Amtsblatt
der Europäischen Union

DE
Reihe L

2026/881

20.4.2026

DELEGIERTE VERORDNUNG (EU) 2026/881 DER KOMMISSION

vom 11. Dezember 2025

zur Ergänzung der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates durch Festlegung der Modalitäten und Bedingungen für die Geltendmachung von Cybersicherheitsgründen im Zusammenhang mit dem Aufschub der Verbreitung von Meldungen

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) ([1]), insbesondere auf Artikel 14 Absatz 9,

in Erwägung nachstehender Gründe:

(1) Unter außergewöhnlichen Umständen und insbesondere auf Antrag des Herstellers und unter Berücksichtigung des Grades der Sensibilität der gemeldeten Informationen und aus berechtigten Gründen der Cybersicherheit kann das als Koordinator benannte Computer-Notfallteam (Computer Security Incident Response Team – CSIRT), das die Meldung über eine aktiv ausgenutzte Schwachstelle oder einen schwerwiegenden Sicherheitsvorfall mit Auswirkungen auf die Sicherheit eines Produkts mit digitalen Elementen ursprünglich erhalten hat (im Folgenden „CSIRT, das die Meldung ursprünglich erhalten hat“), beschließen, die Verbreitung der Meldung über die einheitliche Meldeplattform an die als Koordinatoren benannten CSIRTs, in deren Hoheitsgebiet das Produkt mit digitalen Elementen nach Angaben des Herstellers bereitgestellt wurde (im Folgenden „die zuständigen CSIRTs“), so lange aufschieben, wie unbedingt erforderlich. Daher müssen die Modalitäten und Bedingungen für die Geltendmachung der genannten Gründe festgelegt werden. Liegen solche Gründe vor, darf das CSIRT, das die Meldung ursprünglich erhalten hat, die Verbreitung an die zuständigen CSIRTs so lange aufschieben, wie unbedingt erforderlich, ist jedoch nicht dazu verpflichtet. Nach Artikel 16 Absatz 2 der Verordnung (EU) 2024/2847 sollte das CSIRT, das die Meldung ursprünglich erhalten hat und beschließt, die genannten Gründe geltend zu machen, die Agentur der Europäischen Union für Cybersicherheit (ENISA) unverzüglich über die Entscheidung zum Aufschub, deren Begründung sowie darüber unterrichten, wann es die Meldung weiterzuleiten gedenkt.

(2) Nach Artikel 16 Absatz 2 Unterabsatz 2 der Verordnung (EU) 2024/2847 gelten die in der vorliegenden Verordnung festgelegten Modalitäten und Bedingungen für die Geltendmachung von Cybersicherheitsgründen nicht für den Zugang der ENISA zu den gemeldeten Informationen. Der Zugang der ENISA zu den gemeldeten Informationen darf nur unter besonderen außergewöhnlichen Umständen beschränkt werden — wenn nämlich der Hersteller in seiner Meldung angibt, dass eine der drei in Artikel 16 Absatz 2 Unterabsatz 3 Buchstaben a, b oder c der Verordnung (EU) 2024/2847 genannten Bedingungen erfüllt ist, und auch dann nur in Bezug auf den 72-stündigen Zeitraum für die Meldung von Schwachstellen gemäß Artikel 14 Absatz 2 Buchstabe b der Verordnung (EU) 2024/2847. In solchen Fällen sind die einzigen Informationen, die der ENISA gleichzeitig zur Verfügung zu stellen sind, die Information, dass der Hersteller eine Meldung übermittelt hat, allgemeine Informationen über das Produkt mit digitalen Elementen, Informationen über die allgemeine Art der Ausnutzung sowie die Information, dass sicherheitsrelevante Gründe geltend gemacht wurden.

(3) Der Zugang zu den gemeldeten Informationen ermöglicht es den CSIRTs, sich einen Überblick über das Sicherheitsumfeld in ihrem jeweiligen Hoheitsgebiet zu verschaffen und Abhilfemaßnahmen zu ergreifen, womit das allgemeine Cybersicherheitsniveau in der Union erhöht wird. Daher sollten weitere Beschränkungen für die Verbreitung von Meldungen aufgrund der Art der gemeldeten Informationen nur in Fällen möglich sein, in denen die sich aus der weiteren Verbreitung ergebenden Cybersicherheitsrisiken angesichts der Sensibilität der gemeldeten Informationen die Vorteile für die Sicherheit der Union überwiegen und diese Risiken nicht durch Beschränkungen der Bearbeitung und Weitergabe der Meldung durch geeignete Protokolle, die innerhalb des CSIRTs-Netzes verwendet werden, wie das Traffic Light Protocol (TLP) oder das Permissible Actions Protocol (PAP) angemessen

([1]) ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

gemindert werden können. Dies kann etwa der Fall sein, wenn ein Hersteller dem CSIRT, das die Meldung ursprünglich erhalten hat, meldet, dass er voraussichtlich in Kürze eine Risikominderungsmaßnahme (z. B. einen Patch) bereitstellt. Dies kann auch der Fall sein, wenn das CSIRT, das die Meldung ursprünglich erhalten hat, beschließt, nur Teile der Meldung zu verbreiten, diese Teile aber ausreichend sind, damit die zuständigen CSIRTs angemessene Risikominderungsmaßnahmen ergreifen können. Dies kann im Interesse der Förderung der Zusammenarbeit zwischen Herstellern, CSIRTs und Sicherheitsforschern bei der Ermittlung und Offenlegung von Schwachstellen auch dann der Fall sein, wenn das CSIRT als vertrauenswürdiger Vermittler für ein laufendes Verfahren zur koordinierten Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([2]) fungiert. Beschließt das CSIRT in einem solchen Fall, die Verbreitung einer Meldung aufzuschieben, so schiebt es diese gemäß Artikel 16 Absatz 6 der Verordnung (EU) 2024/2847 um einen Zeitraum auf, der nicht länger ist als unbedingt erforderlich, bis die an dem Verfahren zur koordinierten Offenlegung von Schwachstellen beteiligten Parteien ihre Zustimmung zur Offenlegung erteilt haben.

(4) Die in der Meldung enthaltenen Informationen helfen den CSIRTs, ihre Aufgaben im Zusammenhang mit der Risikominderung und der Bewältigung von Sicherheitsvorfällen zu erfüllen. In seltenen Fällen könnten diese Informationen jedoch ausreichen, um die Entwicklung einer Ausnutzungstechnik ohne weitere Recherchen zu ermöglichen, selbst durch Akteure mit begrenzten Fähigkeiten und Ressourcen. Würden solche Informationen böswilligen Akteuren zugänglich, wäre die Cybersicherheit der Union stark beeinträchtigt, da sie leicht ausgenutzt werden können. Dies könnte etwa der Fall sein, wenn sich die anfällige Version einer Software nur geringfügig von früheren, nicht anfälligen Versionen unterscheidet. Ist in solchen Fällen das CSIRT, das die Meldung ursprünglich erhalten hat, der Auffassung, dass die sich aus der weiteren Verbreitung ergebenden Cybersicherheitsrisiken durch Beschränkungen der Bearbeitung und Weitergabe nicht angemessen gemindert werden können, kann es beschließen, die Verbreitung aufzuschieben, bis eine wirksame Risikominderungsmaßnahme, z. B. eine Sicherheitsaktualisierung oder Orientierungshilfen für die Nutzer, verfügbar ist.

(5) Ist ein zuständiges CSIRT nicht in der Lage, die gemeldeten Informationen angemessen zu schützen, könnten sensible Informationen böswilligen Akteuren zugänglich werden und im gesamten Binnenmarkt ausgenutzt werden. Daher kann das CSIRT, das die Meldung ursprünglich erhalten hat, bei ernsten Bedenken in Bezug auf die Fähigkeit eines zuständigen CSIRT, die Vertraulichkeit der gemeldeten Informationen zu gewährleisten, beschließen, die Verbreitung der Meldung nur gegenüber dem betreffenden zuständigen CSIRT aufzuschieben, bis die Bedenken ausgeräumt sind. Dies kann der Fall sein, wenn ein zuständiges CSIRT von einem Cybersicherheitsvorfall betroffen ist, der seine Fähigkeit zum sicheren Betrieb beeinträchtigt, oder wenn es Belege oder Informationen dafür gibt, dass in Bezug auf die Fähigkeiten des CSIRT erhebliche Mängel festgestellt wurden, z. B. ein schwerwiegender Mangel an Ressourcen, der seine Fähigkeit zur Wahrnehmung seiner Aufgaben beeinträchtigt, oder die Nutzung veralteter oder anfälliger Software.

(6) Um zu verhindern, dass sensible Informationen böswilligen Akteuren zugänglich werden, sollte das CSIRT, das die Meldung ursprünglich erhalten hat, in Fällen, in denen die einheitliche Meldeplattform gemäß Artikel 16 der Verordnung (EU) 2024/2847 durch einen Cybersicherheitsvorfall beeinträchtigt wurde, die Verbreitung über die einheitliche Meldeplattform aufschieben, bis die Plattform die Vertraulichkeit der gemeldeten Informationen wieder gewährleisten kann.

(7) Nach Artikel 16 Absatz 2 Unterabsatz 1 der Verordnung (EU) 2024/2847 muss das CSIRT, das die Meldung ursprünglich erhalten hat, die Meldung nicht an andere zuständige CSIRTs weiterleiten, wenn der Hersteller angibt, dass das Produkt mit digitalen Elementen nur auf dem Markt des Mitgliedstaats des CSIRT, das die Meldung ursprünglich erhalten hat, bereitgestellt wurde.

(8) Die Kommission hat bei der Ausarbeitung des Entwurfs des Delegierten Rechtsakts die einschlägigen Interessenträger konsultiert und deren Ansichten eingeholt; außerdem hat sie die Sachverständigengruppe für die Cybersicherheit von Produkten mit digitalen Elementen konsultiert.

(9) Im Einklang mit Artikel 14 Absatz 9 der Verordnung (EU) 2024/2847 hat die Kommission bei der Ausarbeitung des Entwurfs des Delegierten Rechtsakts eng mit dem gemäß Artikel 15 der Richtlinie (EU) 2022/2555 eingerichteten CSIRTs-Netzwerk und der ENISA zusammengearbeitet —

([2]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand

In dieser Verordnung werden die Modalitäten und Bedingungen für die Geltendmachung der in Artikel 16 Absatz 2 der Verordnung (EU) 2024/2847 genannten Gründe im Zusammenhang mit der Cybersicherheit festgelegt, aus denen das als Koordinator benannten CSIRT, das eine Meldung gemäß Artikel 14 Absätze 1 und 3 und Artikel 15 Absätze 1 und 2 der genannten Verordnung ursprünglich erhalten hat, die Verbreitung der Meldung an die als Koordinatoren benannten CSIRTs, in deren Hoheitsgebiet das Produkt mit digitalen Elementen nach Angabe des Herstellers bereitgestellt wurde, aufschieben kann.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „CSIRT, das die Meldung ursprünglich erhalten hat“ das gemäß Artikel 14 Absätze 1 und 3 und Artikel 15 Absätze 1 und 2 der Verordnung (EU) 2024/2847 als Koordinator benannte CSIRT, bei dem die Meldung ursprünglich eingegangen ist;
2. „zuständiges CSIRT“ bezeichnet das als Koordinator benannte CSIRT, in dessen Hoheitsgebiet das Produkt mit digitalen Elementen nach Angabe des Herstellers bereitgestellt wurde.

Artikel 3

Modalitäten und Bedingungen für die Geltendmachung von Gründen der Cybersicherheit in Bezug auf die Art der gemeldeten Informationen

Das CSIRT, das die Meldung ursprünglich erhalten hat, kann beschließen, die Verbreitung von Meldungen oder Teilen davon an die zuständigen CSIRTs so lange aufzuschieben, wie unbedingt erforderlich, wenn angesichts der Sensibilität der gemeldeten Informationen die aus der Verbreitung ergebenden Cybersicherheitsrisiken gegenüber den Vorteilen in Bezug auf die Sicherheit überwiegen und diese Risiken nicht durch Beschränkungen der Bearbeitung oder Weitergabe der Meldung durch geeignete Protokolle wie das Traffic Light Protocol (TLP) oder das Permissible Actions Protocol (PAP) gemindert werden können und wenn mindestens eine der folgenden Bedingungen erfüllt ist:

a) Der Hersteller hat dem CSIRT, das die Meldung ursprünglich erhalten hat, mitgeteilt, dass voraussichtlich innerhalb von 72 Stunden eine wirksame Risikominderungsmaßnahme, z. B. eine Sicherheitsaktualisierung oder Orientierungshilfen für die Nutzer, verfügbar gemacht wird; wird innerhalb dieses Zeitrahmens keine wirksame Risikominderungsmaßnahme verfügbar gemacht, so leitet das CSIRT, das die Meldung ursprünglich erhalten hat, die Meldung an die zuständigen CSIRTs weiter;

b) die in der Meldung enthaltenen Informationen werden angesichts der Art der gemeldeten aktiv ausgenutzten Schwachstelle als ausreichend erachtet, um eine Technik zu ihrer Ausnutzung zu entwickeln, insbesondere wenn die Schwachstelle von Akteuren mit begrenzten Fähigkeiten und Ressourcen leicht erkannt und ausgenutzt werden kann; sobald eine wirksame Risikominderungsmaßnahme, z. B. eine Sicherheitsaktualisierung oder Orientierungshilfen für die Nutzer, verfügbar ist, leitet das CSIRT, das die Meldung ursprünglich erhalten hat, die Meldung an die zuständigen CSIRTs weiter;

c) das CSIRT, das die Meldung ursprünglich erhalten hat, kann ist den zuständigen CSIRTs ausreichende Informationen zur Verfügung stellen, damit die zuständigen CSIRTs angemessene Risikominderungsmaßnahmen ergreifen können; sobald eine wirksame Risikominderungsmaßnahme, z. B. eine Sicherheitsaktualisierung oder Orientierungshilfen für die Nutzer, verfügbar ist, leitet das CSIRT, das die Meldung ursprünglich erhalten hat, die Meldung an die zuständigen CSIRTs weiter;

d) das CSIRT, das die Meldung zu der aktiv ausgenutzten Schwachstelle ursprünglich erhalten hat, wurde im Rahmen einer koordinierten Offenlegung von Schwachstellen, für die dieses CSIRT als vertrauenswürdiger Vermittler gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 fungiert, darauf aufmerksam gemacht; in einem solchen Fall leitet das CSIRT, das die Meldung ursprünglich erhalten hat, die Meldung im Einklang mit Artikel 16 Absatz 6 der Verordnung (EU) 2024/2847 an die zuständigen CSIRTs weiter, wenn ein Aufschub nicht mehr unbedingt erforderlich ist und die an der koordinierten Offenlegung von Schwachstellen beteiligten Parteien ihre Zustimmung zur Offenlegung erteilt haben.

Artikel 4

Modalitäten und Bedingungen für die Geltendmachung von Gründen im Zusammenhang mit der Cybersicherheit in Bezug auf ein bestimmtes CSIRT

Das CSIRT, das die Meldung ursprünglich erhalten hat, kann beschließen, die Verbreitung von Meldungen oder von Teilen davon an ein bestimmtes zuständiges CSIRT in den folgenden Fällen so lange aufzuschieben, wie unbedingt erforderlich:

a) das zuständige CSIRT ist von einem Cybersicherheitsvorfall betroffen, der Zweifel an seiner Fähigkeit zur Gewährleistung der Vertraulichkeit der gemeldeten Informationen aufkommen lässt;

b) es hat hinreichenden Grund zu der Annahme, dass die Fähigkeiten des zuständigen CSIRT nicht ausreichen, um die Vertraulichkeit der gemeldeten Informationen zu gewährleisten.

In den in Unterabsatz 1 Buchstabe a genannten Fällen kann das CSIRT, das die Meldung ursprünglich erhalten hat, die Verbreitung aufschieben, bis das zuständige CSIRT dem in Artikel 15 der Richtlinie 2022/2555 genannten CSIRTs-Netzwerk mitgeteilt hat, dass es die Vertraulichkeit der Meldungen wieder gewährleisten kann.

In den in Unterabsatz 1 Buchstabe b genannten Fällen kann das CSIRT, das die Meldung ursprünglich erhalten hat, die Verbreitung an das zuständige CSIRT so lange aufschieben, bis das CSIRT nachgewiesen hat, dass es die festgestellten Mängel behoben hat.

Artikel 5

Modalitäten und Bedingungen für die Geltendmachung von Gründen im Zusammenhang in Bezug auf die einheitliche Meldeplattform

Das CSIRT, das die Meldung ursprünglich erhalten hat, kann beschließen, die Verbreitung von Meldungen über die gemäß Artikel 16 der Verordnung (EU) 2024/2847 eingerichtete einheitliche Meldeplattform aufzuschieben, wenn die ENISA dem CSIRTs-Netzwerk gemäß Artikel 16 Absatz 4 der genannten Verordnung mitgeteilt hat, dass die einheitliche Meldeplattform von einem Cybersicherheitsvorfall betroffen ist, der Zweifel an ihrer Fähigkeit aufkommen lässt, die Vertraulichkeit der gemeldeten Informationen zu gewährleisten. In solchen Fällen kann das CSIRT, das die Meldung ursprünglich erhalten hat, die Verbreitung über die einheitliche Meldeplattform aufschieben, bis die ENISA dem CSIRTs-Netzwerk mitgeteilt hat, dass die Plattform die Vertraulichkeit der Meldungen wieder gewährleisten kann.

Artikel 6

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 11. Dezember 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN