CRA
SINGLE
REPORTING
PLATFORM

Factsheet zur einheitlichen Meldeplattform gemäß Cyberresilienz-Verordnung

Meldung von aktiv ausgenutzten Schwachstellen und schwerwiegenden Sicherheitsvorfällen über die einheitliche Meldeplattform (engl. Cyber Resilience Act Single Reporting Platform, CRA-SRP).

Was?

Seit dem 11. September 2026 müssen Hersteller gemäß der Cyberresilienz-Verordnung aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle melden, die sich auf die Sicherheit von Produkten mit digitalen Elementen, die auf dem EU-Markt verkauft werden, auswirken.

Gemäß der Cyberresilienz-Verordnung müssen auch Verwalter quelloffener Software (engl. Open-Source Software Stewards) diese Ereignisse melden, soweit sie an der Entwicklung von Produkten mit digitalen Elementen beteiligt sind.

Für wen?

Hersteller

Verwalter quelloffener Software (Open-Source Software Stewards – OSS Stewards)

Welche neuen Meldepflichten gelten für Sie?

Die einheitliche Meldeplattform gemäß Cyberresilienz-Verordnung ist ein Online-Tool für Hersteller und für Verwalter quelloffener Software, mit dem diese ihrer Pflicht zur Meldung aktiv ausgenutzter Schwachstellen und schwerwiegender Sicherheitsvorfälle nachkommen können. Die einheitliche Meldeplattform gemäß Cyberresilienz-Verordnung wurde entwickelt, um die Meldepflichten in der Europäischen Union (EU) zu vereinfachen. Es handelt sich um ein elektronisches System, mit dem durch eine einzige Meldung alle einschlägigen Behörden informiert werden können. Die Plattform ist mit Sicherheitsvorkehrungen zum Schutz der Vertraulichkeit ausgestattet.

Jede Meldung ermöglicht die automatische Übermittlung von Informationen an Ihr koordinierendes CSIRT, bei dem die Meldung zunächst eingeht, an die anderen nationalen CSIRTs der EU, in deren Ländern das Produkt mit digitalen Elementen erhältlich ist, sowie an die Agentur der Europäischen Agentur für Cybersicherheit (ENISA).

Woher wissen Sie, an welches koordinierende CSIRT Sie Meldung erstatten sollen?

Im Allgemeinen wird das koordinierende CSIRT, an das Sie über die einheitliche Meldeplattform Meldung erstatten sollten, vor allem durch Ihren Hauptgeschäftssitz bestimmt. Artikel 14 Absatz 7 der Cyberresilienz-Verordnung enthält detaillierte Informationen, anhand derer Sie das koordinierende CSIRT ermitteln können, dem Sie Meldung erstatten müssen.

Welche Ereignisse müssen Sie melden?

- **Aktiv ausgenutzte Schwachstellen:** Gemäß Artikel 3 Absatz 42 der Cyberresilienz-Verordnung Schwachstellen in Produkten mit digitalen Elementen, von denen bekannt ist, dass sie derzeit von einem böswilligen Akteur ausgenutzt werden.
- **Schwerwiegende Sicherheitsvorfälle:** Gemäß Artikel 3 Absatz 44 Sicherheitsvorfälle, die schwerwiegende Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen haben (z. B. Beeinträchtigung der Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit); die Kriterien für die Einstufung als „schwerwiegend" sind in Artikel 14 Absatz 5 festgelegt.

Wann müssen Sie solche Ereignisse melden?

Der Meldeprozess beginnt in dem Moment, in dem Sie als Hersteller oder OSS-Verwalter Kenntnis von der aktiven Ausnutzung einer Schwachstelle oder einem schwerwiegenden Sicherheitsvorfall erlangen. Einhaltung der folgenden Fristen:

Frühwarnung

- Innerhalb von **24 Stunden** nach Bekanntwerden der Schwachstelle oder des Sicherheitsvorfalls.

Meldung von aktiv ausgenutzten Schwachstellen / schwerwiegenden Sicherheitsvorfällen

- Innerhalb von **72 Stunden** nach Bekanntwerden unter Bereitstellung allgemeiner Informationen und einer ersten Bewertung.

Abschlussbericht:

- **Bei Schwachstellen:** Spätestens 14 Tage, nachdem eine Korrekturmaßnahme (z. B. ein Patch) zur Verfügung steht.
- **Bei schwerwiegenden Vorfällen:** Innerhalb eines Monats nach Übermittlung der 72-Stunden-Meldung über aktiv ausgenutzte Schwachstellen / schwerwiegende Sicherheitsvorfälle.

CRA
SINGLE
REPORTING
PLATFORM

Was passiert, nachdem die Meldungen übermittelt wurden?

Sobald Meldungen übermittelt wurden, leitet das koordinierende CSIRT, das die Meldung ursprünglich erhalten hat, die Informationen unverzüglich an weitere zuständige CSIRTs in den EU-Mitgliedstaaten weiter, in denen das Produkt ebenfalls erhältlich ist. Die Meldung wird gleichzeitig der ENISA zur Verfügung gestellt.

Die koordinierenden CSIRTs werden zudem bestimmte Informationen an ihre jeweiligen Marktüberwachungsbehörden weitergeben, damit diese ihren Durchsetzungspflichten nachkommen können.

Kann die Verbreitung von Informationen aufgeschoben werden?

Ja, unter außergewöhnlichen Umständen kann die Verbreitung von Informationen gemäß Artikel 16 Absatz 2 der Cyberresilienz-Verordnung verzögert werden. Die Bedingungen dafür sind in der Delegierten Verordnung (EU) 2026/881 der Kommission festgelegt.

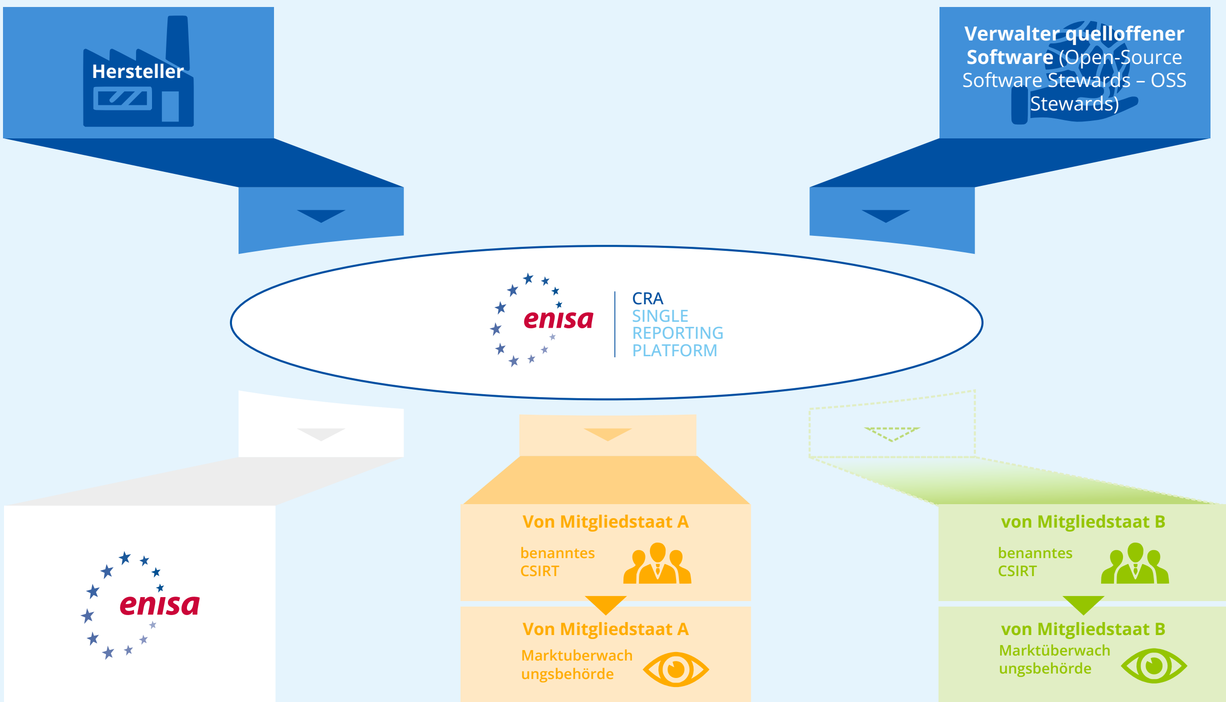
Wie benutzen Sie die Plattform?

1 Anmeldung

2 Koordinierendes CSIRT auswählen

3 Informationen vervollständigen und übermitteln

Einfacher Meldefluss



EUROPEAN UNION AGENCY FOR CYBERSECURITY

Weitere Informationen finden Sie auf der FAQ-Seite der ENISA zur einheitlichen Meldeplattform unter https://www.enisa.europa.eu/cra-srp. Diese umfasst auch Verweise auf die Leitlinien der Europäischen Kommission zur Cyberresilienz-Verordnung („European Commission's guidance on the CRA"), die in Abschnitt 9.1 weitere Erläuterungen zu den Meldepflichten enthalten.

Wenn Sie Hilfe benötigen, wenden Sie sich bitte an: cra-srp-helpdesk@enisa.europa.eu