

ANTWORTEN DER EUROPÄISCHEN KOMMISSION

AUF DEN SONDERBERICHT DES EUROPÄISCHEN RECHNUNGSHOFS

Erkennung und Bewältigung von Cybersicherheitsvorfällen:

Inhalt

I. DIE ANTWORTEN DER KOMMISSION ZUSAMMENGEFASST 2

II. ANTWORTEN AUF DIE EMPFEHLUNGEN 5

Empfehlung 1 – Informationsaustausch zwischen den Mitgliedstaaten stärken 5

Empfehlung 2 – Die EU-Kapazitäten zur Lageerfassung im Bereich der Cybersicherheit rationalisieren und die Verbreitung von Informationen optimieren 5

Empfehlung 3 – Das europäische Warnsystem für Cybersicherheit in die Cybersicherheitslandschaft der EU integrieren 7

Empfehlung 4 – Eine solide Bewertung der Eigentums- und Kontrollverhältnisse von Rechtsträgern, die EU-Mittel im Rahmen des Programms „Digitales Europa“ erhalten, gewährleisten 7

Empfehlung 5 – Den Leistungsüberwachungsrahmen der Cybersicherheitskomponente des Programms „Digitales Europa“ stärken 8

Dieses Dokument enthält die Antworten der Europäischen Kommission auf die Bemerkungen in einem Sonderbericht des Europäischen Rechnungshofes gemäß Artikel 265 der Haushaltsordnung, die zusammen mit dem Sonderbericht zu veröffentlichen sind.

I. DIE ANTWORTEN DER KOMMISSION ZUSAMMENGEFASST

Die Kommission begrüßt das anhaltende Interesse des Europäischen Rechnungshofs (EuRH) an der Cybersicherheit und, wie insbesondere aus diesem Sonderbericht hervorgeht, an der Erkennung von Cybersicherheitsvorfällen und der Reaktion darauf sowie an ihren Programmverwaltungsverfahren.

Die Kommission erinnert daran, dass der EU-Rahmen für erhebliche Sicherheitsvorfälle und Sicherheitsvorfälle großen Ausmaßes relativ neu ist und bislang auf einer Zusammenarbeit und einem Informationsaustausch zwischen den Einrichtungen der EU und den Mitgliedstaaten beruht, die weitgehend freiwillig sind, was Ausdruck des Gleichgewichts zwischen den Zuständigkeiten der EU und jenen der Mitgliedstaaten im Bereich der Sicherheit ist. Erst mit der Annahme der Richtlinie (EU) 2022/2555[1] wurden der Begriff „Sicherheitsvorfälle großen Ausmaßes“ im EU-Recht definiert und das EU-CyCLONe-Netz eingerichtet, um das koordinierte Management von Vorfällen großen Ausmaßes sowie von Krisen im Bereich der Cybersicherheit operativ zu unterstützen und den regelmäßigen Austausch einschlägiger Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU sicherzustellen. Dennoch hat dieser Rahmen, wie in dem Bericht festgestellt wird[2], angesichts der raschen Digitalisierung kritischer Infrastrukturen und der geopolitischen Volatilität, insbesondere angesichts einer eskalierenden Cyberbedrohungslage, immer mehr an Bedeutung gewonnen. In der im Juni 2025 angenommenen Empfehlung des Rates für einen EU-Konzeptentwurf für das Cyberkrisenmanagement (im Folgenden „Konzeptentwurf für Cybersicherheit“)[3] werden der Rahmen und die unterschiedlichen Aufgaben und Zuständigkeiten der verschiedenen Interessenträger beschrieben. Im Konzeptentwurf für Cybersicherheit werden Maßnahmen zur Verbesserung der praktischen Funktionsweise dieses Rahmens empfohlen, wie z. B. die Vereinbarung einer gemeinsamen abgestimmten Taxonomie von Schweregraden für Sicherheitsvorfälle und die nachdrückliche Aufforderung des Netzes der Computer-Notfallteams (CSIRTs) und EU-CyCLONe, wie in der Richtlinie (EU) 2022/2555 gefordert, unverzüglich verfahrenstechnische Vereinbarungen für den Fall eines potenziellen oder andauernden Cybersicherheitsvorfalls großen Ausmaßes zu vereinbaren. Die Kommission arbeitet nun mit anderen diesbezüglich relevanten Einrichtungen der EU und den Mitgliedstaaten an der Umsetzung der Empfehlung des Rates.

Die Mitgliedstaaten waren verpflichtet, die Richtlinie (EU) 2022/2555 bis Oktober 2024 umzusetzen, und die Kommission strengt weiterhin Vertragsverletzungsverfahren gegen Mitgliedstaaten an, die keine Maßnahmen zur Umsetzung der Richtlinie in nationales Recht mitgeteilt haben. Das Cybersolidaritätsgesetz wurde 2025 angenommen, und die mit ihm geschaffenen Instrumente wie die Cybersicherheitsreserve und Cyber-Hubs werden erst nach einiger Zeit voll funktionsfähig sein. Die Kommission erkennt an, dass die Rolle der Agentur der Europäischen Union für Cybersicherheit (ENISA) bei der Vorsorge und Reaktion auf Sicherheitsvorfälle großen Ausmaßes auf EU-Ebene gestärkt werden muss, indem der Agentur unter anderem die Aufgabe übertragen wird, Frühwarnungen auszusprechen und bei der Reaktion auf Sicherheitsvorfälle sowie deren Überprüfung unterstützend einzugreifen. Dies ist daher ein wichtiger Bestandteil des Vorschlags der Kommission zur Überarbeitung des Rechtsakts zur

[1] ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

[2] Sonderbericht, Absätze 01-05.

[3] ABl. C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj.

Cybersicherheit[4]. Aus diesem Grund ist es äußerst dringlich, dass die Mitgliedstaaten die bestehenden Vorschriften vollständig umsetzen und das Paket neuer Maßnahmen vom Parlament und vom Rat möglichst bald angenommen wird.

Die Kommission stimmt der Feststellung des EuRH[5], der sich auf die Berichterstattung der ENISA über die Bedrohungslage stützt, zu, wonach erhebliche Sicherheitsvorfälle, insbesondere solche mit grenzüberschreitendem Charakter, nach wie vor nicht ausreichend gemeldet werden und das Potenzial der EU-weiten Kooperationsmechanismen noch nicht voll ausgeschöpft wird. Gleichzeitig erinnert die Kommission daran, dass die Zusammenarbeit im Bereich der Cybersicherheit auf gegenseitigem Vertrauen beruht und nach den geltenden EU-Vorschriften keine Verpflichtung zum Informationsaustausch zwischen EU-Einrichtungen und Mitgliedstaaten besteht. Das CSIRT-Netz, das mit der ersten Richtlinie über die Sicherheit von Netz- und Informationssystemen[6] eingerichtet wurde, und EU-CyCLONe sollten beim Aufbau einer Kultur des Informationsaustauschs innerhalb der beiden Netze sowie zwischen ihnen bestärkt werden. Die nationale Sicherheit fällt jedoch weiterhin in die ausschließliche Zuständigkeit der einzelnen Mitgliedstaaten, die nicht verpflichtet werden können, Informationen zu übermitteln, deren Offenlegung ihren grundlegenden Interessen der nationalen und der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

Die Kommission stimmt zwar der Empfehlung 2 zu, „die EU-Kapazitäten zur Lageerfassung im Bereich der Cybersicherheit [zu] rationalisieren und die Verbreitung von Informationen [zu] optimieren“, weist jedoch darauf hin, dass es den Kontext zu berücksichtigen gilt: Wie im Konzeptentwurf für Cybersicherheit dargelegt, spielen verschiedene Interessenträger auf EU-Ebene unterschiedliche Rollen beim Management von erheblichen Sicherheitsvorfällen und Sicherheitsvorfällen großen Ausmaßes. Da der Kommission als Organ politische und operative Verantwortung für die Krisenvorsorge und -bewältigung, auch im Falle potenzieller und andauernder Cybersicherheitsvorfälle großen Ausmaßes, zufällt, hat sie innerhalb einer ihrer Dienststellen in die Entwicklung eines Cyber-Lagezentrums investiert, das von einem externen Dienstleister mit maßgeschneiderten Lösungen unterstützt wird, der für einen begrenzten Zeitraum unter Vertrag genommen wurde. Die Kommission räumt ein, dass weitere Synergien mit der ENISA und Effizienzsteigerungen der Agentur angestrebt werden müssen, betont jedoch, dass die Zuständigkeiten der einzelnen Kommissionsdienststellen sowie der Vertrag über die Erbringung externer Dienstleistungen für das Cyber-Lagezentrum getrennt voneinander zu betrachten sind. Es gibt keine Überschneidungen zwischen der Rolle der Kommission und der Rolle der ENISA, da beide Einrichtungen Aufgaben gemäß ihren jeweiligen Mandaten wahrnehmen[7]. Darüber hinaus sind Strukturen vorhanden, die im Falle eines erheblichen Sicherheitsvorfalls oder eines Sicherheitsvorfalls großen Ausmaßes den Informationsfluss zwischen den Kommissionsdienststellen und zwischen den einschlägigen EU-Einrichtungen, zu denen auch ENISA zählt, gewährleisten.

In Bezug auf die Cybersicherheitsreserve[8] erinnert die Kommission an das zugrunde liegende Ziel, allen Mitgliedstaaten, Organen, Einrichtungen und sonstigen Stellen der EU sowie bestimmten mit dem Programm „Digitales Europa“ assoziierten Drittländern bei erheblichen Cybersicherheitsvorfällen oder Cybersicherheitsvorfällen großen Ausmaßes rund um die Uhr ein Instrument zur Verfügung zu stellen. Die Kommission betont jedoch, dass es praktisch unmöglich ist, vorherzusagen, wie viele Cybersicherheitsvorfälle dieses Ausmaßes auftreten werden.

[4] COM(2026) 11 final.

[5] Sonderbericht, Absatz 35.

[6] ABl. L 194 vom 19.7.2016, S. 1, ELI: http://data.europa.eu/eli/dir/2016/1148/oj.

[7] Sonderbericht, „Erkennung und Bewältigung von Cybersicherheitsvorfällen“, Absätze 11 und 48.

[8] Sonderbericht, Absätze 52-61.

In Bezug auf das Europäische Kompetenzzentrum für Cybersicherheit[9] räumt die Kommission ein, dass die Einrichtung der Kompetenzgemeinschaft für Cybersicherheit und der strategischen Beratungsgruppe einige Zeit in Anspruch genommen hat. Es muss jedoch berücksichtigt werden, dass das Netzwerk nationaler Koordinierungszentren seitdem als Mittler und direkte Verbindung zu den Interessengruppen in den Mitgliedstaaten fungiert, um Informationen zusammenzutragen und Arbeitsprogramme auszuarbeiten.

Die Kommission nimmt alle Ergebnisse des Berichts gebührend zur Kenntnis und wird sie beim weiteren Vorgehen umfassend berücksichtigen.

[9] Siehe Bericht, Abschnitte 17 und 77-81.

II. ANTWORTEN AUF DIE EMPFEHLUNGEN

Empfehlung 1 – Informationsaustausch zwischen den Mitgliedstaaten stärken

Um die Erkennung von Cybersicherheitsvorfällen und die Reaktion darauf zu verbessern, sollte die Kommission mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA)

a) vorschlagen, dass die Kooperationsgruppe für Netz- und Informationssicherheit eine detaillierte Analyse der nationalen Sicherheitsbeschränkungen durchführt, die den Informationsaustausch einschränken und sich auf die Cyberresilienz der EU auswirken, sowie rechtliche und technische Lösungen ermittelt, um den Informationsaustausch unter Achtung der nationalen Sicherheit zu verbessern;

b) unbeschadet der Beschlüsse der beiden gesetzgebenden Organe in Zusammenarbeit mit den Mitgliedstaaten sicherstellen, dass die in der Digitalen-Omnibus-Verordnung vorgeschlagene zentrale Anlaufstelle zur Meldung von Vorfällen potenzielle grenzübergreifende Sicherheitsvorfälle erkennen kann;

c) Lösungen erarbeiten, die die Meldung von Sicherheitsvorfällen an die ENISA in Echtzeit ermöglichen.

(Zieldatum für die Umsetzung: a) und b) 2027, c) 2028)

Die Kommission **nimmt** die Empfehlung 1 (a, b und c) **an**.

Empfehlung 2 – Die EU-Kapazitäten zur Lageerfassung im Bereich der Cybersicherheit rationalisieren und die Verbreitung von Informationen optimieren

Um die Effizienz zu erhöhen, sollte die Kommission in Zusammenarbeit mit der ENISA bewerten, inwiefern Informationen zur Lageerfassung gemeinsam beschafft und analysiert werden können. Sie sollte diese Informationen und die damit verbundenen Berichte über Cyberbedrohungen außerdem allen einschlägigen Dienststellen und Agenturen der EU zur Verfügung stellen.

(Zieldatum für die Umsetzung: 2027)

Die Kommission **nimmt** die Empfehlung 2 **an**.

Die Kommission unterstützt diese Empfehlung. Sie steht im Einklang mit der Empfehlung des Rates für einen EU-Konzeptentwurf für das Cyberkrisenmanagement und mit dem Vorschlag der Kommission für eine Verordnung über einen EU-Rechtsakt zur Cybersicherheit, in dem vorgesehen ist, dass die einschlägigen Einrichtungen der EU, einschließlich der Kommission und der ENISA, zusammenarbeiten, um Ablagen mit Erkenntnissen über Cyberbedrohungen zu erstellen, und in dem anerkannt wird, dass eine weitere Straffung bei gleichzeitiger größtmöglicher Wirtschaftlichkeit der Haushaltsführung erforderlich ist.

Die Kommission nimmt diese Empfehlung unbeschadet der Bestimmungen und des Anwendungsbereichs der Verordnung (EU, Euratom) 2023/2841[10] und des unabhängigen Status des CERT-EU an, das in operativen Angelegenheiten weiterhin dem Interinstitutionellen Cybersicherheitsbeirat untersteht.

[10] ABl. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj.

Empfehlung 3 – Das europäische Warnsystem für Cybersicherheit in die Cybersicherheitslandschaft der EU integrieren

Die Kommission sollte gemeinsam mit der ENISA und den Mitgliedstaaten sicherstellen, dass Kooperationsvereinbarungen und Interoperabilitätsstandards bestehen, um den Informationsaustausch zwischen den grenzübergreifenden Hubs, die Teil des europäischen Warnsystems für Cybersicherheit sind, dem CSIRTs-Netzwerk und dem EU-CyCLONe, zu erleichtern.

(Zieldatum für die Umsetzung: 2028)

Die Kommission **nimmt** die Empfehlung 3 **an**.

Empfehlung 4 – Eine solide Bewertung der Eigentums- und Kontrollverhältnisse von Rechtsträgern, die EU-Mittel im Rahmen des Programms „Digitales Europa“ erhalten, gewährleisten

Das Europäische Kompetenzzentrum für Cybersicherheit sollte:

a) ***sollte hinreichende Sicherheit darüber erlangen, dass Begünstigte, die für die finanzielle Unterstützung Dritter verantwortlich sind, über die administrativen und technischen Kapazitäten verfügen, die erforderlich sind, um auf der Grundlage einer soliden Methodik angemessene Bewertungen der Eigentums- und Kontrollverhältnisse durchzuführen; außerdem***

b) ***sollte es stichprobenartige Überprüfungen vornehmen, um auszuschließen, dass nicht förderfähige Rechtsträger EU-Mittel erhalten.***

(Zieldatum für die Umsetzung: a) 2026, b) 2027)

Die Kommission stellt fest, dass sich die Empfehlung an das Europäische Kompetenzzentrum für Cybersicherheit richtet.

Empfehlung 5 – Den Leistungsüberwachungsrahmen der Cybersicherheitskomponente des Programms „Digitales Europa“ stärken

Um eine angemessene Überwachung von Fortschritt und Leistung zu ermöglichen, sollte das Europäische Kompetenzzentrum für Cybersicherheit

a) vor der Unterzeichnung der Finanzhilfevereinbarung sicherstellen, dass für alle Projekte Etappenziele, zu erbringende Leistungen und Leistungsindikatoren festgelegt wurden, die den Anweisungen im Antragsformular entsprechen;

b) ein robustes System zur Erhebung, Rückverfolgbarkeit, Überprüfung und Aggregation der Daten für die Leistungsindikatoren der Cybersicherheitskomponente des Programms „Digitales Europa“ konzipieren und einführen, um sicherzustellen, dass die Indikatoren die erzielten Ergebnisse genau widerspiegeln.

(Zieldatum für die Umsetzung: 2027)

Die Kommission stellt fest, dass sich die Empfehlung an das Europäische Kompetenzzentrum für Cybersicherheit richtet.