Bild: Pixabay

Der CRA legt strenge Anforderungen an Hersteller, Importeure und Händler fest.

Cyber Resilience Act – Erhöhung der Cybersicherheit

Am 10. Oktober 2024 wurde von der EU der Cyber Resilience Act verabschiedet. Diese Verordnung dient der Erhöhung der Cybersicherheit von Produkten mit einer digitalen Komponente, um Verbraucherinnen, Verbraucher und Unternehmen besser zu schützen.

Der Cyber Resilience Act, kurz CRA, zielt darauf ab, Sicherheitsstandards zu schaffen, die den gesamten Lebenszyklus eines Produkts umfassen. Angesichts der Tatsache, dass die Bedrohungslandschaft stetig komplexer wird und die Zahl der vernetzten Geräte rapide zunimmt, sah die EU die Notwendigkeit, ein Gesetz zu schaffen, das den Schutz vor Cyberangriffen stärkt und die Cybersicherheit über den gesamten Produktlebenszyklus hinweg sicherstellt.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Ziele des Cyber Resilience Act

Der CRA hat drei Hauptziele:

1. Verbesserung der Cybersicherheit von Produkten

Der CRA verlangt von Herstellern, dass sie Sicherheitsvorkehrungen bereits in die Entwicklung und das Design von Produkten einbauen. Dies bedeutet, dass die Cybersicherheit eines Produkts ein zentraler Bestandteil seines Lebenszyklus sein muss, von der Entwicklung bis zur Ausserbetriebnahme.

2. Schutz der Verbraucher und Unternehmen

Der CRA stellt sicher, dass Verbraucher und Unternehmen auf dem EU-Markt Produkte mit einem höheren Sicherheitsstandard vorfinden. Ziel ist es, die Risiken für die Nutzer zu minimieren und eine sicherere digitale Umgebung zu schaffen.

3. Erhöhung des Wettbewerbs

Durch die Einführung von einheitlichen Standards fördert der CRA den Wettbewerb auf dem Markt für Cybersicherheitsprodukte und -dienste. Unternehmen müssen sich nun stärker auf die Sicherheit ihrer Produkte konzentrieren, was langfristig zu innovativeren und sichereren Lösungen führen soll.

Anforderungen und Verpflichtungen für Hersteller

Der CRA legt strenge Anforderungen an Hersteller, Importeure und Händler fest. Hier sind einige der wichtigsten Verpflichtungen:

Sicherheitsanforderungen

Hersteller müssen sicherstellen, dass ihre Produkte vor Markteinführung bestimmten Cybersicherheitsanforderungen entsprechen. Dazu gehört der Schutz vor unbefugtem Zugriff, die Sicherstellung der Datenintegrität und die Gewährleistung der Verfügbarkeit von Diensten. Diese Anforderungen gelten für alle Geräte, die eine Netzwerkverbindung haben, wie zum Beispiel IoT-Geräte, Computer und Smart-Home-Systeme. Zu diesem Schritt gehört auch eine umfassende Risiko-Bewertung.

Sicherheitsupdates

Hersteller sind verpflichtet, über den gesamten Lebenszyklus eines Produkts Sicherheitsupdates bereitzustellen, mindestens aber über 5 Jahre. Dies bedeutet, dass Schwachstellen, die nach dem Verkauf eines Produkts entdeckt werden, umgehend behoben werden müssen, und das Produkt kontinuierlich gegen neue Bedrohungen abgesichert wird. Die Hersteller müssen den Nutzern ausserdem Informationen über die Unterstützung und die erwartete Lebensdauer des Produkts zur Verfügung stellen.

Produktüberwachung und -test

Hersteller müssen regelmässige Tests durchführen und Überwachungsmassnahmen implementieren, um mögliche Schwachstellen in ihren Produkten frühzeitig zu erkennen und zu beheben. Dies umfasst die Durchführung von Penetrationstests, die Schwachstellenanalyse und die kontinuierliche Verbesserung der Sicherheitsmassnahmen.

Verpflichtung zur Offenlegung

Sollte ein Hersteller eine Schwachstelle entdecken, ist er verpflich-

tet, diese den zuständigen Behörden zu melden und die betroffenen Nutzer zu informieren. Diese Offenlegungspflicht stellt sicher, dass Sicherheitsprobleme schnell und effektiv behandelt werden können.

Einhaltung und Durchsetzung

Der CRA sieht strenge Massnahmen zur Durchsetzung vor. Hersteller, die die Vorschriften des CRA nicht einhalten, können mit erheblichen Geldstrafen belegt werden. Diese Strafen können bis zu 2,5 Prozent des weltweiten Jahresumsatzes eines Unternehmens betragen (oder bis zu 15 Millionen Euro, je nachdem, welcher Betrag höher ist). Darüber hinaus können Produkte, die nicht den Anforderungen entsprechen, vom Markt genommen oder die Produktion gestoppt werden. In schwerwiegenden Fällen kann eine vollständige Rücknahme oder ein Rückruf des Produkts verlangt werden.

Die Einhaltung wird durch nationale Behörden in den Mitgliedstaaten der EU überwacht, die für die Marktaufsicht zuständig sind. Diese Behörden haben die Befugnis, Kontrollen durchzuführen, Produkte zu testen und bei Bedarf auch zu beschlagnahmen. Auch die Europäische Agentur für Cybersicherheit (ENISA) spielt eine wichtige Rolle bei der Koordination und Unterstützung der nationalen Aufsichtsbehörden.

Betroffene Produkte

Die betroffenen Produkte werden in verschiedene Kategorien gemäss ihrer Risikoklasse eingeteilt. Insbesondere Produkte und Systeme, die in der kritischen Infrastruktur, dem produzierenden Gewerbe und dem Industrie- und Energiesektor zum Einsatz kommen, werden einer höheren Risikoklasse zugeordnet.

Standard-Kategorie

Selbstbewertung und Selbsterklärung
- Foto- und Bildbearbeitung
- Videospiele
- Allgemeine Software und Geräte
- Alle anderen Produkte, die nicht unter die Kategorien wichtige und kritische Produkte fallen

Hinweis: In diese Kategorie fallen etwa 90 Prozent der Produkte.

Wichtige Produkte

Konformitätsbewertung und Zertifizierung durch Zertifizierungsstelle

Klasse 1
- Eigenständige und eingebettete Browser
- Mikrokontroller und Mikroprozessoren mit sicherheitsrelevanten Funktionen
- Passwortmanager
- Betriebssysteme
- Smart Home, virtuelle Assistenten

Klasse 2
- Firewalls
- Angriffserkennungs- und/oder Präventivsysteme
- Manipulationssichere Mikrocontroller und Mikroprozessoren

Kritische Produkte

Verpflichtende Konformitätsbewertung und Zertifizierung durch Zertifizierungsstelle
- Smartcards
- Hardwaregeräte mit Security Boxes
- Smart-Meter-Gateways
- Jedes Produkt, das zu einer kritischen Abhängigkeit wesentlicher Einrichtungen gemäss der NIS2-Richtlinie führt

Zeitplan für die Umsetzung

Der Zeitplan für die Umsetzung der Anforderungen sieht eine schrittweise Anpassung vor. Die Compliance-Anforderungen werden in zwei Schritten eingeführt:

1. Die geforderten Meldepflichten müssen 21 Monate nach der endgültigen Verabschiedung des Gesetzes erfüllt sein – somit Anfang 2026.
2. Hersteller, Importeure und Händler müssen 36 Monate nach der endgültigen Verabschiedung des Gesetzes alle Vorgaben erfüllen – somit Mitte 2027.

Der CRA trat nach seiner Veröffentlichung im Amtsblatt der Europäischen Union Anfang Dezember 2024 in Kraft. Während der zweijährigen Übergangsphase müssen Unternehmen sicherstellen, dass sie die notwendigen Dokumentationen und Compliance-Verfahren etablieren, um die Konformität mit den Vorschriften nachweisen zu können. Ab Ende dieser Übergangsfrist – also voraussichtlich ab 2026 – sind alle Unternehmen verpflichtet, die Anforderungen des CRA vollständig umzusetzen.

Fazit

Der Cyber Resilience Act wird voraussichtlich eine tiefgreifende Auswirkung auf die Cybersicherheitslandschaft haben. Er wird die Sicherheit der Produkte verbessern, die in der EU verkauft werden. Unternehmen, die in der EU tätig sind, werden gezwungen sein, ihre Produkte und Dienstleistungen sicherer zu gestalten, was auch internationale Märkte beeinflussen könnte. Die erfolgreiche Umsetzung des CRA wird jedoch davon abhängen, wie gut die Unternehmen und die zuständigen Behörden die Anforderungen erfüllen können und ob es gelingt, die Herausforderungen bei der Einhaltung und Durchsetzung zu überwinden.