MYRA

FACT SHEET

Cyber Resilience Act: Wenn Security by Design zur Pflicht wird

Wenn Security by Design zur Pflicht wird

Mit dem Cyber Resilience Act (CRA) will die EU-Kommission erstmals verbindliche Cybersicherheitsanforderungen für den gesamten Lebenszyklus von Hardware- und Softwareprodukten definieren und einführen. Dadurch soll es Unternehmen sowie Verbraucherinnen und Verbrauchern in der EU erleichtert werden, das Thema Cybersicherheit als Kriterium bei der Auswahl und der Verwendung von Produkten zu berücksichtigen.

Analog zur NIS-2-Richtlinie, welche die Informationssicherheit auf Betreiberseite regelt, will der CRA als komplementäre Regulierung die Sicherheit digitaler Produkte und Dienste verbessern.

Erfahren Sie in diesem Fact Sheet mehr über die Hintergründe der neuen Gesetzgebung sowie über die praktischen Auswirkungen für Unternehmen.

CRA-Zielsetzung

- Gewährleistung, dass die Hersteller die Sicherheit von Produkten mit digitalen Elementen schon ab der Konzeptions- und Entwicklungsphase sowie über den gesamten Lebenszyklus hinweg verbessern
- Gewährleistung eines kohärenten Cybersicherheitsrahmens, der den Hardware- und Softwareherstellern die Einhaltung der Vorschriften erleichtert
- Erhöhung der Transparenz der Sicherheitseigenschaften von Produkten mit digitalen Elementen
- Befähigung von Unternehmen sowie Verbraucherinnen und Verbrauchern, damit sie Produkte mit digitalen Elementen sicher verwenden können

Was bedeutet das für Hersteller?

- Verpflichtung zu Security by Design: Cybersicherheit muss in der kompletten Planungs-, Entwurfs-, Entwicklungs-, Produktions-, Liefer- und Wartungsphase von Produkten berücksichtigt und umgesetzt werden
- Umfangreiche Dokumentations- und Meldepflichten von Schwachstellen und Sicherheitsvorfällen gegenüber Unternehmenskunden, Verbraucherinnen und Verbrauchern sowie den zuständigen Aufsichtsbehörden
- Verpflichtung zu Support mit Sicherheitsupdates während der erwarteten Produktlebensdauer oder über einen Zeitraum von fünf Jahren (je nachdem, welcher Zeitraum kürzer ist)

Geltungsbereich: Diese Produkte sind betroffen

Die Verordnung betrifft in erster Linie alle Produkte mit digitalen Elementen. Diese sind durch den CRA in drei Klassen eingeordnet. Die Standardkategorie soll rund 90 % aller Produkte umfassen, sie setzt sich aus handelsüblichen Geräten und Programmen mit niedriger Kritikalität zusammen, wie etwa Fotobearbeitungssoftware, Videospiele oder smarte Lautsprecher.

Die übrigen 10 % entfallen auf Produkte der kritischen Klassen I und II, von denen ein höheres Cybersicherheitsrisiko ausgeht. Daher sind hier besondere Konformitätsbewertungsverfahren anzuwenden, einschließlich der externen Bewertung durch Dritte.

Ausgenommen vom CRA sind Software-as-a-Service-Lösungen (SaaS), außer diese sind eng mit einem digitalen Produkt verzahnt und stellen dessen Funktionalität sicher. Generell sind Anbieter sensibler SaaS-Lösungen über die NIS-2-Richtlinie bzw. das NIS-2 Umsetzungsgesetz (NIS2UmsuCG) reguliert.

90% der Produkte	10% der Produkte	
	Kritische Produkte	
Standardkategorie Selbstbewertung	**Kritische „Klasse I“** Standardbewertung oder Bewertung durch Dritte	**Kritische „Klasse II“** Bewertung durch Dritte
Kriterien: entfallen	**Kriterien:** • Funktionalität (z. B. kritische Software) • Beabsichtigte Verwendung (z. B. industrielle Steuerung / NIS-2) • Andere Kriterien (z. B. Ausmaß der Auswirkungen)	
Beispiele: • Fotobearbeitung • Textverarbeitung • Intelligente Lautsprecher • Festplatten • Spiele • usw.	**Beispiele:** • Browser • Passwortmanager • Antivirusprodukte • VPN • usw.	**Beispiele:** • Betriebssysteme • Hypervisoren • Router, Modems • Hardware-Sicherheitsmodule (HSM) • IIoT im KRITIS-Umfeld (NIS-2) • usw.

CRA: Die wichtigsten Anforderungen

Grundlegende Anforderungen an die Cybersicherheit
Produkte mit digitalen Elementen (Produkte) werden nur dann auf dem Markt zugelassen, wenn sie die „grundlegenden Cybersicherheitsanforderungen“ erfüllen, die in Abschnitt 1 von Anhang I des CRA aufgeführt sind. Diese Anforderungen sind darauf ausgelegt, die Sicherheit, Vertraulichkeit und Integrität digitaler Produkte sicherzustellen. Dabei setzt die EU-Kommission auf Best Practices wie Verschlüsselung, Datenminimierung oder eine präventive Absicherung vor Angriffen. Beispiel: Die Produkte müssen „die Verfügbarkeit wesentlicher Funktionen, einschließlich der Abwehrfähigkeit gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe) und deren Eindämmung gewährleisten“.

Anforderungen an den Umgang mit Schwachstellen
Darüber hinaus definiert der CRA verschiedene Anforderungen an die Hersteller für den Umgang mit Schwachstellen (Abschnitt 2 von Anhang I). Die Vorgaben regeln unter anderem die Bereitstellung von Sicherheitsupdates, das Management der Update-Verteilung, regelmäßiges Pentesting sowie Informationspflichten.

Erweiterte Anforderungen für „kritische" Produkte
Während alle Produkte der Standardkategorie wie Textverarbeitungsprogramme oder Fotobearbeitungstools über eine Selbstbewertung die Einhaltung der Anforderungen überprüfen sollen, muss für Produkte der kritischen Klasse I und II eine Konformitätsbewertung vorliegen – bei Klasse-II-Produkten unter Einbeziehung einer externen Prüfinstanz (Bewertung durch Dritte).

Konformität von Produkten sowie Informationen und Anweisungen für Benutzer
In Kapitel III des CRA sind unterschiedliche Konformitätsanforderungen für Hersteller regulierter Produkte definiert. Dem Produkt muss eine EU-Konformitätserklärung (Anhang IV) beigefügt und die CE-Kennzeichnung angebracht werden. Die Konformitätserklärung enthält mitunter Angaben zu Hersteller, Produkttyp, IT-Sicherheitszertifizierungen sowie Zertifizierungsstellen.

Darüber hinaus definiert der CRA konkrete Anforderungen an die technische Dokumentation. Diese muss vor dem Marktstart des Produktes vorliegen und während der gesamten Produktlebensdauer oder über einen Zeitraum von fünf Jahren (je nachdem, welcher Zeitraum kürzer ist) gepflegt werden. Konkrete Angaben zu den dort erforderlichen Inhalten sind in Anhang V enthalten. Hierzu zählen etwa eine Bewertung der Cybersicherheitsrisiken, Berichte über absolvierte Audits und Tests sowie ein Exemplar der EU-Konformitätserklärung.

Weiterführende Informationen und Anleitungen für Nutzerinnen und Nutzer sind ebenso in den Vorgaben des CRA enthalten (Anhang II). Diese umfassen z. B. Kontaktdaten des Herstellers, Produktspezifikationen und -funktionen, Sicherheitseigenschaften sowie Angaben zu bekannten Cybersicherheitsrisiken.

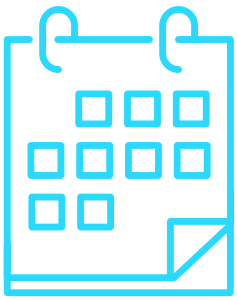
Meldepflichten
Cybersicherheitsvorfälle sind von den Herstellern unverzüglich innerhalb von 24 Stunden an die nationalen Computer Security Incident Response Teams (CSIRTs) zu melden. Das CSIRT, das die Meldung erhält, muss diese über eine einzige Meldeplattform an die anderen CSIRTs weiterleiten. Außerdem müssen Nutzerinnen und Nutzer augenblicklich benachrichtigt und über mögliche Workarounds und Sicherheitsvorkehrungen informiert werden.

Verpflichtungen an Händler und Importeure
Um die Verbreitung von unsicheren digitalen Produkten im EWR zu verhindern, definiert der CRA auch konkrete Anforderungen entlang der Lieferkette gegenüber Importeuren und Händlern. Diese dürfen ausschließlich Produkte in die EU einführen und dort anbieten, die dieselben Sicherheitsvorgaben erfüllen wie die innerhalb des EWR regulierten Produkte. Entsprechend müssen die erforderlichen Konformitätserklärungen, CE-Kennzeichen, Dokumentationen und Informationsmaterialien vorliegen.

Sanktionen: Diese Bußgelder sind vorgesehen

- Grundlegende Verstöße werden mit Bußgeldern von bis zu 15 Mio. Euro bzw. 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet – je nachdem, welcher Betrag höher ist.
- Verstöße gegen andere Verpflichtungen werden mit Bußgeldern von bis zu 10 Mio. Euro bzw. 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet – je nachdem, welcher Betrag höher ist.
- Die Übermittlung falscher, unvollständiger oder irreführender Angaben auf behördliche Anfragen werden mit Geldbußen von bis zu 5 Mio. Euro geahndet.

Timeline: So geht es weiter



Die Mitgliedstaaten haben sich hinsichtlich des CRA auf eine gemeinsame Position geeinigt. Jetzt kann die Verordnung in die Trilogverhandlungen im EU-Parlament eingebracht werden. Mit der finalen Veröffentlichung tritt der CRA nach 20 Tagen in Kraft. Der Geltungsbeginn erfolgt 24 Monate darauf. Unternehmen bleibt also eine Umsetzungsfrist von zwei Jahren.

Myra Security: Mit KRITIS-Expertise die neuen Vorgaben bewältigen

Als spezialisierter Schutzdienstleister für Unternehmen und Organisationen aus hochregulierten Bereichen zählt die Einhaltung strengster Anforderungen an Sicherheit, Datenschutz und Compliance für Myra zum Tagesgeschäft. Grundlage hierfür bilden regelmäßige Audits, eine fortlaufende Qualitätssicherung sowie die umfangreiche Zertifizierung aller zentralen Produkte und Prozesse.

Mit BSI-zertifizierten Lösungen helfen wir Ihnen dabei, Compliance-Hürden zu bewältigen und eine CRA-konforme Absicherung von Webapplikationen und IT-Infrastrukturen aufzubauen.

Made in Germany

Myra Security ist der neue Maßstab für globale IT-Sicherheit.

Sie wollen mehr darüber erfahren, wie Sie mit unseren Lösungen Ihren Umsatz steigern, Ihre Kosten minimieren und Ihre Anwendungen vor bösartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihr Unternehmen. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

Kostenlose Schutzberatung anfordern →

Myra Security GmbH

+49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com