EU Cyber Resilience Act: Neue Meldepflichten – was Schweizer Unternehmen beachten müssen

Author: Elena Martin
Quelle: EU Cyber Resiliance Act - Verordnung EU 2024/2847
Baar, 4. September 2026

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Seit dem 11. September 2026 gelten neue Meldepflichten des EU Cyber Resilience Act (CRA). Hersteller von Hard- und Software müssen bestimmte Sicherheitsvorfälle und aktiv ausgenutzte Schwachstellen teilweise bereits innerhalb von 24 Stunden melden. Auch Schweizer Unternehmen können betroffen sein, wenn ihre Produkte auf dem EU-Markt angeboten werden.

Cyber Resilience Act: Cybersicherheit wird zur Produkteigenschaft

Mit dem **Cyber Resilience Act (CRA), Verordnung (EU) 2024/2847**, schafft die EU einen umfassenden Rechtsrahmen für die Cybersicherheit sogenannter **Produkte mit digitalen Elementen**.

Erfasst werden grundsätzlich Hard- und Softwareprodukte, die auf dem EU-Markt bereitgestellt werden. Dazu gehören beispielsweise Software, Apps, IoT-Geräte, Router und Netzwerkkomponenten, Smart-Home-Produkte, vernetzte Maschinen und Steuerungen sowie bestimmte Hard- und Softwarekomponenten. Die umfassenden Anforderungen des CRA gelten grundsätzlich ab dem **11. Dezember 2027**. Die Meldepflichten nach Art. 14 CRA gelten jedoch bereits seit dem **11. September 2026**.

Was muss gemeldet werden?

Hersteller müssen insbesondere zwei Arten von Cybersecurity-Ereignissen melden:

- **aktiv ausgenutzte Schwachstellen** eines Produkts; sowie
- **schwerwiegende Sicherheitsvorfälle**, die sich auf die Sicherheit eines Produkts mit digitalen Elementen auswirken.

Wichtig zu beachten sind dabei die geltenden kurzen Fristen!

- **24 Stunden:** Frühwarnung
- **72 Stunden:** Hauptmeldung mit weitergehenden Informationen
- **14 Tage:** Abschlussbericht bei aktiv ausgenutzten Schwachstellen nach Verfügbarkeit einer Korrektur- oder Minderungsmassnahme
- **1 Monat:** grundsätzlich Abschlussbericht bei schwerwiegenden Sicherheitsvorfällen.

Die Meldungen erfolgen über die von der EU-Agentur für Cybersicherheit **ENISA** eingerichtete CRA Single Reporting Platform.

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug

Warum betrifft der CRA auch Schweizer Unternehmen?

⇒ Der Sitz eines Unternehmens ausserhalb der EU schützt nicht vor der Anwendung des CRA.

Entscheidend ist insbesondere, ob ein **Produkt mit digitalen Elementen auf dem EU-Markt bereitgestellt wird**. Damit können auch Schweizer Hersteller betroffen sein, die beispielsweise Software, IoT-Produkte, elektronische Komponenten oder digital gesteuerte Produkte in EU-Mitgliedstaaten vertreiben. Dies gilt auch bei einem indirekten Vertrieb über **Importeure oder Distributoren**.

⇒ Schweizer Unternehmen sollten deshalb klären: **Gelangen unsere Produkte direkt oder indirekt auf den EU-Markt – und fallen diese unter den CRA?**

Zu beachten ist zudem, dass die seit September 2026 geltenden Meldepflichten auch Produkte betreffen können, die bereits auf dem EU-Markt bereitgestellt wurden. Unternehmen sollten daher auch ihr bestehendes Produktportfolio überprüfen.

24-Stunden-Frist erfordert klare interne Prozesse

Die kurze Meldefrist stellt Unternehmen vor erhebliche organisatorische Herausforderungen.

Sicherheitsvorfälle müssen schnell erkannt, intern weitergeleitet sowie technisch und rechtlich beurteilt werden. Es muss im Voraus klar sein, **wer einen möglichen CRA-Fall beurteilt, wer entscheidet und wer die Meldung veranlasst**.

Der **interne Prozess** sollte daher möglichst einfach ausgestaltet sein: **Erkennen → Eskalieren → Beurteilen → Entscheiden → Melden**

Verträge mit Lieferanten und Vertriebspartnern überprüfen

Auch die Liefer- und Vertriebskette ist einzubeziehen. Sicherheitslücken können beispielsweise Softwarebibliotheken, Firmware, Hardwarekomponenten, Cloud-Dienste oder Produkte externer Entwickler und Zulieferer betreffen.

Informiert ein Lieferant den Hersteller erst nach mehreren Tagen über eine kritische Schwachstelle, kann die Einhaltung der CRA-Meldefristen gefährdet sein.

Verträge mit **Entwicklern, Zulieferern, EU-Importeuren und Vertriebspartnern** sollten deshalb auf ausreichende Cybersecurity-, Informations-, Eskalations- und Mitwirkungspflichten überprüft werden.

Was Schweizer Unternehmen jetzt tun sollten

Unternehmen mit EU-Handelsbeziehungen sollten insbesondere:

1. **Produktportfolio und EU-Marktzugang prüfen:** Welche Produkte mit digitalen Elementen gelangen in die EU?
2. **Rollen klären:** Wer ist Hersteller, Importeur, Distributor oder Bevollmächtigter?
3. **Meldeprozess einrichten:** Können die 24- und 72-Stunden-Fristen eingehalten werden?
4. **Vulnerability Management überprüfen:** Wie werden Schwachstellen erkannt, bewertet, dokumentiert und behoben?
5. **Verträge anpassen:** Sind Lieferanten und Vertriebspartner zu einer unverzüglichen Information und Mitwirkung verpflichtet?
6. **CRA-Compliance für 2027 vorbereiten:** Sind Produktentwicklung, Sicherheitsupdates, Dokumentation und Konformitätsprozesse auf die vollständige Anwendung des CRA vorbereitet?

Kurz und prägnant ….

Der **EU Cyber Resilience Act betrifft auch Schweizer Unternehmen**, wenn ihre Hard- oder Softwareprodukte auf dem EU-Markt bereitgestellt werden.

Seit dem **11. September 2026** stehen insbesondere die neuen Meldepflichten im Fokus. Unternehmen müssen sicherstellen, dass relevante Schwachstellen und Sicherheitsvorfälle schnell erkannt, beurteilt und gegebenenfalls innerhalb von 24 bzw. 72 Stunden gemeldet werden können.

Gleichzeitig sollte die vollständige CRA-Compliance vorbereitet werden: Ab dem **11. Dezember 2027** gelten grundsätzlich die umfassenden Anforderungen des Cyber Resilience Act.

Für Schweizer Unternehmen mit EU-Geschäft empfiehlt sich daher eine frühzeitige **CRA-Gap-Analyse des Produktportfolios, der internen Cybersecurity-Prozesse und der Verträge innerhalb der Liefer- und Vertriebskette**.