CRA Single Reporting Platform

Ab 11.09.2026

Meldung von Vorfällen & Schwachstellen nach dem Cyber Resilience Act

1. Übersicht: Was ist die Single Reporting Platform? (SRP)

Die **CRA Single Reporting Platform (SRP)** ist das zentrale Online-Tool für Hersteller und Open Source-Software-Stewards zur Erfüllung ihrer gesetzlichen Meldepflichten gemäß dem Cyber Resilience Act (CRA).

Das System dient der Vereinfachung von EU-weiten Meldungen nach dem Prinzip **„Report once“**: Über eine einzige elektronische Plattform werden alle relevanten nationalen und europäischen Behörden gleichzeitig informiert. Höchste Sicherheits- und Verschlüsselungsstandards gewährleisten dabei die Vertraulichkeit der eingereichten Daten.

2. Für wen gilt die Plattform?

Hersteller

Verpflichtet zur Meldung aktiv ausgenutzter Schwachstellen und schwerwiegender Sicherheitsvorfälle bei Produkten mit digitalen Elementen, die auf dem EU-Markt vertrieben werden.

Open-Source-Software-Trägerorganisation

Unterliegen der Meldepflicht, soweit sie aktiv an der Entwicklung von Produkten mit digitalen Elementen beteiligt sind.

3. Was sind die neuen Meldepflichten?

Ab dem **11. September 2026** verpflichtet der CRA zur strukturierten Erfassung und Übermittlung von zwei zentralen Ereignisarten:

Aktiv ausgenutzte Schwachstellen

Sicherheitslücken in Produkten mit digitalen Elementen, bei denen bekannt ist, dass sie aktuell von böswilligen Akteuren ausgenutzt werden (gemäß Artikel 3(42) CRA).

Schwerwiegende Sicherheitsvorfälle

Ereignisse mit schwerwiegenden Auswirkungen auf die Sicherheit des Produkts (z. B. Beeinträchtigung von Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gemäß Artikel 3(44) & 14(5)).

4. Bei welchem nationalen CSIRT müssen Sie melden?

Die Auswahl des zuständigen nationalen CSIRT (Computer Security Incident Response Team) erfolgt primär über den **Hauptsitz / die Hauptniederlassung** Ihres Unternehmens in der Europäischen Union.

Detailkriterien zur exakten Ermittlung des zuständigen CSIRT sind in **Artikel 14(7) des CRA** geregelt. Die Plattform leitet die Meldung nach der Eingabe automatisch an das richtige nationale CSIRT weiter.

5. Wann müssen die Vorfälle gemeldet werden?

Der Meldeprozess beginnt in dem Moment, in dem Sie als Hersteller oder OSS-Steward Kenntnis von einer aktiven Ausnutzung oder einem schwerwiegenden Vorfall erlangen:

24 Std.

1. Frühmeldung

Innerhalb von 24 Stunden nach Kenntnisnahme über das Ereignis.

72 Std.

2. Vorfallsmeldung (Notification)

Innerhalb von 72 Stunden mit allgemeinen Informationen und Erstbewertung.

Final

3. Abschlussbericht (Report)

Schwachstellen: Max. 14 Tage nach Patch Verfügbarkeit.
Vorfälle: Innerhalb von 1 Monat nach der 72h Meldung

6. Was geschieht, nachdem die Meldungen eingereicht wurden?

1. **Erstempfang & Weiterleitung:** Das primär zuständige nationale CSIRT empfängt die Meldung und verbreitet die Informationen unverzüglich an andere betroffene CSIRTs in EU Mitgliedstaaten, in denen das Produkt ebenfalls verfügbar ist.
2. **Synchrone Einbindung der ENISA:** Die Benachrichtigung wird zeitgleich der Agentur der Europäischen Union für Cybersicherheit (ENISA) zugänglich gemacht.
3. **Einbindung der Marktüberwachung:** Die nationalen CSIRTs teilen relevante Informationen mit den jeweiligen nationalen Marktüberwachungsbehörden, damit diese ihren Durchsetzungsaufgaben nachkommen können.

7. Kann die Verbreitung von Informationen verzögert werden?

Ausnahmeregelung gemäß Artikel 16(2) CRA

Ja. Unter außergewöhnlichen Umständen kann die Verbreitung von Benachrichtigungen und Informationen an andere Behörden oder die Öffentlichkeit vorübergehend verzögert werden.

Die genauen Bedingungen und Kriterien für eine solche Verzögerung sind in der Delegierten Verordnung (EU) 2026/881 der Kommission präzise festgelegt (z. B. zur Vermeidung unmittelbarer Cybersicherheitsrisiken während der Patch-Entwicklung)