CYBERSECURITY FÜR GEBÄUDE STEUERUNGEN

EU Cybersecurity Resilience Act (CRA)

Inhalt

1. Zweck des Dokuments **2**

2. Was ist die EU CRA? **2**

3. Anwendungsbereich und Zielsetzung **2**

4. CRA-bezogene Rollen **2**

4.1. Verbraucher/Nutzer 2

4.2. Hersteller 2

5. Was bedeutet "Secure by Default"? **2**

6. Herstellerverantwortung für Cybersicherheit **3**

7. Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen **3**

8. Verantwortlichkeiten der Hersteller **4**

9. Ausnahmeregelungen **5**

9.1. Übergangsbestimmungen (§ 69) 5

9.2. Ausnahmen für gewerbliche Nutzer 5

10. Verhältnis zu anderen Verordnungen **5**

1. Zweck des Dokuments

Dies ist ein kurzer Überblick über den EU Cyber Resilience Act (CRA). Der EU Cybersecurity Resilience Act (CRA) ist eine Verordnung, die darauf abzielt, die Cybersicherheit in der Europäischen Union zu stärken, indem sie verpflichtende Anforderungen an Produkte mit digitalen Komponenten stellt – von intelligenten Geräten und industriellen Steuerungssystemen bis hin zu Softwareplattforme.

2. Was ist die EU CRA?

Der Cyber Resilience Act (CRA) ist eine EU-Verordnung zur Verbesserung der Cybersicherheit digitaler Produkte. Sie wurde am 20. März 2024 verabschiedet, trat am 10. Dezember 2024 in Kraft und gilt ab dem 11. Dezember 2027 vollständig.

3. Anwendungsbereich und Zielsetzung

Die Verordnung regelt:

- Anforderungen an das Inverkehrbringen und die Cybersicherheit digitaler Produkte,
- Vorgaben für Entwurf, Entwicklung, Herstellung und Pflichten der Wirtschaftsakteure,
- Standards für Schwachstellenmanagement während der Nutzung sowie entsprechende Herstellerpflichten,
- Rahmenbedingungen für Marktüberwachung und Durchsetzung der Regeln.

4. CRA-bezogene Rollen

4.1. Verbraucher/Nutzer

Die CRA bezeichnet Verbraucher als Personen, die Produkte für den persönlichen oder beruflichen Zweck erwerben und diese nicht gewerblich weitergeben oder weiterverkaufen. Die Bezeichnungen „Verbraucher“ und „Nutzer“ werden synonym verwendet.

4.2. Hersteller

Gemäß der CRA bezeichnet der Begriff „Hersteller“ jede natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt, produziert oder produzieren lässt und diese unter eigenem Namen oder eigener Marke vertreibt – unabhängig davon, ob die Bereitstellung entgeltlich oder unentgeltlich erfolgt.

5. Was bedeutet "Secure by Default"?

Hersteller müssen die CRA-Standards einhalten, um Cybersicherheitsrisiken im gesamten Produktlebenszyklus – inklusive Drittanbieter-Komponenten und Support – zu minimieren. Sicherheitsstufen und „Secure by Default“-Anforderungen richten sich nach der Art der verarbeiteten Daten.

- Systemdaten sind Daten, die nicht als sensibel oder kritisch eingestuft werden. Eine Kompromittierung dieser Daten hätte keine signifikanten Auswirkungen auf die Sicherheit.

- Sensible Systemdaten: Keine Personenbezüge, aber ein Verlust könnte erheblichen Schaden anrichten oder die Sicherheit der Nutzer gefährden (z. B. vertrauliche Geschäftsinfos, Überwachungsdaten).
- Personenbezogene Daten: Hierzu zählen Informationen, bei deren Offenlegung lediglich ein geringes Schadenspotenzial besteht, wie beispielsweise Namen oder öffentlich zugängliche Fotos.
- Sensible personenbezogene Daten sind Informationen, bei denen eine Offenlegung nachteilige Folgen haben kann. Dazu zählen beispielsweise Gesundheitsdaten, private Nachrichten oder Finanzdaten.
- Sicherheitsdaten: Diese sind sicherheitsrelevant, jedoch nicht personenbezogen. Eine Gefährdung dieser Daten kann die Produktsicherheit beeinträchtigen, beispielsweise bei Passwörtern oder kritischen Konfigurationseinstellungen.
- Kritische Sicherheitsdaten: Hochsensibel und nicht personenbezogen; jede Beeinträchtigung von Integrität oder Vertraulichkeit kann gravierende Folgen für das Produkt und Dritte haben (z. B. Hauptschlüssel).

Ein weiterer Aspekt ist die potenzielle Angriffsfläche, die von den Kommunikationsmethoden und der physischen Zugänglichkeit eines Produkts beeinflusst wird. Produkte mit ausschließlich lokalen Schnittstellen weisen in der Regel andere Sicherheitsanforderungen auf als Produkte, die kontinuierlich mit öffentlichen Netzwerken verbunden sind.

"Secure by Default" beschreibt die Vorgehensweise, Produkte für den europäischen Binnenmarkt mit geeigneten Cybersicherheitsmaßnahmen auszustatten. Produkte mit digitalen Komponenten werden so gestaltet, entwickelt und hergestellt, dass sie ein an die identifizierten Risiken angepasstes Maß an Cybersicherheit gewährleisten.

6. Herstellerverantwortung für Cybersicherheit

Hersteller müssen gewährleisten, dass Produkte mit digitalen Komponenten auf dem EU-Markt die geltenden Sicherheitsanforderungen erfüllen. Dazu gehören Maßnahmen wie Risikobewertungen im Bereich Cybersicherheit, das Ausstellen von Konformitätserklärungen sowie die Kooperation mit zuständigen Behörden.

Ein Verfahren für das Schwachstellenmanagement ist durch Hersteller einzuführen, um die Cybersicherheit digitaler Produkte zu unterstützen. Importeure und Händler sind verpflichtet, bestimmte Vorgaben im Zusammenhang mit diesen Verfahren einzuhalten.

Hersteller haben die Aufgabe, Verbraucher transparent über die Sicherheitsmerkmale ihrer Hard- und Software zu informieren.

Der EU Cyber Resilience Act (CRA) schreibt die Einhaltung der Vorschriften für Hersteller und Anbieter vor. Systeme oder deren Konfigurationen sind nicht ausdrücklich vom CRA erfasst.

7. Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

Produkte mit digitalen Komponenten müssen bei Markteinführung keine bekannten Schwachstellen aufweisen und sichere Standardeinstellungen haben.

- Schwachstellen sollen per Sicherheitsupdate – möglichst automatisch – behoben werden können.
- Zugriffe sind durch Authentifizierung zu sichern.
- Sensible Daten müssen verschlüsselt oder anderweitig geschützt werden.
- Es dürfen nur notwendige Daten verarbeitet werden.
- Wesentliche Funktionen auch bei Zwischenfällen bereitgestellt werden (z. B. Schutz vor Denial-of-Service-Angriffen).
- Die Verfügbarkeit anderer Dienste und Netzwerke darf nicht beeinträchtigt werden; externe Schnittstellen sind zu minimieren.

Mit Inkrafttreten der CRA müssen alle Produkte ihre Cyber-Resilienz nachweisen und Cybersicherheitsmängel klar kennzeichnen.

Im EU-Cyber Resilience Act bedeutet „standardmäßig sicher", dass digitale Produkte von Anfang an sicher nutzbar sind, ohne dass Nutzer Einstellungen ändern müssen. Ein Zurücksetzen auf den Ursprungszustand sollte alle lokalen Daten löschen, die Software zurücksetzen und die Standardkonfiguration wiederherstellen. Die Software darf keine fest programmierten oder kritischen Sicherheitsdaten enthalten.

8. Verantwortlichkeiten der Hersteller

Hersteller von Produkten mit digitalen Elementen sind verpflichtet:

- Schwachstellen sowie Komponenten dieser Produkte zu identifizieren und zu dokumentieren, einschließlich der Erstellung einer maschinenlesbaren Software-Stückliste, die mindestens die Hauptabhängigkeiten umfasst.
- Schwachstellen auf Grundlage des Risikos für Produkte mit digitalen Elementen zeitnah zu beheben und Sicherheitsupdates bereitzustellen; sofern technisch möglich sollten diese Updates unabhängig von Funktionsupdates erfolgen.
- Regelmäßige Tests und Überprüfungen zur Sicherheit der Produkte durchzuführen.
- Nach Bereitstellung eines Sicherheitsupdates Informationen über behobene Schwachstellen zu veröffentlichen, einschließlich Beschreibung, Produktidentifikation, Auswirkungen, Schweregrad und klaren Nutzeranleitungen zur Behebung.
- Eine Richtlinie für die koordinierte Offenlegung von Schwachstellen festzulegen und umzusetzen.
- Maßnahmen zu ergreifen, die den Informationsaustausch über potenzielle Schwachstellen in eigenen und Drittanbieter-Komponenten ermöglichen, beispielsweise durch Angabe einer Kontaktadresse für Meldezwecke.
- Mechanismen zur sicheren Verteilung von Updates für digitale Produkte zu bieten, damit Schwachstellen unverzüglich behoben werden können; automatische Updates sind bei relevanten Sicherheitsaktualisierungen zu ermöglichen.
- Sicherzustellen, dass Sicherheitsupdates zur Behebung erkannter Probleme umgehend und kostenlos verteilt werden, zusammen mit Hinweisen und Empfehlungen, sofern mit Geschäftskunden keine abweichende Vereinbarung für maßgeschneiderte Produkte besteht.

9. Ausnahmeregelungen

9.1. Übergangsbestimmungen (§ 69)

Produkte mit digitalen Komponenten müssen die Verordnung nur erfüllen, wenn sie nach 36 Monaten erheblich geändert werden. Die Meldepflicht gilt für alle relevanten Produkte mit digitalen Elementen, auch für bereits verfügbare.

9.2. Ausnahmen für gewerbliche Nutzer

Produkte mit digitalen Elementen müssen sicher vorkonfiguriert sein, es sei denn, bei kundenspezifischen Lösungen für einen gewerblichen Nutzer wird etwas anderes vereinbart, inklusive deutlicher Hinweise für nötige Nutzeraktionen.

10. Verhältnis zu anderen Verordnungen

Die CRA ergänzt bestehende EU-Regelungen wie die **Richtlinie über Funkanlagen** und die **NIS2-Richtlinie** und sorgt für einheitliche Cybersicherheitsstandards.