwachstellen in ihren Produkten CRA-konform umsetzen
+ sicherstellen, dass auch Komponenten, die von anderen Herstellern bezogen werden, die Cybersicherheit des eigenen Produkts nicht beeinträchtigen
+ Anforderungen zur Cybersicherheit ihrer Produkte umsetzen (wie sichere Standardkonfigurationen, Schutz vor dem Zugriff Unbefugter, Authentifizierungssysteme, Verschlüsselung, Datensparsamkeit, …)
+ CE-Kennzeichen und eine Seriennummer anbringen
+ weitere Dokumentations-, Informations-, Melde- und Aufbewahrungspflichten erfüllen

Siehe Whitepaper Seite 29

Ferner auch:

Händler und Importeure

Sie müssen prüfen, ob Produkte, die sie auf den EU-Markt bringen wollen, bestimmte CRA-Anforderungen erfüllen, wobei Importeure hier umfangreichere Pflichten haben. Sie kontrollieren beispielsweise, ob:

+ Produkte eine CE-Kennzeichnung haben
+ Informationen des Herstellers korrekt sind
+ Seriennummer und Kontakt des Herstellers angebracht sind
+ das Ende des Support-Zeitraums leicht ersichtlich
+ Sie haben außerdem noch weitere Informations- und Nachmarktpflichten.

Die Pflichten sind detailliert im Whitepaper aufgelistet, Seite 30 für Importeure, Seite 31 für Händler

Kontakt
Dr. Michael Kreutzer
Kontakt Strategie
+49 6151 869-348
michael.kreutzer@sit.fraunhofer.de

Fraunhofer-Institut für
Sichere Informationstechnologie
Rheinstraße 75
64295 Darmstadt

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Das Whitepaper und weitere Informationen finden Sie auf unsere Website unter:
www.sit.fraunhofer.de/cra