EUROPÄISCHE
KOMMISSION

Straßburg, den 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Diese Begründung ist dem Vorschlag für ein Cybersolidaritätsgesetz beigefügt. Die Nutzung und Abhängigkeit von Informations- und Kommunikationstechnologien sind von grundlegender Bedeutung in allen Wirtschaftssektoren, da öffentliche Verwaltungen, Unternehmen und Bürger stärker als je zuvor branchen- und grenzübergreifend miteinander vernetzt und voneinander abhängig sind. Durch die stärkere Verbreitung digitaler Technologien erhöht sich die Exposition gegenüber Cybersicherheitsvorfällen und ihre potenziellen Auswirkungen. Gleichzeitig sind die Mitgliedstaaten mit wachsenden Cybersicherheitsrisiken und einer insgesamt komplexen Bedrohungslage konfrontiert, wobei die eindeutige Gefahr besteht, dass Cybervorfälle rasch von einem Mitgliedstaat auf andere übergreifen.

Darüber hinaus werden Cyberoperationen zunehmend in hybride Strategien und in Kriegsführungsstrategien integriert, die sich erheblich auf das Angriffsziel auswirken. Insbesondere der militärischen Aggression Russlands gegen die Ukraine ging eine Strategie der feindseligen Cyberoperationen voraus, die auch weiterhin andauert, was die Wahrnehmung und Bewertung der kollektiven Vorsorge im Hinblick auf das Cyberkrisenmanagement grundlegend verändert hat und zu Forderungen nach Sofortmaßnahmen führte. Die Gefahr eines möglichen Vorfalls großen Ausmaßes, der erhebliche Störungen und Schäden an kritischen Infrastrukturen zur Folge hat, macht eine erhöhte Abwehrbereitschaft auf allen Ebenen des Cybersicherheitsökosystems der EU erforderlich. Diese Bedrohung geht über die militärische Aggression Russlands gegen die Ukraine hinaus und schließt anhaltende Cyberbedrohungen durch staatliche und nichtstaatliche Akteure ein, die angesichts der Vielzahl staatsnaher, krimineller und hacktivistischer Akteure, die an den derzeitigen geopolitischen Spannungen beteiligt sind, wahrscheinlich andauern werden. In den letzten Jahren hat die Zahl der Cyberangriffe dramatisch zugenommen, darunter Angriffe auf Lieferketten im Zusammenhang mit Cyberspionage, Ransomware oder Störungen. Im Jahr 2020 betraf der Angriff auf die Lieferkette von SolarWinds weltweit mehr als 18 000 Organisationen, darunter staatliche Stellen und große Unternehmen. Schwerwiegende Cybersicherheitsvorfälle können zu erheblich sein, als dass die von einem oder mehreren betroffenen Mitgliedstaaten allein bewältigt werden könnten. Aus diesem Grund ist eine verstärkte Solidarität auf Unionsebene erforderlich, um die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen zu verbessern.

Im Hinblick auf die Erkennung von Cyberbedrohungen und -vorfällen ist es dringend erforderlich, den Informationsaustausch zu intensivieren und unsere kollektiven Kapazitäten zu verbessern, sodass die für die Erkennung von Cyberbedrohungen benötigte Zeit drastisch verkürzt wird, bevor erhebliche Schäden und Kosten verursacht werden können[1]. Obwohl zahlreiche Cybersicherheitsbedrohungen und -vorfälle aufgrund der Vernetzung digitaler Infrastrukturen eine potenziell grenzübergreifende Dimension aufweisen, ist der Austausch

[1] Einem Bericht des Ponemon-Instituts und von IBM Security zufolge wurden Sicherheitsverletzungen im Jahr 2022 im Durchschnitt nach 207 Tagen festgestellt und nach weiteren 70 Tagen eingedämmt. Gleichzeitig beliefen sich die durchschnittlichen Kosten von Datenschutzverletzungen mit einem Lebenszyklus von mehr als 200 Tagen im Jahr 2022 auf 4,86 Mio. EUR gegenüber 3,74 Mio. EUR bei weniger als 200 Tagen. („Cost of a data breach 2022“, https://www.ibm.com/reports/data-breach).

relevanter Informationen zwischen den Mitgliedstaaten nach wie vor begrenzt. Der Aufbau eines Netzes grenzübergreifender Sicherheitseinsatzzentren (SOCs) zur Verbesserung der Erkennungs- und Reaktionsfähigkeiten soll zur Lösung dieses Problems beitragen.

Im Hinblick auf die Abwehrbereitschaft und Reaktion auf Cybersicherheitsvorfälle gibt es derzeit nur wenig Unterstützung auf Unionsebene und eine begrenzte Solidarität zwischen den Mitgliedstaaten. In den Schlussfolgerungen des Rates vom Oktober 2021 wurde hervorgehoben, dass diese Lücken angegangen werden müssen, und hierzu die Kommission aufgefordert, einen Vorschlag für einen neuen Cybersicherheits-Notfallfonds vorzulegen[2].

Mit dieser Verordnung wird auch die im Dezember 2020 angenommene EU-Cybersicherheitsstrategie[3] umgesetzt, in der die Schaffung eines europäischen Cyberschutzschilds angekündigt wurde, mit dem die Fähigkeiten zur Erkennung von Cyberbedrohungen und zum Informationsaustausch in der Europäischen Union durch einen Zusammenschluss nationaler und grenzübergreifender SOCs gestärkt werden sollen.

Diese Verordnung baut auf ersten Schritten auf, die bereits in enger Zusammenarbeit mit den wichtigsten Interessenträgern ausgearbeitet wurden und durch das Programm Digitales Europa unterstützt werden. Insbesondere in Bezug auf SOCs wurden im Rahmen des Arbeitsprogramms für Cybersicherheit 2021–2022 zum Programm Digitales Europa eine Aufforderung zur Interessenbekundung für die gemeinsame Beschaffung von Instrumenten und Infrastrukturen für die Einrichtung grenzübergreifender SOCs und eine Aufforderung zur Beantragung von Finanzhilfen für den Kapazitätsaufbau der SOCs im Dienste öffentlicher und privater Organisationen durchgeführt. Im Hinblick auf die Abwehrbereitschaft und die Bewältigung von Vorfällen hat die Kommission ein kurzfristiges Unterstützungsprogramm für die Mitgliedstaaten aufgestellt und der Agentur der Europäischen Union für Cybersicherheit (ENISA) zusätzliche Mittel zugewiesen, um die Abwehrbereitschaft und Reaktionsfähigkeit bei großen Cybersicherheitsvorfällen unverzüglich zu stärken. Beide Maßnahmen wurden in enger Abstimmung mit den Mitgliedstaaten vorbereitet. Diese Verordnung behebt bisherige Mängel und berücksichtigt Erkenntnisse aus diesen Maßnahmen.

Darüber hinaus wird mit diesem Vorschlag die Verpflichtung erfüllt, im Einklang mit der am 10. November angenommenen Gemeinsamen Mitteilung über die Cyberabwehr[4] einen Vorschlag für eine EU-Initiative zur Cybersolidarität mit folgenden Zielen auszuarbeiten: Stärkung der gemeinsamen Fähigkeiten der EU zur Erkennung, Lageerfassung und Reaktion, um schrittweise eine Cybersicherheitsreserve auf EU-Ebene mit Diensten vertrauenswürdiger privater Anbieter aufzubauen und die Prüfung kritischer Einrichtungen zu unterstützen.

Vor diesem Hintergrund schlägt die Kommission das vorliegende Cybersolidaritätsgesetz zur Stärkung der Solidarität auf Unionsebene vor, um die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen zu verbessern, und zwar durch die folgenden spezifischen Ziele:

---

2 Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union, die der Rat auf seiner Tagung vom 23. Mai 2022 gebilligt hat, Dok. 9364/22.

3 Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final.

4 Gemeinsame Mitteilung an das Europäische Parlament und den Rat – EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

- Stärkung der gemeinsamen Fähigkeiten der EU zur Erkennung und Lageerfassung im Bereich der Cyberbedrohungen und -vorfälle und damit Leistung eines Beitrags zur technologischen Souveränität Europas im Bereich der Cybersicherheit;
- Stärkung der Abwehrbereitschaft kritischer Einrichtungen in der gesamten EU und Stärkung der Solidarität durch den Aufbau gemeinsamer Kapazitäten für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, indem u. a. die Unterstützung für die Bewältigung auch Drittländern, die mit dem Programm Digitales Europa assoziiert sind, zur Verfügung gestellt wird;
- Stärkung der Abwehrfähigkeit der Union und Leistung eines Beitrags zu einer wirksamen Bewältigung durch die Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes, einschließlich der Gewinnung von Erkenntnissen und gegebenenfalls der Formulierung von Empfehlungen.

Diese Ziele werden durch die folgenden Maßnahmen umgesetzt:

- Aufbau einer europaweiten Infrastruktur von Sicherheitseinsatzzentren („europäischer Cyberschutzschild“), um gemeinsame Fähigkeiten zur Erkennung und Lageerfassung aufzubauen und zu verbessern;
- Schaffung eines Cybernotfallmechanismus zur Unterstützung der Mitgliedstaaten bei der Vorsorge für, Bewältigung von und sofortigen Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes. Auch die Organe, Einrichtungen und sonstigen Stellen der Union werden Unterstützung für die Bewältigung von Vorfällen erhalten;
- Einrichtung eines europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle zur Überprüfung und Bewertung von bestimmten schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes.

Der europäische Cyberschutzschild und der Cybernotfallmechanismus werden durch Mittel aus dem Programm Digitales Europa gefördert, das durch dieses Rechtsinstrument geändert wird, um die oben genannten Maßnahmen festzulegen, finanzielle Unterstützung für ihre Entwicklung bereitzustellen und die Bedingungen für die Inanspruchnahme der finanziellen Unterstützung zu präzisieren.

- **Kohärenz mit den bestehenden Vorschriften in diesem Politikbereich**

Der EU-Rahmen umfasst einige Rechtsakte, die auf Unionsebene vorgeschlagen wurden oder bereits in Kraft getreten sind, um die Resilienz kritischer Einrichtungen gegenüber Cybersicherheitsrisiken zu stärken und die koordinierte Bewältigung von Cybersicherheitsvorfällen und -krisen großen Ausmaßes zu unterstützen, darunter vor allem die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau von Netz- und Informationssystemen in der Union (NIS-2-Richtlinie)[5], der Rechtsakt zur

[5] 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).

Cybersicherheit[6], die Richtlinie über Angriffe auf Informationssysteme[7] und die Empfehlung (EU) 2017/1584 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen[8].

Die im Rahmen des Cybersolidaritätsgesetzes vorgeschlagenen Maßnahmen betreffen die Lageerfassung und den Informationsaustausch sowie die Unterstützung der Abwehrbereitschaft und Reaktionsfähigkeit bei Cybervorfällen. Diese Maßnahmen stehen im Einklang mit dem auf Unionsebene geltenden Rechtsrahmen, insbesondere gemäß der Richtlinie (EU) 2022/2555 (im Folgenden „NIS-2-Richtlinie"), und unterstützen dessen Ziele. Das Cybersolidaritätsgesetz wird insbesondere auf den bestehenden Rahmen für die operative Zusammenarbeit und das Krisenmanagement im Bereich der Cybersicherheit aufbauen und diese unterstützen, vor allem das europäische Netz der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) und das Netz der Computer-Notfallteams (CSIRTs).

Die grenzübergreifenden SOCs-Plattformen sollten eine neue Kapazität bilden, die das CSIRTs-Netz ergänzt, indem sie Daten über Bedrohungen der Cybersicherheit von öffentlichen und privaten Einrichtungen zusammenführen und weitergeben, den Wert solcher Daten durch Expertenanalysen und modernste Instrumente steigern und zur Entwicklung der Fähigkeiten und der technologischen Souveränität der Union beitragen.

Dieser Vorschlag steht ebenfalls mit der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur[9] im Einklang, in der die Mitgliedstaaten aufgefordert werden, sofortige wirksame Maßnahmen zu ergreifen und loyal, effizient, solidarisch und in koordinierter Weise mit der Kommission und anderen einschlägigen Behörden sowie den betreffenden Einrichtungen zusammenzuarbeiten, um die Resilienz kritischer Infrastrukturen, die für die Erbringung wesentlicher Dienste im Binnenmarkt genutzt werden, zu erhöhen.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Der Vorschlag steht im Einklang mit anderen Krisennotfallmechanismen und -protokollen wie der Integrierten Regelung für die politische Reaktion auf Krisen (IPCR). Das Cybersolidaritätsgesetz wird diese Rahmen und Protokolle für das Krisenmanagement durch die Bereitstellung einer gezielten Unterstützung für die Abwehrbereitschaft und Reaktion auf Cybersicherheitsvorfälle ergänzen. Der Vorschlag steht auch im Einklang mit dem auswärtigen Handeln der EU als Reaktion auf Vorfälle großen Ausmaßes im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP), unter anderem auch durch das EU-Instrumentarium für die Cyberdiplomatie. Der Vorschlag ergänzt Maßnahmen, die im Zusammenhang mit Artikel 42 Absatz 7 des Vertrags über die Europäische Union oder in den in Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union genannten Situationen durchgeführt werden.

---

6 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

7 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates.

8 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.

9 Empfehlung des Rates vom 8. Dezember 2022 für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur (ABl. C 20 vom 20.1.2023, S. 1).

Er ergänzt ferner das Katastrophenschutzverfahren der Union (UCPM)[10], das im Dezember 2013 eingerichtet und durch einen im Mai 2021 angenommenen neuen Rechtsakt[11] ergänzt wurde, mit dem die Säulen Prävention, Vorsorge und Bewältigung des Katastrophenschutzverfahrens der Union gestärkt, und der EU zusätzliche Kapazitäten für die Reaktion auf neue Risiken in Europa und der Welt an die Hand gegeben werden sowie die rescEU-Reserve aufgestockt wird.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Die Rechtsgrundlage dieses Vorschlags sind Artikel 173 Absatz 3 und Artikel 322 Absatz 1 Buchstabe a des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Artikel 173 AEUV sieht vor, dass die Union und die Mitgliedstaaten dafür sorgen, dass die notwendigen Voraussetzungen für die Wettbewerbsfähigkeit der Industrie der Union gewährleistet sind. Diese Verordnung zielt darauf ab, die Wettbewerbsposition der Industrie- und Dienstleistungssektoren in Europa in der gesamten digitalisierten Wirtschaft zu stärken und ihren digitalen Wandel voranzutreiben, indem das Cybersicherheitsniveau im digitalen Binnenmarkt erhöht wird. Sie zielt insbesondere darauf ab, die Widerstandsfähigkeit von Bürgerinnen und Bürgern, Unternehmen und in kritischen und hochkritischen Sektoren tätigen Einrichtungen gegenüber den zunehmenden Bedrohungen der Cybersicherheit zu erhöhen, die verheerende gesellschaftliche und wirtschaftliche Auswirkungen haben können.

Der Vorschlag stützt sich auch auf Artikel 322 Absatz 1 Buchstabe a AEUV, da er besondere Übertragungsregeln enthält, die von dem in der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates[12] (im Folgenden „Haushaltsordnung“) verankerten Grundsatz der Jährlichkeit abweichen. Im Interesse der wirtschaftlichen Haushaltsführung und angesichts des unvorhersehbaren, außergewöhnlichen und besonderen Charakters der Cybersicherheitslandschaft und der Cyberbedrohungen sollte dem Cybernotfallmechanismus ein gewisses Maß an Flexibilität bei der Haushaltsführung eingeräumt werden, insbesondere indem die automatische Übertragung nicht in Anspruch genommener Mittel für Verpflichtungen und Zahlungen für Maßnahmen zur Verfolgung der in der Verordnung festgelegten Ziele auf das folgende Haushaltsjahr ermöglicht wird. Da diese neue Regelung Fragen im Zusammenhang mit der Haushaltsordnung aufwirft, könnte diese Frage im Rahmen der laufenden Verhandlungen über die Neufassung der Haushaltsordnung behandelt werden.

• Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Aufgrund des ausgeprägten grenzübergreifenden Charakters von Cybersicherheitsbedrohungen und der zunehmenden Zahl der Risiken und Sicherheitsvorfälle, die sich über Grenzen, Sektoren und Produkte hinweg auswirken, können die Ziele der vorliegenden Maßnahme von den Mitgliedstaaten allein nicht wirksam erreicht werden und erfordern ein gemeinsames Vorgehen und Solidarität auf Unionsebene.

Die Erfahrungen mit der Abwehr von Cyberbedrohungen, die sich aus dem Krieg gegen die Ukraine ergeben, sowie die Lehren aus einer unter französischem Ratsvorsitz durchgeführten

---

10 Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union (Text von Bedeutung für den EWR).

11 Verordnung (EU) 2021/836 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Änderung des Beschlusses Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union (Text von Bedeutung für den EWR).

12 Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union (ABl. L 193 vom 30.7.2018, S. 1).

Cybersicherheitsübung (EU-CyCLES) haben gezeigt, dass konkrete Mechanismen zur gegenseitigen Unterstützung, insbesondere für die Zusammenarbeit mit dem Privatsektor, entwickelt werden sollten, um Solidarität auf EU-Ebene zu erreichen. Vor diesem Hintergrund wurde die Kommission in den Schlussfolgerungen des Rates vom 23. Mai 2022 zur Entwicklung der Cyberabwehr der Europäischen Union aufgefordert, einen Vorschlag für einen neuen Cybersicherheits-Notfallfonds vorzulegen.

Unterstützung und Maßnahmen zur besseren Erkennung von Cybersicherheitsbedrohungen auf Unionsebene und zur Erhöhung der Abwehrbereitschaft und Reaktionskapazitäten stellen einen Mehrwert dar, da so Doppelarbeit in der gesamten Union und in den Mitgliedstaaten vermieden werden kann. Dies würde zu einer besseren Verwendung der vorhandenen Ressourcen, einer besseren Koordinierung und einem besseren Informationsaustausch über gewonnene Erkenntnisse führen. Der Cybernotfallmechanismus sieht auch eine Unterstützung der mit dem Programm Digitales Europa assoziierten Drittländer aus der EU-Cybersicherheitsreserve vor.

Die Unterstützung im Rahmen der verschiedenen Initiativen, die auf Unionsebene eingerichtet und finanziert werden sollen, wird die nationalen Fähigkeiten in den Bereichen Erkennung, Lageerfassung, Abwehrbereitschaft und Reaktion auf Cyberbedrohungen und -vorfälle ergänzen, aber nicht reproduzieren.

- **Verhältnismäßigkeit**

Die Maßnahmen gehen nicht über das zur Erreichung der allgemeinen und spezifischen Ziele der Verordnung erforderliche Maß hinaus. Die Maßnahmen dieser Verordnung lassen die Zuständigkeiten der Mitgliedstaaten für die nationale Sicherheit, die öffentliche Sicherheit sowie die Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten unberührt. Sie berühren auch nicht die rechtlichen Verpflichtungen von in kritischen und hochkritischen Sektoren tätigen Einrichtungen, Maßnahmen im Bereich der Cybersicherheit im Einklang mit der NIS-2-Richtlinie zu ergreifen.

Die unter diese Verordnung fallenden Maßnahmen ergänzen diese Bemühungen und Maßnahmen, indem sie die Schaffung von Infrastrukturen für eine bessere Erkennung und Analyse von Bedrohungen und die Unterstützung von Vorsorge- und Bewältigungsmaßnahmen im Hinblick auf schwerwiegende Vorfälle oder Vorfällen großen Ausmaßes fördern.

- **Wahl des Instruments**

Bei dem vorgeschlagenen Rechtsakt handelt es sich um eine Verordnung des Europäischen Parlaments und des Rates. Dies ist das am besten geeignete Rechtsinstrument, da nur eine Verordnung mit ihren unmittelbar anwendbaren Rechtsvorschriften das erforderliche Maß an Einheitlichkeit für die Einrichtung und den Betrieb eines europäischen Cyberschutzschilds und eines Cybernotfallmechanismus bieten kann, indem darin die Unterstützung aus dem Programm Digitales Europa für deren Einrichtung sowie klare Bedingungen für die Verwendung und Zuweisung dieser Unterstützung vorgesehen werden.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Konsultation der Interessenträger**

Die Maßnahmen dieser Verordnung werden durch das Programm Digitales Europa unterstützt, das Gegenstand einer umfassenden Konsultation war. Darüber hinaus werden sie auf ersten Schritten aufbauen, die in enger Zusammenarbeit mit den wichtigsten

Interessenträgern bereits vorbereitet wurden. In Bezug auf die SOCs hat die Kommission in enger Zusammenarbeit mit den Mitgliedstaaten im Rahmen des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) ein Konzeptpapier zur Entwicklung grenzübergreifender SOCs-Plattformen und eine Aufforderung zur Interessenbekundung ausgearbeitet. In diesem Zusammenhang wurde eine Erhebung über die Kapazitäten nationaler SOCs durchgeführt, und in der technischen Arbeitsgruppe des ECCC, der Vertreter der Mitgliedstaaten angehören, wurden gemeinsame Ansätze und technische Anforderungen erörtert. Darüber hinaus fand ein Austausch mit der Branche statt, insbesondere im Rahmen der von der ENISA und der Europäischen Cybersicherheitsorganisation (ECSO) eingesetzten Expertengruppe für SOCs.

Zweitens hat die Kommission im Hinblick auf die Abwehrbereitschaft und die Bewältigung von Vorfällen ein kurzfristiges Unterstützungsprogramm für die Mitgliedstaaten aufgestellt und der ENISA zusätzliche Mittel aus dem Programm Digitales Europa zugewiesen, um die Abwehrbereitschaft und Reaktionsfähigkeit bei großen Cybersicherheitsvorfällen unverzüglich zu stärken. Die Rückmeldungen der Mitgliedstaaten und der Branche, die während der Durchführung dieses kurzfristigen Programms gesammelt wurden, liefern bereits wertvolle Erkenntnisse, die in die Ausarbeitung der vorgeschlagenen Verordnung zur Behebung der festgestellten Mängel eingeflossen sind. Dies war ein erster Schritt entsprechend den Schlussfolgerungen des Rates zur Cyberabwehr, in denen die Kommission aufgefordert wurde, einen Vorschlag für einen Notfallfonds für Cybersicherheit vorzulegen.

Darüber hinaus fand am 16. Februar 2023 ein Workshop mit Sachverständigen der Mitgliedstaaten zum Cybernotfallmechanismus auf der Grundlage eines Diskussionspapiers statt. Alle Mitgliedstaaten nahmen an diesem Workshop teil, und elf Mitgliedstaaten reichten schriftlich weitere Beiträge ein.

- **Folgenabschätzung**

Aufgrund der Dringlichkeit des Vorschlags wurde keine Folgenabschätzung durchgeführt. Die Maßnahmen dieser Verordnung werden durch das Programm Digitales Europa (DEP) unterstützt und stehen im Einklang mit den Maßnahmen der DEP-Verordnung, die einer speziellen Folgenabschätzung unterzogen wurde. Die vorliegende Verordnung wird keine erheblichen administrativen oder ökologischen Auswirkungen haben, die über diejenigen hinausgehen, die bereits in der Folgenabschätzung der Verordnung für das Programm Digitales Europa bewertet wurden.

Darüber hinaus baut sie auf ersten Maßnahmen auf, die – wie bereits dargelegt – in enger Zusammenarbeit mit den wichtigsten Interessenträgern entwickelt wurden, und entspricht der Forderung der Mitgliedstaaten, dass die Kommission bis Ende des dritten Quartals 2022 einen Vorschlag für einen neuen Cybersicherheits-Notfallfonds vorlegen sollte.

Insbesondere in Bezug auf die Lageerfassung und Erkennung unter dem europäischen Cyberschutzschild wurden im Rahmen des Arbeitsprogramms für Cybersicherheit 2021–2022 zum Programm Digitales Europa eine Aufforderung zur Interessenbekundung für die gemeinsame Beschaffung von Instrumenten und Infrastrukturen für die Einrichtung grenzübergreifender SOCs und eine Aufforderung zur Beantragung von Finanzhilfen für den Kapazitätsaufbau der SOCs im Dienste öffentlicher und privater Organisationen durchgeführt.

Im Bereich der Abwehrbereitschaft und der Bewältigung von Vorfällen hat die Kommission, wie bereits erwähnt, ein kurzfristiges Programm zur Unterstützung der Mitgliedstaaten im Rahmen des Programms Digitales Europa aufgestellt, das von der ENISA umgesetzt wird. Die Unterstützungsdienste im Rahmen des Programms umfassen Vorsorgemaßnahmen, wie Penetrationstests kritischer Einrichtungen zur Ermittlung von Schwachstellen. Außerdem

sieht das Programm zusätzliche Möglichkeiten vor, um Mitgliedstaaten im Falle eines schwerwiegenden Sicherheitsvorfalls bei einer kritischen Einrichtung zu unterstützen. Die Umsetzung dieses kurzfristigen Programms durch die ENISA ist im Gange und hat bereits einschlägige Erkenntnisse hervorgebracht, die bei der Ausarbeitung dieser Verordnung berücksichtigt wurden.

- **Grundrechte**

Durch seinen Beitrag zur Sicherheit digitaler Informationen wird dieser Vorschlag den Schutz des Rechts auf Freiheit und Sicherheit gemäß Artikel 6 der Charta der Grundrechte der Europäischen Union und des Rechts auf Achtung des Privat- und Familienlebens gemäß Artikel 7 der Charta der Grundrechte der Europäischen Union unterstützen. Indem Unternehmen vor wirtschaftlich schädlichen Cyberangriffen geschützt werden, wird der Vorschlag einen Beitrag zur Gewährleistung des Rechts auf unternehmerische Freiheit gemäß Artikel 16 der Charta der Grundrechte der Europäischen Union und des Eigentumsrechts gemäß Artikel 17 der Charta der Grundrechte der Europäischen Union leisten. Schließlich wird der Vorschlag durch den Schutz der Integrität kritischer Infrastrukturen vor Cyberangriffen zur Wahrung des Rechts auf Gesundheitsschutz gemäß Artikel 35 der Charta der Grundrechte der Europäischen Union und des Rechts auf Zugang zu Dienstleistungen von allgemeinem wirtschaftlichem Interesse gemäß Artikel 36 der Charta der Grundrechte der Europäischen Union beitragen.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die Maßnahmen dieser Verordnung werden im Rahmen des strategischen Ziels „Cybersicherheit“ des Programms Digitales Europa unterstützt.

Die Gesamtmittelausstattung enthält eine Aufstockung um 100 Mio. EUR, indem – wie in dieser Verordnung vorgeschlagen – Mittel aus anderen strategischen Zielen des Programms Digitales Europa umgeschichtet werden. Damit erhöht sich der neue Gesamtbetrag, der für Cybersicherheitsmaßnahmen im Rahmen des Programms Digitales Europa zur Verfügung steht, auf 842,8 Mio. EUR.

Ein Teil der zusätzlichen 100 Mio. EUR wird in das vom ECCC verwaltete Budget für die Durchführung von Maßnahmen in Bezug auf SOCs und auf die Abwehrbereitschaft im Rahmen des bzw. der Arbeitsprogramme einfließen. Darüber hinaus werden die zusätzlichen Mittel dazu dienen, die Einrichtung der EU-Cybersicherheitsreserve zu unterstützen.

Sie ergänzen die bereits für ähnliche Maßnahmen im Arbeitsprogramme für das Hauptprogramm Digitales Europa und das strategische Ziel „Cybersicherheit“ für den Zeitraum 2023–2027 vorgesehenen Mittel, wodurch sich der Gesamtbetrag für den Zeitraum 2023–2027 auf 551 Mio. EUR erhöhen könnte, während 115 Mio. EUR bereits für Pilotprojekte im Zeitraum 2021–2022 eingesetzt wurden. Einschließlich der Beiträge der Mitgliedstaaten könnte sich das Gesamtbudget auf bis zu 1,109 Mrd. EUR belaufen.

Ein Überblick über die anfallenden Kosten ist dem diesem Vorschlag beigefügten Finanzbogen zu entnehmen.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Die Kommission wird die Durchführung, Anwendung und Einhaltung dieser neuen Bestimmungen überwachen, um auch deren Wirksamkeit zu bewerten. Spätestens vier Jahre

nach dem Geltungsbeginn dieser Verordnung wird die Kommission dem Europäischen Parlament und dem Rat einen Bericht über ihre Bewertung und Überprüfung vorlegen.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Allgemeine Ziele, Gegenstand und Begriffsbestimmungen (Kapitel I)

In Kapitel I werden die Ziele der Verordnung in Bezug auf die Stärkung der Solidarität auf Unionsebene festgelegt, um die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen zu verbessern und insbesondere die gemeinsamen Fähigkeiten der Union zur Erkennung und Lageerfassung im Bereich der Cyberbedrohungen und -vorfälle, die Abwehrbereitschaft der in kritischen und hochkritischen Sektoren tätigen Einrichtungen in der gesamten Union und die Solidarität durch den Aufbau gemeinsamer Kapazitäten für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes sowie die Resilienz der Union durch die Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu stärken. In diesem Kapitel werden auch die Maßnahmen dargelegt, mit denen die folgenden Ziele erreicht werden sollen: Aufbau eines europäischen Cyberschutzschilds, Schaffung eines Cybernotfallmechanismus und Einrichtung eines Überprüfungsmechanismus für Cybersicherheitsvorfälle. Darüber hinaus enthält es die Begriffsbestimmungen, die in diesem Rechtsinstrument durchweg verwendet werden.

Der europäische Cyberschutzschild (Kapitel II)

In Kapitel II werden der europäische Cyberschutzschild und seine verschiedenen Elemente sowie die Bedingungen für die Beteiligung festgelegt. Erstens werden darin das übergeordnete Ziel des europäischen Cyberschutzschilds, nämlich die Entwicklung fortgeschrittener Fähigkeiten der Union zur Erkennung, Analyse und Verarbeitung von Daten über Cyberbedrohungen und -vorfälle in der Union, sowie die spezifischen operativen Ziele dargelegt. Demnach erfolgt die Finanzierung des europäischen Cyberschutzschilds durch die Union im Einklang mit der Verordnung für das Programm Digitales Europa.

Darüber hinaus wird in dem Kapitel die Art der Einrichtungen beschrieben, die den europäischen Cyberschutzschild bilden sollen. Der Schutzschild soll aus nationalen Sicherheitseinsatzzentren („nationalen SOCs“) und grenzübergreifenden Sicherheitseinsatzzentren („grenzgreifenden SOCs“) bestehen. Jeder beteiligte Mitgliedstaat benennt ein nationales SOC. Dieses fungiert als Bezugspunkt und Zugangstor zu anderen öffentlichen und privaten Organisationen auf nationaler Ebene für die Sammlung und Auswertung von Informationen über Cybersicherheitsbedrohungen und -vorfälle und trägt zu einem grenzübergreifenden SOC bei. Im Anschluss an eine Aufforderung zur Interessenbekundung kann das ECCC ein nationales SOC zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen mit dem ECCC und für den Erhalt einer Finanzhilfe für deren Betrieb auswählen. Erhält ein nationales SOC Unterstützung durch die Union, so verpflichtet es sich, sich innerhalb von zwei Jahren an einem grenzübergreifenden SOC zu beteiligen.

Grenzübergreifende SOCs bestehen aus einem Konsortium aus mindestens drei Mitgliedstaaten, vertreten durch nationale SOCs, die sich verpflichtet haben, bei der Koordinierung ihrer Tätigkeiten zur Erkennung und Überwachung von Cyberbedrohungen zusammenzuarbeiten. Im Anschluss an eine erste Aufforderung zur Interessenbekundung kann das ECCC ein Aufnahmekonsortium zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen mit dem ECCC und für den Erhalt einer Finanzhilfe für deren Betrieb auswählen. Die Mitglieder des Aufnahmekonsortiums schließen eine

schriftliche Konsortialvereinbarung, in der sie ihre internen Regelungen festlegen. Ferner werden in diesem Kapitel die Anforderungen an den Informationsaustausch zwischen den Teilnehmern eines grenzübergreifenden SOC und an den Informationsaustausch zwischen einem grenzübergreifenden SOC und anderen entsprechenden SOCs sowie mit einschlägigen EU-Einrichtungen dargelegt. Nationale SOCs, die sich an einem grenzübergreifenden SOC beteiligten, müssen untereinander einschlägige Informationen über Cyberbedrohungen austauschen, und die diesbezüglichen Einzelheiten, einschließlich der Verpflichtung zur Weitergabe einer erheblichen Menge an Daten und deren Bedingungen, sollten in einer Konsortialvereinbarung festgelegt werden. Grenzübergreifende SOCs sollen ein hohes Maß an Interoperabilität untereinander gewährleisten. Grenzübergreifende SOCs sollten außerdem Kooperationsvereinbarungen mit anderen grenzübergreifenden SOCs schließen, in denen die Grundsätze für den Informationsaustausch festgelegt werden. Wenn grenzübergreifende SOCs Informationen über einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, stellen sie dem europäischen Netz der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), dem CSIRTs-Netz und der Kommission im Hinblick auf ihre jeweiligen Krisenmanagementaufgaben gemäß der Richtlinie (EU) 2022/2555 alle einschlägigen Informationen zur Verfügung. Abschließend werden in Kapitel II die Sicherheitsbedingungen für die Beteiligung am europäischen Cyberschutzschild festgelegt.

Cybernotfallmechanismus (Kapitel III)

Mit Kapitel III wird der Cybernotfallmechanismus eingerichtet, um die Resilienz der Union gegenüber großen Cybersicherheitsbedrohungen zu verbessern, sie im Geiste der Solidarität auf die kurzfristigen Auswirkungen von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes vorzubereiten und diese Auswirkungen einzudämmen. Maßnahmen zur Umsetzung des Cybernotfallmechanismus werden aus Mitteln des Programms Digitales Europa finanziert. Der Mechanismus sieht Maßnahmen zur Unterstützung der Abwehrbereitschaft, einschließlich koordinierter Tests von in hochkritischen Sektoren tätigen Einrichtungen, sowie zur Reaktion und sofortigen Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes sowie gegenseitige Amtshilfe vor.

Die Vorsorgemaßnahmen im Rahmen des Cybernotfallmechanismus umfassen koordinierte Tests der Abwehrbereitschaft von in hochkritischen Sektoren tätigen Einrichtungen. Die Kommission sollte nach Konsultation der ENISA und der NIS-Kooperationsgruppe regelmäßig einschlägige Sektoren oder Teilsektoren aus den in Anhang I der Richtlinie (EU) 2022/2555 aufgeführten Sektoren mit hoher Kritikalität festlegen, aus denen Einrichtungen den koordinierten Tests der Abwehrbereitschaft auf EU-Ebene unterzogen werden können.

Für die Zwecke der Durchführung der vorgeschlagenen Maßnahmen zur Reaktion auf Sicherheitsvorfälle wird mit dieser Verordnung eine EU-Cybersicherheitsreserve eingerichtet, die aus Sicherheitsvorfall-Notdiensten vertrauenswürdiger Anbieter besteht, die nach den in dieser Verordnung festgelegten Kriterien ausgewählt werden. Zu den Nutzern der Dienste der EU-Cybersicherheitsreserve gehören die Behörden für das Cyberkrisenmanagement und die CSIRTs der Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der Union. Die Kommission trägt die Gesamtverantwortung für die Umsetzung der EU-Cybersicherheitsreserve und kann die ENISA ganz oder teilweise mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve betrauen.

Um Unterstützung aus der EU-Cybersicherheitsreserve zu erhalten, sollten die Nutzer ihre eigenen Maßnahmen zur Eindämmung der Auswirkungen des Sicherheitsvorfalls, für den die Unterstützung beantragt wird, ergreifen. Die Anträge auf Unterstützung aus der EU-

Cybersicherheitsreserve sollten die erforderlichen einschlägigen Informationen über den Sicherheitsvorfall und die von den Nutzern bereits ergriffenen Maßnahmen enthalten. In dem Kapitel werden auch die Durchführungsmodalitäten beschrieben, einschließlich der Bewertung von Anträgen auf Unterstützung aus der EU-Cybersicherheitsreserve.

Die Verordnung enthält auch die Grundsätze für die Beschaffung und die Auswahlkriterien für vertrauenswürdige Anbieter der EU-Cybersicherheitsreserve.

Drittländer können Unterstützung aus der EU-Cybersicherheitsreserve beantragen, wenn die Assoziierungsabkommen über ihre Teilnahme am Programm Digitales Europa dies vorsehen. In diesem Kapitel werden weitere Bedingungen und Modalitäten einer solchen Teilnahme beschrieben.

Überprüfungsmechanismus für Cybersicherheitsvorfälle (Kapitel IV)

Auf Ersuchen der Kommission, des EU-CyCLONe-Netzes oder des CSIRTs-Netzes sollte die ENISA Bedrohungen, Schwachstellen und Eindämmungsmaßnahmen im Zusammenhang mit einem bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes überprüfen und bewerten. Die Überprüfung und Bewertung sollte von der ENISA in Form eines Berichts über die Überprüfung von Sicherheitsvorfällen an das CSIRTs-Netz, das EU-CyCLONe-Netz und die Kommission übermittelt werden, um sie bei der Wahrnehmung ihrer Aufgaben zu unterstützen. Betrifft der Vorfall ein Drittland, so sollte die Kommission den Bericht auch an den Hohen Vertreter weitergeben. Der Bericht sollte die gewonnenen Erkenntnisse und gegebenenfalls Empfehlungen zur Verbesserung der Cyberabwehr in der Union enthalten.

Schlussbestimmungen (Kapitel V)

Kapitel V enthält Änderungen der Verordnung für das Programm Digitales Europa und verpflichtet die Kommission, regelmäßig Berichte zur Bewertung und Überprüfung der Verordnung für das Europäische Parlament und den Rat zu erstellen. Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte gemäß dem in Artikel 21 genannten Prüfverfahren zu erlassen, um die Bedingungen für die Interoperabilität zwischen grenzübergreifenden SOCs festzulegen; die Verfahrensmodalitäten für den Informationsaustausch im Zusammenhang mit einem potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes zwischen grenzübergreifenden SOCs und Einrichtungen der Union sowie technische Anforderungen zur Gewährleistung eines hohen Maßes an Datensicherheit und physischer Sicherheit der Infrastruktur und zum Schutz der Sicherheitsinteressen der Union beim Austausch von Informationen mit Einrichtungen, bei denen es sich nicht um öffentliche Stellen der Mitgliedstaaten handelt, festzulegen; die Art und die Anzahl der für die EU-Cybersicherheitsreserve erforderlichen Notdienste die genauen Modalitäten für die Zuweisung der Unterstützungsdienste der EU-Cybersicherheitsreserve zu präzisieren.

2023/0109 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 173 Absatz 3 und Artikel 322 Absatz 1 Buchstabe a,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Rechnungshofs[1],

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[2],

nach Stellungnahme des Ausschusses der Regionen[3],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Die Nutzung und Abhängigkeit von Informations- und Kommunikationstechnologien sind von grundlegender Bedeutung in allen Wirtschaftssektoren, da öffentliche Verwaltungen, Unternehmen und Bürger stärker als je zuvor branchen- und grenzübergreifend miteinander vernetzt und voneinander abhängig sind.

(2) Die Tragweite, die Häufigkeit und die Auswirkungen von Cybersicherheitsvorfällen nehmen zu, was auch Cyberangriffe im Zusammenhang mit Cyberspionage, Ransomware oder Störungen einschließt. Sie stellen eine große Bedrohung für das Funktionieren von Netz- und Informationssystemen dar. Angesichts der sich wandelnden Bedrohungslandschaft ist wegen der Gefahr von Vorfällen großen Ausmaßes, die erhebliche Störungen oder Schäden an kritischen Infrastrukturen verursachen, eine erhöhte Abwehrbereitschaft auf allen Ebenen des Cybersicherheitsrahmens der Union erforderlich. Diese Bedrohung geht über die militärische Aggression Russlands gegen die Ukraine hinaus und wird angesichts der Vielzahl staatsnaher, krimineller und hacktivistischer Akteure, die an den derzeitigen geopolitischen Spannungen beteiligt sind, wahrscheinlich andauern. Solche Vorfälle können – auch in kritischen oder hochkritischen Sektoren – die Erbringung öffentlicher Dienstleistungen und die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, erhebliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft der Union schweren Schaden zufügen und sogar gesundheitliche oder lebensbedrohliche Folgen haben. Darüber hinaus sind

[1] ABl. C […] vom […], S. […].
[2] ABl. C … vom …, S. ….
[3] ABl. C … vom …, S. ….

Cybersicherheitsvorfälle unvorhersehbar, da sie oft innerhalb sehr kurzer Zeiträume auftreten und sich fortentwickeln, nicht auf ein bestimmtes geografisches Gebiet beschränkt sind, sondern sich gleichzeitig in vielen Ländern ereignen oder sich rasch in andere Länder ausbreiten können.

(3) Es ist notwendig, die Wettbewerbsposition der Industrie- und Dienstleistungssektoren in der Union in der gesamten digitalisierten Wirtschaft zu stärken und ihren digitalen Wandel zu unterstützen, indem das Cybersicherheitsniveau im digitalen Binnenmarkt erhöht wird. Wie in drei verschiedenen Vorschlägen der Konferenz zur Zukunft Europas[4] empfohlen, muss die Resilienz der Bürgerinnen und Bürger und der Unternehmen und Einrichtungen, die kritische Infrastrukturen betreiben, gegenüber den zunehmenden Cybersicherheitsbedrohungen, die verheerende gesellschaftliche und wirtschaftliche Auswirkungen haben können, erhöht werden. Daher sind Investitionen in Infrastrukturen und Dienste erforderlich, die eine schnellere Erkennung von Cybersicherheitsbedrohungen und -vorfällen und eine schnellere Reaktion darauf unterstützen, und die Mitgliedstaaten benötigen Unterstützung zur Verbesserung der Vorsorgemaßnahmen und der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes. Auch die Union sollte ihre Kapazitäten in diesen Bereichen ausbauen, insbesondere in Bezug auf die Erhebung und Analyse von Daten über Cybersicherheitsbedrohungen und -vorfälle.

(4) Die Union hat bereits eine Reihe von Rechtsakten erlassen, um Sicherheitslücken zu verringern und die Resilienz kritischer Infrastrukturen und Einrichtungen gegenüber Cybersicherheitsrisiken zu erhöhen, darunter insbesondere die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[5], die Empfehlung (EU) 2017/1584 der Kommission[6], die Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates[7] und die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[8]. Ferner wurden die Mitgliedstaaten in der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur aufgefordert, unverzüglich wirksame Maßnahmen zu ergreifen und loyal, effizient, solidarisch und in koordinierter Weise mit der Kommission und anderen einschlägigen Behörden sowie den betreffenden Einrichtungen zusammenzuarbeiten, um die Resilienz kritischer Infrastrukturen, die für die Erbringung wesentlicher Dienste im Binnenmarkt genutzt werden, zu erhöhen.

(5) Die zunehmenden Cybersicherheitsrisiken und eine insgesamt komplexe Bedrohungslandschaft mit der eindeutigen Gefahr einer raschen Ausbreitung von Cybervorfällen von einem Mitgliedstaat auf einen anderen sowie von Drittländern in

---

4 https://futureu.europa.eu/de/

5 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 (ABl. L 333 vom 27.12.2022, S. 80).

6 Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

7 Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8).

8 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

die Union erfordern eine verstärkte Solidarität auf Unionsebene, um die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen zu verbessern. Die Mitgliedstaaten haben die Kommission ferner in den Schlussfolgerungen des Rates zur Cyberabwehr der EU[9] aufgefordert, einen Vorschlag für einen neuen Notfallfonds für Cybersicherheit vorzulegen.

(6) In der am 10. November 2022 angenommenen Gemeinsamen Mitteilung über die EU-Cyberabwehrpolitik[10] wurde eine EU-Initiative zur Cybersolidarität mit folgenden Zielen angekündigt: Stärkung der gemeinsamen Fähigkeiten der EU zur Erkennung, Lageerfassung und Bewältigung durch Förderung des Aufbaus einer EU-Infrastruktur von Sicherheitseinsatzzentren (SOCs), Unterstützung des schrittweisen Aufbaus einer Cybersicherheitsreserve auf EU-Ebene mit Diensten vertrauenswürdiger privater Anbieter und Prüfung von kritischen Einrichtungen auf potenzielle Schwachstellen auf der Grundlage von EU-Risikobewertungen.

(7) Es ist notwendig, in der gesamten Union sowohl die Erkennung und Lageerfassung im Bereich der Cyberbedrohungen und -vorfälle als auch die Solidarität zu stärken, indem die Abwehrbereitschaft und die Fähigkeiten der Mitgliedstaaten und der Union zur Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes verbessert werden. Daher sollte eine europaweite Infrastruktur von Sicherheitseinsatzzentren („europäischer Cyberschutzschild“) aufgebaut werden, um gemeinsame Fähigkeiten zur Erkennung und Lageerfassung aufzubauen und zu verbessern; ein Cybernotfallmechanismus sollte eingerichtet werden, um die Mitgliedstaaten bei der Vorsorge für, der Bewältigung von und der sofortigen Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu unterstützen; ferner sollte ein Überprüfungsmechanismus für Cybersicherheitsvorfälle eingerichtet werden, um bestimmte schwerwiegende Cybersicherheitsvorfälle bzw. Cybersicherheitsvorfälle großen Ausmaßes zu überprüfen und zu bewerten. Diese Maßnahmen lassen Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unberührt.

(8) Um diese Ziele zu erreichen, ist es auch erforderlich, die Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates[11] in bestimmten Bereichen zu ändern. Insbesondere sollte mit dieser Verordnung die Verordnung (EU) 2021/694 geändert werden, um im Rahmen des spezifischen Ziels 3 des Programms Digitales Europa, das darauf abzielt, die Widerstandsfähigkeit, Integrität und Vertrauenswürdigkeit des digitalen Binnenmarkts zu gewährleisten, die Kapazitäten zur Überwachung von Cyberangriffen und -bedrohungen zu stärken und darauf zu reagieren, die grenzüberschreitende Zusammenarbeit im Bereich der Cybersicherheit zu verbessern und neue operative Ziele im Zusammenhang mit dem europäischen Cyberschutzschild und dem Cybernotfallmechanismus hinzuzufügen. Dies wird durch die spezifischen Bedingungen ergänzt werden, unter denen für diese Maßnahmen finanzielle Unterstützung gewährt werden kann, sowie durch die Steuerungs- und

---

9 Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union, die der Rat auf seiner Tagung vom 23. Mai 2022 gebilligt hat, Dok. 9364/22.

10 Gemeinsame Mitteilung an das Europäische Parlament und den Rat – EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

11 Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Aufstellung des Programms „Digitales Europa“ und zur Aufhebung des Beschlusses (EU) 2015/2240 (ABl. L 166 vom 11.5.2021, S. 1).

Koordinierungsmechanismen, die erforderlich sind, um die angestrebten Ziele zu erreichen. Weitere Änderungen der Verordnung (EU) 2021/694 sollten Beschreibungen der im Rahmen der neuen operativen Ziele vorgeschlagenen Maßnahmen sowie messbare Indikatoren zur Überwachung der Umsetzung dieser neuen operativen Ziele enthalten.

(9) Die Finanzierung von Maßnahmen im Rahmen dieser Verordnung sollte in der Verordnung (EU) 2021/694 vorgesehen werden, die weiterhin der einschlägige Basisrechtsakt für diese im spezifischen Ziel 3 des Programms Digitales Europa verankerten Maßnahmen bleiben sollte. Die besonderen Teilnahmebedingungen für die einzelnen Maßnahmen werden im Einklang mit der geltenden Bestimmung der Verordnung (EU) 2021/694 in den einschlägigen Arbeitsprogrammen festgelegt.

(10) Auf diese Verordnung finden die vom Europäischen Parlament und dem Rat gemäß Artikel 322 AEUV erlassenen horizontalen Haushaltsvorschriften Anwendung. Diese Vorschriften sind in der Haushaltsordnung festgelegt und regeln insbesondere das Verfahren für die Aufstellung und Ausführung des Haushaltsplans der Union sowie die Kontrolle der Verantwortung der Finanzakteure. Die auf der Grundlage des Artikels 322 AEUV erlassenen Vorschriften erstrecken sich auch auf die allgemeine Konditionalitätsregelung zum Schutz des Haushalts der Union, wie sie in der Verordnung (EU, Euratom) 2020/2092 des Europäischen Parlaments und des Rates festgelegt ist.

(11) Um eine wirtschaftliche Haushaltsführung zu gewährleisten, sollten spezifische Vorschriften für die Übertragung nicht in Anspruch genommener Verpflichtungs- und Zahlungsermächtigungen festgelegt werden. Unter Wahrung des Grundsatzes der Jährlichkeit des Unionshaushalts sollten in dieser Verordnung angesichts des unvorhersehbaren, außergewöhnlichen und besonderen Charakters der Cybersicherheitslandschaft über die in der Haushaltsordnung festgelegten Möglichkeiten hinaus weitere Möglichkeiten vorgesehen werden, nicht verwendete Mittel zu übertragen und so die Fähigkeit des Cybernotfallmechanismus zur Unterstützung der Mitgliedstaaten bei der wirksamen Abwehr von Cyberbedrohungen zu maximieren.

(12) Um Cyberbedrohungen und -vorfälle wirksamer zu verhüten, zu bewerten und zu bewältigen, ist es notwendig, umfassendere Kenntnisse über die bestehenden Bedrohungen für kritische Anlagen und Infrastrukturen im Gebiet der Union zu erlangen, einschließlich ihrer geografischen Verteilung, ihres Zusammenwirkens und ihrer potenziellen Auswirkungen im Falle von Cyberangriffen, die diese Infrastrukturen betreffen. Es sollte eine große Unionsinfrastruktur für SOCs (im Folgenden „europäischer Cyberschutzschild“) eingerichtet werden, die aus mehreren interoperativen grenzübergreifenden Plattformen besteht, die jeweils mehrere nationale SOCs zusammenführen. Diese Infrastruktur sollte den Interessen und Bedürfnissen der Mitgliedstaaten und der Union im Bereich der Cybersicherheit dienen, indem sie den neuesten Stand der Technik für fortgeschrittene Instrumente der Datenerhebung und -analyse nutzt, die Fähigkeiten zur Erkennung und Bewältigung von Cyberangriffen verbessert und eine Echtzeit-Lageerfassung ermöglicht. Sie sollte auch dazu dienen, die Erkennung von Cybersicherheitsbedrohungen und -vorfällen zu verbessern und somit die für das Krisenmanagement in der Union zuständigen Einrichtungen und Netze der Union, insbesondere das EU-Netz der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) im Sinne der Richtlinie

(EU) 2022/2555 des Europäischen Parlaments und des Rates[12], zu ergänzen und zu unterstützen.

(13) Jeder Mitgliedstaat sollte auf nationaler Ebene eine öffentliche Stelle benennen, die mit der Koordinierung von Tätigkeiten zur Erkennung von Cyberbedrohungen in diesem Mitgliedstaat betraut ist. Diese nationalen SOCs sollten auf nationaler Ebene als Bezugspunkt und Zugangstor für die Beteiligung am Europäischen Cyberschutzschild fungieren und sicherstellen, dass Informationen über Cyberbedrohungen von öffentlichen und privaten Einrichtungen auf nationaler Ebene wirksam und effizient ausgetauscht und gesammelt werden.

(14) Im Rahmen des europäischen Cyberschutzschilds sollte eine Reihe grenzübergreifender Cybersicherheitseinsatzzentren („grenzübergreifende SOCs“) eingerichtet werden. Darin sollten sich nationale SOCs aus mindestens drei Mitgliedstaaten zusammenfinden, damit die Vorteile der grenzübergreifenden Erkennung von Bedrohungen sowie des Informationsaustauschs und -managements voll ausgeschöpft werden können. Das allgemeine Ziel grenzübergreifender SOCs sollte darin bestehen, die Kapazitäten zur Analyse, Verhütung und Erkennung von Cybersicherheitsbedrohungen zu stärken und die Gewinnung hochwertiger Erkenntnisse über Cybersicherheitsbedrohungen zu unterstützen, insbesondere durch den Austausch von Daten aus verschiedenen öffentlichen oder privaten Quellen sowie durch die Weitergabe und die gemeinsame Nutzung modernster Instrumente und die gemeinsame Entwicklung von Erkennungs-, Analyse- und Präventionsfähigkeiten in einem vertrauenswürdigen Umfeld. Sie sollten neue zusätzliche Kapazitäten bereitstellen, die auf bestehenden SOCs und Computer-Notfallteams (CSIRTs) und anderen einschlägigen Akteuren aufbauen und diese ergänzen.

(15) Auf nationaler Ebene wird die Überwachung, Erkennung und Analyse von Cyberbedrohungen in der Regel durch SOCs öffentlicher und privater Einrichtungen in Kombination mit CSIRTs sichergestellt. Darüber hinaus tauschen die CSIRTs im Rahmen des CSIRT-Netzes Informationen gemäß der Richtlinie (EU) 2022/2555 aus. Die grenzübergreifenden SOCs-Plattformen sollten eine neue Kapazität bilden, die das CSIRTs-Netz ergänzt, indem sie Daten über Bedrohungen der Cybersicherheit von öffentlichen und privaten Einrichtungen zusammenführen und weitergeben, den Wert solcher Daten durch Expertenanalysen, gemeinsam beschaffte Infrastrukturen und modernste Instrumente steigern und zur Entwicklung der Fähigkeiten und technologischen Souveränität der Union beitragen.

(16) Die grenzübergreifenden SOCs sollten als zentrale Stelle fungieren, die eine umfassende Zusammenführung einschlägiger Daten und Erkenntnisse über Cyberbedrohungen und die Verbreitung von Informationen über Bedrohungen in einer großen und vielfältigen Gruppe von Akteuren ermöglicht (z. B. Soforteinsatzteams für IT-Sicherheitsvorfälle (CERTs), CSIRTs, Informationsaustausch- und -analysezentren (ISACs), Betreiber kritischer Infrastrukturen). Der Informationsaustausch zwischen den Teilnehmern eines grenzübergreifenden SOC könnte Daten von Netzwerken und Sensoren sowie laufende Erkenntnisse über Bedrohungen, Kompromittierungsindikatoren und kontextualisierte Informationen über Vorfälle,

[12] 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).

Bedrohungen und Schwachstellen umfassen. Darüber hinaus sollten die grenzübergreifenden SOCs auch Kooperationsvereinbarungen mit anderen grenzübergreifenden SOCs schließen.

(17) Die gemeinsame Lageerfassung unter den zuständigen Behörden ist eine unabdingbare Voraussetzung für die unionsweite Abwehrbereitschaft und Koordinierung in Bezug auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes. Zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Cyberkrisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union wird mit der Richtlinie (EU) 2022/2555 das EU-CyCLONe-Netz eingerichtet. Die Empfehlung (EU) 2017/1584 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen befasst sich mit der Rolle aller einschlägigen Akteure. In der Richtlinie (EU) 2022/2555 wird auch auf die Zuständigkeiten der Kommission im Rahmen des mit dem Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates eingerichteten Katastrophenschutzverfahrens der Union (UCPM) sowie für die Bereitstellung analytischer Berichte für die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) gemäß dem Durchführungsbeschluss (EU) 2018/1993 hingewiesen. Wenn grenzübergreifende SOCs Informationen im Zusammenhang mit einem potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, sollten sie daher dem EU-CyCLONe-Netz, dem CSIRTs-Netz und der Kommission einschlägige Informationen zur Verfügung stellen. Je nach Lage könnten die auszutauschenden Informationen insbesondere technische Informationen, Informationen über die Art und die Motive des tatsächlichen oder potenziellen Angreifers sowie übergeordnete nichttechnische Informationen über einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes umfassen. In diesem Zusammenhang sollte dem Grundsatz „Kenntnis nur, wenn nötig“ und dem potenziell sensiblen Charakter der ausgetauschten Informationen gebührend Rechnung getragen werden.

(18) Stellen, die sich am europäischen Cyberschutzschild beteiligen, sollten ein hohes Maß an Interoperabilität untereinander gewährleisten, gegebenenfalls auch in Bezug auf Datenformate, Taxonomie, Datenverarbeitungs- und Datenanalyseinstrumente sowie sichere Kommunikationskanäle, ein Mindestmaß an Sicherheit auf Anwendungsebene, Lagebewusstsein und Indikatoren. Bei der Annahme einer gemeinsamen Taxonomie und der Entwicklung einer Vorlage für Lageberichte zur Beschreibung der technischen Ursache und der Auswirkungen von Cybersicherheitsvorfällen sollten die laufenden Arbeiten zur Meldung von Sicherheitsvorfällen im Zusammenhang mit der Umsetzung der Richtlinie (EU) 2022/2555 berücksichtigt werden.

(19) Um den Austausch von Daten über Cybersicherheitsbedrohungen aus verschiedenen Quellen in einem vertrauenswürdigen Umfeld in großem Maßstab zu ermöglichen, sollten Stellen, die sich am europäischen Cyberschutzschild beteiligen, mit modernsten und hochsicheren Instrumenten, Ausrüstungen und Infrastrukturen ausgestattet sein. Dies sollte es ermöglichen, die kollektiven Datenerhebungskapazitäten zu verbessern und die Behörden und einschlägigen Einrichtungen rechtzeitig zu warnen, insbesondere durch den Einsatz der neuesten Techniken der künstlichen Intelligenz und der Datenanalyse.

(20) Durch die Sammlung, die Weitergabe und den Austausch von Daten sollte der europäische Cyberschutzschild die technologische Souveränität der Union stärken. Die

Zusammenführung hochwertiger kuratierter Daten sollte auch zur Entwicklung fortgeschrittener Techniken der künstlichen Intelligenz und der Datenanalyse beitragen. Dies sollte durch die Verbindung des europäischen Cyberschutzschilds mit der dank der Verordnung (EU) 2021/1173 des Rates[13] geschaffenen europaweiten Hochleistungsrecheninfrastruktur erleichtert werden.

(21) Obwohl der europäische Cyberschutzschild ein ziviles Projekt ist, könnten die Cyberabwehrkreise von besseren zivilen Fähigkeiten zur Erkennung und Lageerfassung profitieren, die für den Schutz kritischer Infrastrukturen entwickelt werden. Grenzübergreifende SOCs sollten mit Unterstützung der Kommission und des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) und in Zusammenarbeit mit dem Hohen Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) schrittweise spezielle Protokolle und Standards entwickeln, um die Zusammenarbeit mit den Cyberabwehrkreisen, auch in Bezug auf Sicherheitsüberprüfungen und -bedingungen, zu ermöglichen. Die Entwicklung des europäischen Cyberschutzschilds sollte von Überlegungen begleitet werden, die eine künftige Zusammenarbeit mit Netzen und Plattformen, die dem Informationsaustausch in der Cyberabwehrgemeinschaft dienen, in enger Abstimmung mit dem Hohen Vertreter ermöglichen sollen.

(22) Bei der Informationsweitergabe zwischen den Teilnehmern des europäischen Cyberschutzschilds sollten die bestehenden rechtlichen Anforderungen, insbesondere die Datenschutzvorschriften der Union und der Mitgliedstaaten, sowie die Wettbewerbsvorschriften der Union bezüglich des Informationsaustauschs eingehalten werden. Der Empfänger der Informationen sollte, soweit die Verarbeitung personenbezogener Daten erforderlich ist, technische und organisatorische Maßnahmen ergreifen, um die Rechte und Freiheiten der betroffenen Personen zu schützen, die Daten vernichten, sobald sie für den angegebenen Zweck nicht mehr erforderlich sind, und die Stelle, die die Daten zur Verfügung stellt, darüber informieren, dass die Daten vernichtet wurden.

(23) Unbeschadet des Artikels 346 AEUV sollte der Austausch von Informationen, die gemäß Unions- oder nationalen Vorschriften vertraulich sind, auf den Austausch der Daten beschränkt werden, die für den Zweck dieses Austauschs relevant und verhältnismäßig sind. Beim Austausch solcher Informationen sollte ihre Vertraulichkeit gewahrt werden und es sollten die Sicherheit und die geschäftlichen Interessen der betreffenden kritischen Einrichtungen unter vollumfänglicher Achtung des Geschäftsgeheimnisses geschützt werden.

(24) Angesichts der zunehmenden Risiken und der wachsenden Zahl von Cybervorfällen, von denen die Mitgliedstaaten betroffen sind, ist es erforderlich, ein Krisenhilfeinstrument einzurichten, um die Resilienz der Union gegenüber schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu verbessern und die Maßnahmen der Mitgliedstaaten durch finanzielle Hilfe zur Unterstützung der Abwehrbereitschaft, Reaktion und sofortigen Wiederherstellung wesentlicher Dienste zu ergänzen. Dieses Instrument sollte eine rasche Hilfeleistung unter festgelegten Voraussetzungen und unter klaren Bedingungen sowie eine sorgfältige Überwachung und Bewertung der Verwendung

[13] Verordnung (EU) 2021/1173 des Rates vom 13. Juli 2021 zur Gründung des Gemeinsamen Unternehmens für europäisches Hochleistungsrechnen und zur Aufhebung der Verordnung (EU) 2018/1488 (ABl. L 256 vom 19.7.2021, S. 3).

der Ressourcen ermöglichen. Während die primäre Zuständigkeit für Prävention, Vorsorge und Bewältigung bei Cybersicherheitsvorfällen und -krisen bei den Mitgliedstaaten liegt, fördert der Cybernotfallmechanismus die Solidarität zwischen den Mitgliedstaaten gemäß Artikel 3 Absatz 3 des Vertrags über die Europäische Union (EUV).

(25) Der Cybernotfallmechanismus sollte die Mitgliedstaaten in Ergänzung ihrer eigenen Maßnahmen und Ressourcen sowie anderer bestehender Unterstützungsoptionen – wie der von der Agentur der Europäischen Union für Cybersicherheit (ENISA) im Einklang mit ihrem Mandat bereitgestellten Dienste, der koordinierten Reaktion und der Unterstützung durch das CSIRTs-Netz, der Unterstützung der Eindämmung durch das EU-CyCLONe-Netz sowie der Amtshilfe zwischen den Mitgliedstaaten, auch im Zusammenhang mit Artikel 42 Absatz 7 EUV, der SSZ-Teams für die rasche Reaktion auf Cybervorfälle[14] und der Soforteinsatzteams für hybride Bedrohungen – im Falle einer Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes und deren sofortiger Bewältigung unterstützen. Er sollte der Notwendigkeit Rechnung tragen, dass spezialisierte Mittel zur Verfügung stehen müssen, um die Abwehrbereitschaft und die Reaktion auf Cybersicherheitsvorfälle in der gesamten Union und in Drittländern zu unterstützen.

(26) Dieses Instrument lässt die Verfahren und Rahmen für die Koordinierung der Krisenreaktion auf Unionsebene, insbesondere das UCPM[15], die IPCR[16] und die Richtlinie (EU) 2022/2555 unberührt. Es kann zu Maßnahmen beitragen oder diese ergänzen, die im Zusammenhang mit Artikel 42 Absatz 7 EUV oder in den in Artikel 222 AEUV genannten Situationen durchgeführt werden. Der Einsatz dieses Instruments sollte gegebenenfalls auch mit der Umsetzung der Maßnahmen des Instrumentariums für die Cyberdiplomatie koordiniert werden.

(27) Die im Rahmen dieser Verordnung geleistete Hilfe sollte die von den Mitgliedstaaten auf nationaler Ebene ergriffenen Maßnahmen unterstützen und ergänzen. Dazu sollte für eine enge Zusammenarbeit und Konsultation zwischen der Kommission und dem betroffenen Mitgliedstaat gesorgt werden. Wenn ein Mitgliedstaat Unterstützung im Rahmen des Cybernotfallmechanismus beantragt, sollte er einschlägige Informationen bereitstellen, die den Unterstützungsbedarf begründen.

(28) Gemäß der Richtlinie (EU) 2022/2555 müssen die Mitgliedstaaten eine oder mehrere Behörden für das Cyberkrisenmanagement benennen oder einrichten und sicherstellen, dass sie über angemessene Ressourcen verfügen, um die ihnen übertragenen Aufgaben wirksam und effizient ausführen zu können. Ferner werden die Mitgliedstaaten darin dazu verpflichtet, Kapazitäten, Mittel und Verfahren zu ermitteln, die im Fall einer Krise eingesetzt werden können, sowie einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und auf Cyberkrisen aufzustellen, in dem die Ziele und Modalitäten für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen festgelegt sind. Überdies sind die Mitgliedstaaten verpflichtet, ein oder mehrere CSIRTs einzurichten, die mit der Bewältigung von

---

14 Beschluss (GASP) 2017/2315 des Rates vom 11. Dezember 2017 über die Begründung der Ständigen Strukturierten Zusammenarbeit (PESCO) und über die Liste der daran teilnehmenden Mitgliedstaaten.

15 Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union (ABl. L 347 vom 20.12.2013, S. 924).

16 Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) und im Einklang mit der Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

Sicherheitsvorfällen nach einem genau festgelegten Ablauf betraut sind und mindestens die in den Anwendungsbereich der genannten Richtlinie fallenden Sektoren, Teilsektoren und Arten von Einrichtungen abdecken, und dafür zu sorgen, dass sie mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam wahrnehmen können. Diese Verordnung lässt die Rolle der Kommission bei der Gewährleistung der Einhaltung der Verpflichtungen aus der Richtlinie (EU) 2022/2555 durch die Mitgliedstaaten unberührt. Der Cybernotfallmechanismus sollte Unterstützung für Maßnahmen zur Stärkung der Abwehrbereitschaft sowie für Maßnahmen zur Reaktion auf Sicherheitsvorfälle bereitstellen, um die Auswirkungen von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes abzumildern, die sofortige Wiederherstellung zu unterstützen und/oder die Funktionsfähigkeit wesentlicher Dienste wiederherzustellen.

(29) Im Rahmen der Vorsorgemaßnahmen sollten koordinierte Tests und eine entsprechende Bewertung der Cybersicherheit von in hochkritischen Sektoren tätigen Einrichtungen gemäß der Richtlinie (EU) 2022/2555 unterstützt werden, um einen kohärenten Ansatz zu fördern und die Sicherheit in der gesamten Union und ihrem Binnenmarkt zu erhöhen. Dazu sollte die Kommission mit Unterstützung der ENISA und in Zusammenarbeit mit der durch die Richtlinie (EU) 2022/2555 eingesetzten NIS-Kooperationsgruppe regelmäßig einschlägige Sektoren oder Teilsektoren festlegen, die für eine finanzielle Unterstützung für koordinierte Tests auf Unionsebene in Betracht kommen sollen. Die Sektoren oder Teilsektoren sollten aus Anhang I der Richtlinie (EU) 2022/2555 („Sektoren der hohen Kritikalität“) ausgewählt werden. Die koordinierten Tests sollten auf gemeinsamen Risikoszenarien und -methoden beruhen. Auch angesichts der Notwendigkeit, Doppelarbeit zu vermeiden, sollten bei der Auswahl der Sektoren und der Entwicklung von Risikoszenarien einschlägige unionsweite Risikobewertungen und -szenarien berücksichtigt werden, darunter etwa die Risikobewertung und -szenarien, zu deren Durchführung die Kommission, der Hohe Vertreter und die NIS-Kooperationsgruppe in Abstimmung mit den einschlägigen zivilen und militärischen Einrichtungen und Agenturen sowie bestehenden Netzwerken wie dem EU-CyCLONe in den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union aufgefordert werden; dazu zählen auch die Risikobewertung von Kommunikationsnetzen und -infrastrukturen, die im gemeinsamen Ministeraufruf von Nevers gefordert und von der NIS-Kooperationsgruppe mit Unterstützung der Kommission und der ENISA und in Zusammenarbeit mit dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) durchgeführt wird, die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchzuführenden koordinierten Risikobewertungen und das Testen der digitalen operationalen Resilienz gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates[17]. Bei der Auswahl der Sektoren sollte auch der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastrukturen Rechnung getragen werden.

(30) Darüber hinaus sollte der Cybernotfallmechanismus Unterstützung für andere Vorsorgemaßnahmen und die Abwehrbereitschaft in anderen Sektoren bieten, die

[17] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.

nicht von den koordinierten Tests von in hochkritischen Sektoren tätigen Einrichtungen erfasst werden. Diese Maßnahmen könnten verschiedene Arten nationaler Vorsorgemaßnahmen umfassen.

(31) Der Cybernotfallmechanismus sollte auch Unterstützung für Maßnahmen zur Reaktion auf Sicherheitsvorfälle bereitstellen, um die Auswirkungen von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes abzumildern, die sofortige Wiederherstellung zu unterstützen oder die Funktionsfähigkeit wesentlicher Dienste wiederherzustellen. Gegebenenfalls sollte er das UCPM ergänzen, um einen umfassenden Ansatz für die Bewältigung der Folgen von Cybervorfällen für die Bürgerinnen und Bürger zu gewährleisten.

(32) Der Cybernotfallmechanismus sollte den Mitgliedstaaten bei der Unterstützung eines von einem schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes betroffenen Mitgliedstaat helfen, auch mithilfe des CSIRTs-Netzes gemäß Artikel 15 der Richtlinie (EU) 2022/2555. Mitgliedstaaten, die Unterstützung leisten, sollten die Möglichkeit haben, die Erstattung der Kosten im Zusammenhang mit der Entsendung von Sachverständigenteams im Rahmen der Amtshilfe zu beantragen. Die erstattungsfähigen Kosten könnten Reise- und Unterbringungskosten sowie Tagegelder für Cybersicherheitsexperten umfassen.

(33) Es sollte schrittweise eine Cybersicherheitsreserve auf Unionsebene eingerichtet werden, die aus Diensten privater Anbieter verwalteter Sicherheitsdienste besteht, um die Reaktion und sofortige Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu unterstützen. Die EU-Cybersicherheitsreserve sollte die Verfügbarkeit und Einsatzbereitschaft der betroffenen Dienste gewährleisten. Die Dienste der EU-Cybersicherheitsreserve sollten dazu dienen, den nationalen Behörden bei der Unterstützung betroffener in kritischen oder hochkritischen Sektoren tätiger Einrichtungen ergänzend zu ihren eigenen Maßnahmen auf nationaler Ebene zu helfen. Wenn die Mitgliedstaaten Unterstützung aus der EU-Cybersicherheitsreserve beantragen, sollten sie angeben, welche Unterstützung die betroffene Einrichtung auf nationaler Ebene erhält, und dies sollte bei der Prüfung des Antrags des Mitgliedstaats berücksichtigt werden. Die Dienste der EU-Cybersicherheitsreserve können auch dazu dienen, die Organe, Einrichtungen und sonstigen Stellen der Union unter ähnlichen Bedingungen zu unterstützen.

(34) Im Hinblick auf die Auswahl privater Dienstleister für die Bereitstellung von Diensten im Rahmen der EU-Cybersicherheitsreserve muss eine Reihe von Mindestkriterien festgelegt werden, die in die Ausschreibung für die Auswahl dieser Anbieter aufgenommen werden sollten, damit die Bedürfnisse der Behörden und der in kritischen oder hochkritischen Sektoren tätigen Einrichtungen in den Mitgliedstaaten erfüllt werden.

(35) Zur Unterstützung der Einrichtung der EU-Cybersicherheitsreserve könnte die Kommission in Erwägung ziehen, die ENISA mit der Ausarbeitung eines möglichen Zertifizierungssystems gemäß der Verordnung (EU) 2019/881 für verwaltete Sicherheitsdienste in den vom Cybernotfallmechanismus abgedeckten Bereichen zu beauftragen.

(36) Um die Ziele dieser Verordnung, nämlich die Förderung einer gemeinsamen Lageerfassung, die Stärkung der Resilienz der Union und die Ermöglichung einer wirksamen Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, zu unterstützen, sollten das EU-

CyCLONe-Netz, das CSIRT-Netz oder die Kommission die ENISA beauftragen können, Bedrohungen, Schwachstellen und Eindämmungsmaßnahmen im Zusammenhang mit einem bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes zu überprüfen und zu bewerten. Nach Abschluss der Überprüfung und Bewertung eines Sicherheitsvorfalls sollte die ENISA in Zusammenarbeit mit den einschlägigen Beteiligten, einschließlich Vertretern des Privatsektors, der Mitgliedstaaten, der Kommission und anderer einschlägiger Organe, Einrichtungen und sonstiger Stellen der EU, einen Bericht über die Überprüfung des Sicherheitsvorfalls erstellen. Was den Privatsektor betrifft, entwickelt die ENISA derzeit Kanäle für den Informationsaustausch mit spezialisierten Anbietern, darunter auch mit Anbietern verwalteter Sicherheitslösungen, um zur Erfüllung des Auftrags der ENISA beizutragen, ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union zu erreichen. Aufbauend auf der Zusammenarbeit mit Interessenträgern, einschließlich des Privatsektors, sollte der Bericht über die Überprüfung bestimmter Sicherheitsvorfälle darauf abzielen, die Ursachen, Auswirkungen und Eindämmungsmaßnahmen eines Sicherheitsvorfalls nach seinem Auftreten zu bewerten. Besonderes Augenmerk sollte auf die Beiträge und Erkenntnisse gelegt werden, die von den Anbietern verwalteter Sicherheitsdienste geteilt werden, die die in dieser Verordnung geforderten Bedingungen der größtmöglichen beruflichen Integrität, Unparteilichkeit und des erforderlichen technischen Fachwissens erfüllen. Der Bericht sollte vorgelegt werden und in die Arbeit des EU-CyCLONe-Netzes, des CSIRTs-Netzes und der Kommission einfließen. Betrifft der Vorfall ein Drittland, so sollte die Kommission den Bericht auch an den Hohen Vertreter weitergeben.

(37) Angesichts des unvorhersehbaren Charakters von Cybersicherheitsangriffen und der Tatsache, dass sie häufig nicht auf ein bestimmtes geografisches Gebiet beschränkt sind und ein hohes Ausbreitungsrisiko bergen, trägt die Stärkung der Resilienz von Nachbarländern und ihrer Fähigkeit, wirksam auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes zu reagieren, auch zum Schutz der Union als Ganzes bei. Daher können Drittländer, die mit dem Programm Digitales Europa assoziiert sind, aus der EU-Cybersicherheitsreserve unterstützt werden, sofern dies im jeweiligen Assoziierungsabkommen mit dem Programm Digitales Europa vorgesehen ist. Die Fördermittel für assoziierte Drittländer sollten von der Union im Rahmen einschlägiger Partnerschafts- und Finanzierungsinstrumente für diese Länder gewährt werden. Die Unterstützung sollte Dienste im Bereich der Reaktion und sofortigen Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes abdecken. Die in dieser Verordnung festgelegten Bedingungen für die EU-Cybersicherheitsreserve und für vertrauenswürdige Anbieter sollten auch bei der Unterstützung der mit dem Programm Digitales Europa assoziierten Drittländer gelten.

(38) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden, damit sie die Bedingungen für die Interoperabilität zwischen grenzübergreifenden SOCs, die Verfahrensmodalitäten für den Informationsaustausch im Zusammenhang mit einem potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes zwischen grenzübergreifenden SOCs und Einrichtungen der Union sowie technische Anforderungen zur Gewährleistung eines hohen Maßes an Datensicherheit und physischer Sicherheit, die Art und die Anzahl der für die EU-Cybersicherheitsreserve erforderlichen Notdienste die genauen Modalitäten für die Zuweisung der Unterstützungsdienste der EU-Cybersicherheitsreserve zu präzisieren. Diese

Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden.

(39) Das Ziel dieser Verordnung kann besser auf Unionsebene als durch die Mitgliedstaaten erreicht werden. Die Union kann daher im Einklang mit dem Subsidiaritätsprinzip und dem Grundsatz der Verhältnismäßigkeit, die in Artikel 5 des Vertrags über die Europäische Union niedergelegt sind, tätig werden. Diese Verordnung geht nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Kapitel I

ALLGEMEINE ZIELE, GEGENSTAND UND BEGRIFFSBESTIMMUNGEN

Artikel 1

Gegenstand und Ziele

(1) In dieser Verordnung werden Maßnahmen zur Stärkung der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen festgelegt, und zwar insbesondere durch

a) den Aufbau einer europaweiten Infrastruktur von Sicherheitseinsatzzentren („europäischer Cyberschutzschild“), um gemeinsame Fähigkeiten zur Erkennung und Lageerfassung aufzubauen und zu verbessern;

b) die Schaffung eines Cybernotfallmechanismus zur Unterstützung der Mitgliedstaaten bei der Vorsorge für, Bewältigung von und sofortigen Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes;

c) die Einrichtung eines europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle zur Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes.

(2) Mit dieser Verordnung wird das Ziel verfolgt, die Solidarität auf Unionsebene durch die Verwirklichung folgender spezifischer Ziele zu stärken:

a) Stärkung der gemeinsamen Fähigkeiten der Union zur Erkennung und Lageerfassung im Bereich der Cyberbedrohungen und -vorfälle, um so in der gesamten digitalen Wirtschaft der Union eine Stärkung der Wettbewerbsfähigkeit der Industrie- und Dienstleistungszweige zu ermöglichen und zur technologischen Souveränität der Union im Bereich der Cybersicherheit beizutragen;

b) Stärkung der Abwehrbereitschaft der in kritischen und hochkritischen Sektoren tätigen Einrichtungen in der gesamten Union und Stärkung der Solidarität durch den Aufbau gemeinsamer Kapazitäten für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, indem u. a. die Unionsunterstützung für die Bewältigung von Cybersicherheitsvorfällen auch Drittländern, die mit dem Programm Digitales Europa (DEP) assoziiert sind, zur Verfügung gestellt wird;

c) Stärkung der Abwehrfähigkeit der Union und Leistung eines Beitrags zu einer wirksamen Bewältigung durch die Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes, einschließlich der Gewinnung von Erkenntnissen und gegebenenfalls der Formulierung von Empfehlungen.

(3) Diese Verordnung lässt die vorrangige Zuständigkeit der Mitgliedstaaten für die nationale Sicherheit, die öffentliche Sicherheit sowie die Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten unberührt.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:

1. „**grenzübergreifendes Sicherheitseinsatzzentrum**“ („grenzübergreifendes SOC“) ist eine länderübergreifende Plattform, auf der nationale SOCs aus mindestens drei Mitgliedstaaten, die zusammen ein Aufnahmekonsortium bilden, in einer koordinierten Netzstruktur zusammenarbeiten und die dazu bestimmt ist, Cyberbedrohungen und -vorfälle zu verhüten und die Gewinnung hochwertiger Erkenntnisse zu unterstützen, insbesondere durch den Austausch von Daten aus verschiedenen öffentlichen und privaten Quellen sowie die gemeinsame Nutzung modernster Instrumente und die gemeinsame Entwicklung von Erkennungs-, Analyse-, Präventions- und Schutzfähigkeiten gegenüber Cyberangriffen in einem vertrauenswürdigen Umfeld;

2. „**öffentliche Stelle**“ ist eine Einrichtung des öffentlichen Rechts im Sinne des Artikels 2 Absatz 1 Nummer 4 der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates[18];

3. „**Aufnahmekonsortium**“ ist ein Konsortium aus beteiligten Staaten, die durch nationale SOCs vertreten werden und vereinbart haben, ein grenzübergreifendes SOC einzurichten und zu betreiben und hierzu an der Beschaffung von Instrumenten und Infrastrukturen mitzuwirken;

4. „**Einrichtung**“ ist eine Einrichtung im Sinne des Artikels 6 Nummer 38 der Richtlinie (EU) 2022/2555;

5. „**in kritischen oder hochkritischen Sektoren tätige Einrichtungen**“ bezeichnet die Arten von Einrichtungen, die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführt sind;

6. „**Cyberbedrohung**“ ist eine Cyberbedrohung im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/881;

7. „**schwerwiegender Cybersicherheitsvorfall**“ ist ein Cybersicherheitsvorfall, der die Kriterien in Artikel 23 Absatz 3 der Richtlinie (EU) 2022/2555 erfüllt;

8. „**Cybersicherheitsvorfall großen Ausmaßes**“ ist ein Sicherheitsvorfall im Sinne des Artikels 6 Nummer 7 der Richtlinie (EU) 2022/2555;

[18] Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

9. „**Abwehrbereitschaft**“ bezeichnet einen Zustand der Bereitschaft und Fähigkeit, eine wirksame rasche Reaktion auf einen schwerwiegenden Cybersicherheitsvorfall oder einen Cybersicherheitsvorfall großen Ausmaßes zu gewährleisten, der sich aus vorab getroffenen Risikobewertungs- und Überwachungsmaßnahmen ergibt;

10. „**Reaktion**“ bezeichnet eine Maßnahme, die aufgrund eines schwerwiegenden Cybersicherheitsvorfalls oder eines Cybersicherheitsvorfalls großen Ausmaßes bzw. während oder nach einem solchen Vorfall zur Bewältigung seiner unmittelbaren und kurzfristigen nachteiligen Folgen ergriffen wird;

11. „**vertrauenswürdige Anbieter**“ sind Anbieter verwalteter Sicherheitsdienste im Sinne des Artikels 6 Nummer 40 der Richtlinie (EU) 2022/2555, die gemäß Artikel 16 der vorliegenden Verordnung ausgewählt wurden.

Kapitel II

DER EUROPÄISCHE CYBERSCHUTZSCHILD

Artikel 3

Einrichtung des europäischen Cyberschutzschilds

(1) Eine vernetzte europaweite Infrastruktur aus Sicherheitseinsatzzentren (im Folgenden „europäischer Cyberschutzschild“) wird eingerichtet, um fortgeschrittene Fähigkeiten der Union zur Erkennung, Analyse und Verarbeitung von Daten über Cyberbedrohungen und -vorfälle in der Union zu entwickeln. Diese Infrastruktur besteht aus allen nationalen Sicherheitseinsatzzentren („nationale SOCs“) und grenzübergreifenden Sicherheitseinsatzzentren („grenzübergreifende SOCs“).

Maßnahmen zur Umsetzung des europäischen Cyberschutzschilds werden mit Mitteln aus dem Programm Digitales Europa unterstützt und im Einklang mit der Verordnung (EU) 2021/694 und insbesondere deren spezifischen Ziel 3 durchgeführt.

(2) Der europäische Cyberschutzschild hat folgende Aufgaben:

a) Zusammenführung und Austausch von Daten über Cyberbedrohungen und -vorfälle aus verschiedenen Quellen durch grenzübergreifende SOCs;

b) Erstellung hochwertiger, handlungsrelevanter Informationen und Erkenntnisse über Cyberbedrohungen unter Nutzung modernster Instrumente, darunter insbesondere Techniken der künstlichen Intelligenz und der Datenanalyse;

c) Leisten eines Beitrags zu einem besseren Schutz vor Cyberbedrohungen und einer besseren Reaktion darauf;

d) Leisten eines Beitrags zur schnelleren Erkennung von Cyberbedrohungen und zur Lageerfassung in der gesamten Union;

e) Erbringung von Dienstleistungen und Durchführung von Tätigkeiten für die Cybersicherheitskreise in der Union, einschließlich eines Beitrags zur Entwicklung fortgeschrittener Instrumente der künstlichen Intelligenz und der Datenanalyse.

Sein Aufbau erfolgt in Zusammenarbeit mit der europaweiten Hochleistungsrecheninfrastruktur, die gemäß der Verordnung (EU) 2021/1173 eingerichtet worden ist.

Artikel 4

Nationale Sicherheitseinsatzzentren

(1) Jeder Mitgliedstaat benennt zur Beteiligung am europäischen Cyberschutzschild mindestens ein nationales Sicherheitseinsatzzentrum (SOC). Das nationale SOC ist eine öffentliche Stelle.

Es muss in der Lage sein, als Bezugspunkt und Zugangstor zu anderen öffentlichen und privaten Organisationen auf nationaler Ebene für die Sammlung und Auswertung von Informationen über Cybersicherheitsbedrohungen und -vorfälle zu fungieren und zu einem grenzübergreifenden SOC beizutragen. Es wird mit modernster Technik ausgestattet, die es ermöglicht, Daten in Bezug auf Cybersicherheitsbedrohungen und -vorfälle zu erkennen, zu aggregieren und zu analysieren.

(2) Im Anschluss an eine Aufforderung zur Interessenbekundung wählt das Europäische Kompetenzzentrum für Cybersicherheit (ECCC) nationale SOCs zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen mit dem ECCC aus. Das ECCC kann den ausgewählten nationalen SOCs Finanzhilfen zur Finanzierung des Betriebs dieser Instrumente und Infrastrukturen gewähren. Der Finanzbeitrag der Union deckt bis zu 50 % der Beschaffungskosten der Instrumente und Infrastrukturen und bis zu 50 % der Betriebskosten; die verbleibenden Kosten trägt der betreffende Mitgliedstaat. Bevor das Verfahren für die Beschaffung der Instrumente und Infrastrukturen eingeleitet wird, schließen das ECCC und das nationale SOC eine Aufnahme- und Nutzungsvereinbarung, in der die Verwendung der Instrumente und Infrastrukturen geregelt wird.

(3) Ein gemäß Absatz 2 ausgewähltes nationales SOC verpflichtet sich, innerhalb von zwei Jahren nach dem Zeitpunkt der Beschaffung der Instrumente und Infrastrukturen oder des Empfangs der Finanzhilfe, je nachdem, welcher Zeitpunkt früher eintritt, einen Antrag auf Teilnahme an einem grenzübergreifenden SOC zu stellen. Nimmt ein nationales SOC bis dahin nicht an einem grenzübergreifenden SOC teil, kann es keine weitere Unionsunterstützung im Rahmen dieser Verordnung erhalten.

Artikel 5

Grenzübergreifende Sicherheitseinsatzzentren

(1) Ein Aufnahmekonsortium aus mindestens drei Mitgliedstaaten, vertreten durch deren nationale SOCs, die sich verpflichtet haben, bei der Koordinierung ihrer Tätigkeiten zur Erkennung und Überwachung von Cyberbedrohungen zusammenzuarbeiten, kann an Maßnahmen zur Einrichtung eines grenzübergreifenden SOC teilnehmen.

(2) Im Anschluss an eine Aufforderung zur Interessenbekundung wählt das ECCC ein Aufnahmekonsortium zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten und Infrastrukturen mit dem ECCC aus. Das ECCC kann dem Aufnahmekonsortium eine Finanzhilfe zur Finanzierung des Betriebs der Instrumente und Infrastrukturen gewähren. Der Finanzbeitrag der Union deckt bis zu

75 % der Beschaffungskosten der Instrumente und Infrastrukturen und bis zu 50 % der Betriebskosten; die verbleibenden Kosten trägt das Aufnahmekonsortium. Bevor das Verfahren für die Beschaffung der Instrumente und Infrastrukturen eingeleitet wird, schließen das ECCC und das Aufnahmekonsortium eine Aufnahme- und Nutzungsvereinbarung, in der die Verwendung der Instrumente und Infrastrukturen geregelt wird.

(3) Die Mitglieder des Aufnahmekonsortiums schließen eine schriftliche Konsortialvereinbarung, in der sie ihre internen Regelungen für die Durchführung der Aufnahme- und Nutzungsvereinbarung festlegen.

(4) Ein grenzübergreifendes SOC wird zu rechtlichen Zwecken durch ein nationales SOC, das als Koordinierungsstelle fungiert, oder durch das Aufnahmekonsortium, falls es Rechtspersönlichkeit besitzt, vertreten. Das koordinierende SOC ist für die Einhaltung der Anforderungen der Aufnahme- und Nutzungsvereinbarung und dieser Verordnung verantwortlich.

Artikel 6

Zusammenarbeit und Informationsaustausch in und zwischen grenzübergreifenden Sicherheitseinsatzzentren

(1) Die Mitglieder eines Aufnahmekonsortiums tauschen untereinander im grenzübergreifenden SOC relevante Informationen aus, darunter Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren (*Indicators of Compromise*, IoC), gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Erkennung von Cyberangriffen, sofern

a) dieser Informationsaustausch darauf abzielt, Sicherheitsvorfälle zu verhindern, zu erkennen, darauf zu reagieren oder sich von ihnen zu erholen oder ihre Folgen einzudämmen;

b) durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die Fähigkeit solcher Bedrohungen, sich zu verbreiten, eingedämmt bzw. behindert wird und eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen, Eindämmungsstrategien, Reaktions- und Wiederherstellungsphasen unterstützt werden oder indem die gemeinsame Erforschung von Bedrohungen zwischen öffentlichen und privaten Einrichtungen gefördert wird.

(2) In der schriftlichen Konsortialvereinbarung gemäß Artikel 5 Absatz 3 wird Folgendes festgelegt:

a) eine Verpflichtung zur Weitergabe einer erheblichen Menge an Daten gemäß Absatz 1 und die Bedingungen, unter denen diese Informationen ausgetauscht werden sollen;

b) ein Governance-Rahmen, der Anreize für die Weitergabe von Information durch alle Teilnehmer gibt;

c) Zielsetzungen für Beiträge zur Entwicklung fortgeschrittener Instrumente der künstlichen Intelligenz und der Datenanalyse.

(3) Um den Informationsaustausch zwischen grenzübergreifenden SOCs zu fördern, gewährleisten grenzübergreifende SOCs ein hohes Maß an Interoperabilität untereinander. Die Kommission kann im Wege von Durchführungsrechtsakten nach Anhörung des ECCC die Bedingungen für diese Interoperabilität festlegen, um die Interoperabilität zwischen den grenzübergreifenden SOCs zu erleichtern. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 21 Absatz 2 dieser Verordnung genannten Prüfverfahren erlassen.

(4) Grenzübergreifende SOCs schließen Kooperationsvereinbarungen miteinander, in denen die Grundsätze für den Informationsaustausch zwischen den grenzübergreifenden Plattformen festgelegt werden.

Artikel 7

Zusammenarbeit und Informationsaustausch mit Einrichtungen der Union

(1) Wenn die grenzübergreifenden SOCs Informationen über einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, stellen sie dem EU-CyCLONe-Netz, dem CSIRTs-Netz und der Kommission im Hinblick auf ihre jeweiligen Krisenmanagementaufgaben unverzüglich alle einschlägigen Informationen im Einklang mit der Richtlinie (EU) 2022/2555 zur Verfügung.

(2) Die Kommission kann im Wege von Durchführungsrechtsakten die Verfahrensmodalitäten für die Informationsweitergabe nach Absatz 1 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 21 Absatz 2 dieser Verordnung genannten Prüfverfahren erlassen.

Artikel 8

Sicherheit

(1) Die am europäischen Cyberschutzschild beteiligten Mitgliedstaaten gewährleisten ein hohes Maß an Datensicherheit und physischer Sicherheit der Infrastruktur des europäischen Cyberschutzschilds und stellen sicher, dass die Infrastruktur angemessen verwaltet und kontrolliert wird, um sie vor Bedrohungen zu schützen und ihre Sicherheit sowie die Sicherheit der Systeme und der über die Infrastruktur ausgetauschten Daten zu gewährleisten.

(2) Die am europäischen Cyberschutzschild beteiligten Mitgliedstaaten stellen sicher, dass durch den Informationsaustausch innerhalb des europäischen Cyberschutzschilds mit Einrichtungen, die keine öffentlichen Stellen der Mitgliedstaaten sind, die Sicherheitsinteressen der Union nicht beeinträchtigt werden.

(3) Die Kommission kann Durchführungsrechtsakte erlassen, in denen sie technische Anforderungen festgelegt, nach denen die Mitgliedstaaten ihrer Verpflichtung gemäß den Absätzen 1 und 2 nachkommen müssen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 21 Absatz 2 dieser Verordnung genannten Prüfverfahren erlassen. Dabei berücksichtigt die Kommission mit Unterstützung des Hohen Vertreters einschlägige Sicherheitsstandards auf Verteidigungsebene, um die Zusammenarbeit mit militärischen Akteuren zu erleichtern.

Kapitel III

CYBERNOTFALLMECHANISMUS

Artikel 9

Einrichtung des Cybernotfallmechanismus

(1) Ein Cybernotfallmechanismus wird eingerichtet, um die Resilienz der Union gegenüber großen Cybersicherheitsbedrohungen zu verbessern, sie im Geiste der Solidarität auf die kurzfristigen Auswirkungen von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes vorzubereiten und diese Auswirkungen einzudämmen (im Folgenden der „Mechanismus“).

(2) Maßnahmen zur Umsetzung des Cybernotfallmechanismus werden mit Mitteln aus dem Programm Digitales Europa unterstützt und im Einklang mit der Verordnung (EU) 2021/694 und insbesondere deren spezifischen Ziel 3 durchgeführt.

Artikel 10

Art der Maßnahmen

(1) Der Mechanismus soll folgende Arten von Maßnahmen unterstützen:

a) Vorsorgemaßnahmen, einschließlich koordinierter Tests der Abwehrbereitschaft der in hochkritischen Sektoren tätigen Einrichtungen in der gesamten Union;

b) Reaktionsmaßnahmen zur Unterstützung der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes sowie der anschließenden sofortigen Wiederherstellung durch vertrauenswürdige Anbieter, die sich an der gemäß Artikel 12 eingerichteten EU-Cybersicherheitsreserve beteiligen;

c) Amtshilfe, die darin besteht, dass nationale Behörden eines Mitgliedstaats einen anderen Mitgliedstaat unterstützen, insbesondere gemäß Artikel 11 Absatz 3 Buchstabe f der Richtlinie (EU) 2022/2555.

Artikel 11

Koordinierte Tests der Abwehrbereitschaft von Einrichtungen

(1) Zur Unterstützung der in Artikel 10 Absatz 1 Buchstabe a genannten koordinierten Tests der Abwehrbereitschaft von Einrichtungen in der gesamten Union legt die Kommission nach Konsultation der NIS-Kooperationsgruppe und der ENISA die betroffenen Sektoren oder Teilsektoren aus den in Anhang I der Richtlinie (EU) 2022/2555 aufgeführten Sektoren bzw. Teilsektoren fest, aus denen Einrichtungen solchen koordinierten Tests der Abwehrbereitschaft unterzogen werden können, wobei bestehende und geplante koordinierte Risikobewertungen und Resilienztests auf Unionsebene zu berücksichtigen sind.

(2) Die NIS-Kooperationsgruppe entwickelt in Zusammenarbeit mit der Kommission, der ENISA und dem Hohen Vertreter gemeinsame Risikoszenarien und -methoden für die Durchführung der koordinierten Tests.

Artikel 12

Einrichtung der EU-Cybersicherheitsreserve

(1) Eine EU-Cybersicherheitsreserve wird eingerichtet, um die in Absatz 3 genannten Nutzer bei der Reaktion bzw. der Hilfestellung für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle oder Cybersicherheitsvorfälle großen Ausmaßes und bei der sofortigen Wiederherstellung nach solchen Vorfällen zu unterstützen.

(2) Die EU-Cybersicherheitsreserve besteht aus Sicherheitsvorfall-Notdiensten vertrauenswürdiger Anbieter, die nach den in Artikel 16 festgelegten Kriterien ausgewählt wurden. Die Reserve umfasst vorab zugesagte Dienste. Die Dienste müssen in allen Mitgliedstaaten durchführbar sein.

(3) Zu den Nutzern der Dienste der EU-Cybersicherheitsreserve gehören

a) die in Artikel 9 Absätze 1 und 2 bzw. Artikel 10 der Richtlinie (EU) 2022/2555 genannten Behörden für das Cyberkrisenmanagement und CSIRTs der Mitgliedstaaten;

b) die Organe, Einrichtungen und sonstigen Stellen der Union.

(4) Die in Absatz 3 Buchstabe a genannten Nutzer nehmen die Dienste der EU-Cybersicherheitsreserve in Anspruch, um auf schwerwiegende Sicherheitsvorfälle oder Sicherheitsvorfälle großen Ausmaßes, von denen in kritischen und hochkritischen Sektoren tätige Einrichtungen betroffen sind, zu reagieren oder die Reaktion darauf und die anschließende sofortige Wiederherstellung zu unterstützen.

(5) Die Kommission trägt die Gesamtverantwortung für die Umsetzung der EU-Cybersicherheitsreserve. Die Kommission legt die Prioritäten und die Entwicklung der EU-Cybersicherheitsreserve im Einklang mit den Anforderungen der in Absatz 3 genannten Nutzer fest; sie überwacht ihre Umsetzung und sorgt für Komplementarität, Kohärenz, Synergien und Verbindungen mit anderen Unterstützungsmaßnahmen im Rahmen dieser Verordnung sowie mit anderen Maßnahmen und Programmen der Union.

(6) Die Kommission kann die ENISA ganz oder teilweise mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve im Wege von Beitragsvereinbarungen betrauen.

(7) Zur Unterstützung der Kommission bei der Einrichtung der EU-Cybersicherheitsreserve arbeitet die ENISA nach Konsultation der Mitgliedstaaten und der Kommission eine Aufstellung der benötigten Dienste aus. Die ENISA arbeitet nach Konsultation der Kommission eine ähnliche Aufstellung aus, um den Bedarf von Drittländern zu ermitteln, die nach Artikel 17 Unterstützung aus der EU-Cybersicherheitsreserve erhalten können. Dabei konsultiert die Kommission gegebenenfalls den Hohen Vertreter.

(8) Die Kommission kann im Wege von Durchführungsrechtsakten die Art und die Anzahl der für die EU-Cybersicherheitsreserve erforderlichen Notdienste festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 21 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 13

Beantragung der Unterstützung aus der EU-Cybersicherheitsreserve

(1) Die in Artikel 12 Absatz 3 genannten Nutzer können Dienste der EU-Cybersicherheitsreserve anfordern, um die Reaktion auf schwerwiegende Sicherheitsvorfälle oder Sicherheitsvorfälle großen Ausmaßes und die anschließende sofortige Wiederherstellung zu unterstützen.

(2) Um Unterstützung aus der EU-Cybersicherheitsreserve zu erhalten, ergreifen die in Artikel 12 Absatz 3 genannten Nutzer Maßnahmen zur Eindämmung der Auswirkungen des Sicherheitsvorfalls, für den die Unterstützung beantragt wird, und stellen direkte technische Hilfe und andere Ressourcen zur Unterstützung der Reaktion auf den Sicherheitsvorfall und der anschließenden sofortigen Wiederherstellung bereit.

(3) Unterstützungsanträge der in Artikel 12 Absatz 3 Buchstabe a dieser Verordnung genannten Nutzer werden der Kommission und der ENISA über die von dem Mitgliedstaat gemäß Artikel 8 Absatz 3 der Richtlinie (EU) 2022/2555 benannte oder eingerichtete zentrale Anlaufstelle übermittelt.

(4) Die Mitgliedstaaten unterrichten das CSIRTs-Netz und gegebenenfalls das EU-CyCLONe-Netz über ihre gemäß diesem Artikel übermittelten Anträge auf Sicherheitsvorfall-Notdienste und auf Unterstützung bei der sofortigen Wiederherstellung.

(5) Anträge auf Sicherheitsvorfall-Notdienste und auf Unterstützung bei der sofortigen Wiederherstellung müssen Folgendes enthalten:

a) zweckmäßige Informationen über die betroffene Einrichtung und die möglichen Auswirkungen des Sicherheitsvorfalls sowie über die geplante Verwendung der beantragten Unterstützung, einschließlich einer Bedarfsschätzung;

b) Informationen über gemäß Absatz 2 ergriffene Maßnahmen zur Eindämmung der Auswirkungen des Vorfalls, für den die Unterstützung beantragt wird;

c) Informationen über andere Formen der Unterstützung, die der betroffenen Einrichtung zur Verfügung stehen, einschließlich bestehender vertraglicher Vereinbarungen über Sicherheitsvorfall-Notdienste und Dienste zur sofortigen Wiederherstellung sowie Versicherungsverträge, die möglicherweise diese Art von Vorfällen abdecken.

(6) Die ENISA erstellt in Zusammenarbeit mit der Kommission und der NIS-Kooperationsgruppe ein Musterformular, um das Beantragen von Unterstützung aus der EU-Cybersicherheitsreserve zu erleichtern.

(7) Die Kommission kann im Wege von Durchführungsrechtsakten die genauen Modalitäten für die Zuweisung der Unterstützungsdienste der EU-Cybersicherheitsreserve präzisieren. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 21 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 14

Umsetzung der Unterstützung aus der EU-Cybersicherheitsreserve

(1) Anträge auf Unterstützung aus der EU-Cybersicherheitsreserve werden von der Kommission mit Unterstützung der ENISA oder nach Maßgabe der

Beitragsvereinbarungen gemäß Artikel 12 Absatz 6 geprüft, und den in Artikel 12 Absatz 3 genannten Nutzern wird unverzüglich eine Antwort übermittelt.

(2) Bei mehreren gleichzeitig eingehenden Anträgen erfolgt gegebenenfalls eine Priorisierung nach folgenden Kriterien:

a) Schwere des Sicherheitsvorfalls,

b) Art der betroffenen Einrichtung, wobei Sicherheitsvorfälle, die wesentliche Einrichtungen im Sinne des Artikels 3 Absatz 1 der Richtlinie (EU) 2022/2555 betreffen, eine höhere Priorität haben,

c) potenzielle Auswirkungen auf betroffene Mitgliedstaaten oder Nutzer;

d) potenziell grenzüberschreitender Charakter des Sicherheitsvorfalls und Risiko eines Übergreifens auf andere Mitgliedstaaten oder Nutzer;

e) vom Nutzer ergriffene Maßnahmen zur Unterstützung der Reaktion und der sofortigen Wiederherstellung gemäß Artikel 13 Absatz 2 und Artikel 13 Absatz 5 Buchstabe b.

(3) Die Bereitstellung der Dienste der EU-Cybersicherheitsreserve erfolgt im Einklang mit besonderen Vereinbarungen zwischen dem Diensteanbieter und dem Nutzer, dem die Unterstützung aus der EU-Cybersicherheitsreserve gewährt wird. Diese Vereinbarungen müssen Haftungsbedingungen enthalten.

(4) Die in Absatz 3 genannten Vereinbarungen können auf Mustern beruhen, die von der ENISA nach Konsultation der Mitgliedstaaten erstellt werden.

(5) Die Kommission und die ENISA übernehmen keine vertragliche Haftung für Schäden, die Dritten durch die im Rahmen der Umsetzung der EU-Cybersicherheitsreserve bereitgestellten Dienste entstehen.

(6) Innerhalb eines Monats nach Abschluss der Unterstützungsmaßnahme übermitteln die Nutzer der Kommission und der ENISA einen zusammenfassenden Bericht über den erbrachten Dienst, die erzielten Ergebnisse und die gewonnenen Erkenntnisse. Stammt der Nutzer aus einem Drittland gemäß Artikel 17, so wird dieser Bericht auch an den Hohen Vertreter übermittelt.

(7) Die Kommission berichtet der NIS-Kooperationsgruppe regelmäßig über die Inanspruchnahme und die Ergebnisse der Unterstützung.

Artikel 15

Koordinierung mit Krisenmanagementmechanismen

(1) Wenn schwerwiegende Cybersicherheitsvorfälle oder Cybersicherheitsvorfälle großen Ausmaßes von Katastrophen im Sinne des Beschlusses Nr. 1313/2013/EU[19] verursacht werden oder zu solchen Katastrophen führen, ergänzt die im Rahmen dieser Verordnung geleistete Unterstützung der Reaktion auf solche Vorfälle die Maßnahmen im Rahmen des Beschlusses Nr. 1313/2013/EU, der davon unberührt bleibt.

[19] Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union (ABl. L 347 vom 20.12.2013, S. 924).

(2) Im Falle eines grenzüberschreitenden Cybersicherheitsvorfalls großen Ausmaßes, bei dem die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) aktiviert wird, erfolgt die im Rahmen dieser Verordnung geleistete Unterstützung der Reaktion auf einen solchen Vorfall im Einklang mit den einschlägigen Protokollen und Verfahren der IPCR.

(3) Die Unterstützung des Cybernotfallmechanismus kann in Absprache mit dem Hohen Vertreter die im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik und der Gemeinsamen Sicherheits- und Verteidigungspolitik geleistete Hilfe ergänzen, auch durch die Teams für die rasche Reaktion auf Cybervorfälle. Sie kann auch die Hilfe ergänzen, die ein Mitgliedstaat einem anderen Mitgliedstaat gemäß Artikel 42 Absatz 7 des Vertrags über die Europäische Union gewährt, oder dazu beitragen.

(4) Die Unterstützung des Cybernotfallmechanismus kann Teil der gemeinsamen Reaktion der Union und der Mitgliedstaaten in den in Artikel 222 des Vertrags über die Arbeitsweise der Europäischen Union genannten Situationen sein.

Artikel 16

Vertrauenswürdige Anbieter

(1) In Beschaffungsverfahren zur Einrichtung der EU-Cybersicherheitsreserve handelt der öffentliche Auftraggeber im Einklang mit den in der Verordnung (EU, Euratom) 2018/1046 festgelegten Grundsätzen und im Einklang mit den folgenden Grundsätzen:

a) Gewährleistung, dass die EU-Cybersicherheitsreserve Dienste umfasst, die in allen Mitgliedstaaten durchgeführt werden können, wobei insbesondere nationale Anforderungen an die Erbringung solcher Dienste, einschließlich der Zertifizierung oder Akkreditierung, zu berücksichtigen sind;

b) Gewährleistung des Schutzes der wesentlichen Sicherheitsinteressen der Union und ihrer Mitgliedstaaten;

c) Gewährleistung, dass die EU-Cybersicherheitsreserve einen EU-Mehrwert erbringt, indem sie zu den in Artikel 3 der Verordnung (EU) 2021/694 gesetzten Zielen beiträgt, einschließlich der Förderung der Entwicklung von Cybersicherheitskompetenzen in der EU.

(2) Zur Beschaffung von Diensten für die EU-Cybersicherheitsreserve nimmt der öffentliche Auftraggeber die folgenden Auswahlkriterien in die Beschaffungsunterlagen auf:

a) Der Anbieter weist nach, dass sein Personal über ein Höchstmaß an beruflicher Integrität, Unabhängigkeit, Verantwortungsbewusstsein und die erforderlichen fachlichen Kompetenzen verfügt, um die Tätigkeiten in seinem betreffenden Bereich durchzuführen, und er gewährleistet die Dauerhaftigkeit/Kontinuität des Fachwissens sowie die erforderlichen technischen Ressourcen.

b) Der Anbieter, seine Tochterunternehmen und seine Unterauftragnehmer verfügen über einen Rahmen zum Schutz sensibler Informationen in Bezug auf den Dienst, insbesondere von Beweismitteln, Erkenntnissen und Berichten, und befolgt die Sicherheitsvorschriften der Union für den Schutz von EU-Verschlusssachen.

c) Der Anbieter weist hinreichend nach, dass seine Leitungsstruktur transparent ist und dass sie nicht geeignet ist, seine Unparteilichkeit und die Qualität seiner Dienstleistungen zu beeinträchtigen oder Interessenkonflikte zu verursachen.

d) Der Anbieter verfügt über eine angemessene Sicherheitsüberprüfung, zumindest für das Personal, das für den Betrieb des Dienstes bestimmt ist.

e) Der Anbieter gewährleistet das entsprechende Sicherheitsniveau für seine IT-Systeme.

f) Der Anbieter verfügt über die technische Hardware- und Softwareausrüstung, die zur Unterstützung des angeforderten Dienstes erforderlich ist.

g) Der Anbieter kann seine Erfahrung mit der Erbringung ähnlicher Dienste für einschlägige nationale Behörden oder Einrichtungen, die in kritischen oder hochkritischen Sektoren tätig sind, nachweisen.

h) Der Anbieter kann den Dienst kurzfristig in dem/den Mitgliedstaat(en) erbringen, in dem/denen er ihn anbietet.

i) Der Anbieter kann den Dienst in der Sprache des/der Mitgliedstaat(en) erbringen, in dem/denen er ihn anbietet.

j) Sobald ein EU-Zertifizierungssystem für verwaltete Sicherheitsdienste gemäß der Verordnung (EU) 2019/881 besteht, wird der Anbieter nach diesem System zertifiziert.

Artikel 17

Unterstützung für Drittländer

(1) Drittländer können Unterstützung aus der EU-Cybersicherheitsreserve beantragen, wenn die Assoziierungsabkommen über ihre Teilnahme am Programm Digitales Europa dies vorsehen.

(2) Die Unterstützung aus der EU-Cybersicherheitsreserve erfolgt im Einklang mit dieser Verordnung und unterliegt allen besonderen Bedingungen, die in den in Absatz 1 genannten Assoziierungsabkommen festgelegt sind.

(3) Zu den Nutzern aus assoziierten Drittländern, die Dienste aus der EU-Cybersicherheitsreserve in Anspruch nehmen können, gehören zuständige Behörden wie CSIRTs und Behörden für das Cyberkrisenmanagement.

(4) Jedes Drittland, das Unterstützung aus der EU-Cybersicherheitsreserve erhalten kann, benennt eine Behörde als zentrale Anlaufstelle für die Zwecke dieser Verordnung.

(5) Bevor sie Unterstützung aus der EU-Cybersicherheitsreserve erhalten, übermitteln Drittländer der Kommission und dem Hohen Vertreter Informationen über ihre Cyberresilienz- und Risikomanagementfähigkeiten, darunter zumindest Informationen über nationale Maßnahmen, die zur Vorbereitung auf schwerwiegende Cybersicherheitsvorfälle oder Cybersicherheitsvorfälle großen Ausmaßes getroffen wurden, sowie Informationen über ihre zuständigen nationalen Stellen, einschließlich CSIRTs oder gleichwertige Einrichtungen, deren Fähigkeiten und die ihnen zugewiesenen Ressourcen. Soweit sich Bestimmungen der Artikel 13 und 14 dieser Verordnung auf Mitgliedstaaten beziehen, gelten sie auch für Drittländer gemäß Absatz 1.

(6) Die Kommission stimmt sich mit dem Hohen Vertreter über die eingegangenen Anträge und die Umsetzung der Drittländern aus der EU-Cybersicherheitsreserve gewährten Unterstützung ab.

Kapitel IV

ÜBERPRÜFUNGSMECHANISMUS FÜR CYBERSICHERHEITSVORFÄLLE

Artikel 18

Überprüfungsmechanismus für Cybersicherheitsvorfälle

(1) Auf Ersuchen der Kommission, des EU-CyCLONe-Netzes oder des CSIRTs-Netzes nimmt die ENISA eine Überprüfung und Bewertung von Bedrohungen, Schwachstellen und Eindämmungsmaßnahmen im Zusammenhang mit einem bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes vor. Nach Abschluss der Überprüfung und Bewertung eines Sicherheitsvorfalls legt die ENISA dem CSIRTs-Netz, dem EU-CyCLONe-Netz und der Kommission einen Bericht über die Überprüfung des Sicherheitsvorfalls vor, um sie – insbesondere auch im Hinblick auf die in den Artikeln 15 und 16 der Richtlinie (EU) 2022/2555 festgelegten Aufgaben – bei der Wahrnehmung ihrer Aufgaben zu unterstützen. Soweit dies zweckmäßig ist, gibt die Kommission den Bericht an den Hohen Vertreter weiter.

(2) Bei der Erstellung des in Absatz 1 genannten Berichts über die Überprüfung des Sicherheitsvorfalls arbeitet die ENISA mit allen einschlägigen Beteiligten zusammen, darunter mit Vertretern der Mitgliedstaaten, der Kommission, anderen einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU, Anbietern verwalteter Sicherheitsdienste und Nutzern von Cybersicherheitsdiensten. Soweit dies zweckmäßig ist, arbeitet die ENISA auch mit Einrichtungen zusammen, die von schwerwiegenden Sicherheitsvorfällen oder Sicherheitsvorfällen großen Ausmaßes betroffen sind. Zur Unterstützung der Überprüfung kann die ENISA auch andere Arten von Interessenträgern befragen. Befragte Vertreter müssen etwaige Interessenkonflikte offenlegen.

(3) Der Bericht enthält eine Überprüfung und Analyse des konkreten schwerwiegenden Sicherheitsvorfalls oder Sicherheitsvorfalls großen Ausmaßes, einschließlich der Hauptursachen, Schwachstellen und gewonnenen Erkenntnisse. Vertrauliche Informationen sind im Einklang mit den Rechtsvorschriften der Union oder der Mitgliedstaaten über den Schutz vertraulicher oder als Verschlusssache eingestufter Informationen zu schützen.

(4) Gegebenenfalls enthält der Bericht Empfehlungen zur Verbesserung der Cyberabwehr der Union.

(5) Soweit möglich wird eine Fassung des Berichts öffentlich zugänglich gemacht. Diese Fassung darf nur öffentliche Informationen enthalten.

Kapitel V

SCHLUSSBESTIMMUNGEN

Artikel 19

Änderungen der Verordnung (EU) 2021/694

Die Verordnung (EU) 2021/694 wird wie folgt geändert:

1. Artikel 6 wird wie folgt geändert:

   a) Absatz 1 wird wie folgt geändert:

   1. Folgender Buchstabe aa wird eingefügt:

   „aa) Unterstützung des Aufbaus eines EU-Cyberschutzschilds, einschließlich der Entwicklung, der Einführung und des Betriebs nationaler und grenzübergreifender SOC-Plattformen, die zur Lageerfassung in der Union und zur Erweiterung der Kapazitäten der Union zur Gewinnung von Erkenntnissen über Cyberbedrohungen beitragen;“

   2. Folgender Buchstabe g wird angefügt:

   „g) Einrichtung und Betrieb eines Cybernotfallmechanismus zur Unterstützung der Mitgliedstaaten bei der Vorbereitung und Reaktion auf schwerwiegende Cybersicherheitsvorfälle, ergänzend zu nationalen Ressourcen und Kapazitäten und anderen auf Unionsebene verfügbaren Formen der Unterstützung, einschließlich der Einrichtung einer EU-Cybersicherheitsreserve.“

   b) Absatz 2 erhält folgende Fassung:

   „(2) Die Maßnahmen im Rahmen des spezifischen Ziels 3 werden in erster Linie durch das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und das Netz nationaler Koordinierungszentren gemäß der Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates[20] durchgeführt, mit Ausnahme der Maßnahmen zur Umsetzung der EU-Cybersicherheitsreserve, die von der Kommission und der ENISA durchgeführt werden.“

2. Artikel 9 wird wie folgt geändert:

   a) In Absatz 2 erhalten die Buchstaben b, c und d folgende Fassung:

   „b) 1 776 956 000 EUR für das spezifische Ziel 2 – Künstliche Intelligenz;

   c) 1 629 566 000 EUR für das spezifische Ziel 3 – Cybersicherheit und Vertrauen;

   d) 482 347 000 EUR für das spezifische Ziel 4 – Fortgeschrittene digitale Kompetenzen;“

[20] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1).

b) Folgender Absatz 8 wird angefügt:

„(8) Abweichend von Artikel 12 Absatz 4 der Verordnung (EU, Euratom) 2018/1046 werden nicht verwendete Mittel für Verpflichtungen und Zahlungen, die für Maßnahmen zur Verfolgung der in Artikel 6 Absatz 1 Buchstabe g der vorliegenden Verordnung genannten Ziele vorgesehen sind, automatisch übertragen und können bis zum 31. Dezember des folgenden Haushaltsjahres gebunden und ausgezahlt werden."

3. Artikel 14 Absatz 2 erhält folgende Fassung:

„(2) Im Rahmen des Programms können Mittel in allen in der Haushaltsordnung vorgesehenen Formen zur Verfügung gestellt werden, insbesondere durch Auftragsvergabe – als primärer Form – oder als Finanzhilfen und Preisgelder.

Erfordert die Erreichung des Ziels einer Maßnahme die Beschaffung innovativer Güter und Dienstleistungen, so dürfen Finanzhilfen nur Begünstigten gewährt werden, die Auftraggeber oder öffentliche Auftraggeber im Sinne der Richtlinien 2014/24/EU[27] und 2014/25/EU[28] des Europäischen Parlaments und des Rates sind.

Ist die Bereitstellung innovativer Güter oder Dienstleistungen, die noch nicht in großem Umfang kommerziell verfügbar sind, für die Erreichung der Ziele einer Maßnahme erforderlich, so kann der Auftraggeber oder öffentliche Auftraggeber die Vergabe mehrerer Aufträge im Rahmen desselben Vergabeverfahrens genehmigen.

Der Auftraggeber oder öffentliche Auftraggeber kann aus hinreichend gerechtfertigten Gründen der öffentlichen Sicherheit verlangen, dass der Erfüllungsort des Auftrags im Gebiet der Union liegt.

Bei der Durchführung von Vergabeverfahren für die mit Artikel 12 der Verordnung (EU) 2023/XX eingerichtete EU-Cybersicherheitsreserve können die Kommission und die ENISA als zentrale Beschaffungsstelle auftreten, um Aufträge anstelle oder im Namen von mit dem Programm assoziierten Drittländern gemäß Artikel 10 zu vergeben. Die Kommission und die ENISA können auch als Großhändler auftreten, indem sie Güter und Dienstleistungen zugunsten dieser Drittländer einkaufen, lagern und weiterverkaufen oder spenden oder vermieten. Abweichend von Artikel 169 Absatz 3 der Verordnung (EU) XXX/XXXX [Neufassung der Haushaltsordnung] reicht hierzu der Antrag eines einzigen Drittlands als Handlungsauftrag für die Kommission oder die ENISA aus.

Bei der Durchführung von Vergabeverfahren für die mit Artikel 12 der Verordnung (EU) 2023/XX eingerichtete EU-Cybersicherheitsreserve können die Kommission und die ENISA als zentrale Beschaffungsstelle auftreten, um Aufträge anstelle oder im Namen von Organen, Einrichtungen und sonstigen Stellen der Union zu vergeben. Die Kommission und die ENISA können auch als Großhändler auftreten, indem sie Güter und Dienstleistungen zugunsten der Organe, Einrichtungen und sonstigen Stellen der Union einkaufen, lagern und weiterverkaufen oder spenden oder vermieten. Abweichend von Artikel 169 Absatz 3 der Verordnung (EU) XXX/XXXX [Neufassung der Haushaltsordnung] reicht hierzu der Antrag eines einzigen Organs, einer Einrichtung oder einer sonstigen Stelle der Union als Handlungsauftrag für die Kommission oder die ENISA aus.

Ferner können durch das Programm Finanzierungen in Form von Finanzierungsinstrumenten im Rahmen von Mischfinanzierungsmaßnahmen bereitgestellt werden."

4. Der folgende Artikel 16a wird eingefügt:

„Für Maßnahmen zur Umsetzung des mit Artikel 3 der Verordnung (EU) 2023/XX eingerichteten europäischen Cyberschutzschilds gelten die Vorschriften der Artikel 4 und 5 der Verordnung (EU) 2023/XX. Im Falle eines Konflikts zwischen den Bestimmungen der vorliegenden Verordnung und denen der Artikel 4 und 5 der Verordnung (EU) 2023/XX gehen letztere Bestimmungen vor und finden auf diese spezifischen Maßnahmen Anwendung.“

5. Artikel 19 erhält folgende Fassung:

„Finanzhilfen im Rahmen des Programms werden nach Maßgabe des Titels VIII der Haushaltsordnung gewährt und verwaltet und können bis zu 100 % der förderfähigen Kosten decken, unbeschadet des Kofinanzierungsgrundsatzes gemäß Artikel 190 der Haushaltsordnung. Solche Finanzhilfen werden entsprechend den Vorgaben für jedes spezifische Ziel gewährt und verwaltet.

Unterstützung in Form von Finanzhilfen kann den in Artikel 4 der Verordnung (EU) XXXX genannten nationalen SOCs und dem in Artikel 5 der Verordnung (EU) XXXX genannten Aufnahmekonsortium im Einklang mit Artikel 195 Absatz 1 Buchstabe d der Haushaltsordnung ohne Aufforderung zur Einreichung von Vorschlägen vom ECCC direkt gewährt werden.

Unterstützung in Form von Finanzhilfen für den in Artikel 10 der Verordnung (EU) XXXX genannten Cybernotfallmechanismus kann den Mitgliedstaaten im Einklang mit Artikel 195 Absatz 1 Buchstabe d der Haushaltsordnung ohne Aufforderung zur Einreichung von Vorschlägen vom ECCC direkt gewährt werden.

Bei Maßnahmen gemäß Artikel 10 Absatz 1 Buchstabe c der Verordnung (EU) 202X/XXXX unterrichtet das ECCC die Kommission und die ENISA über Anträge der Mitgliedstaaten auf Gewährung direkter Finanzhilfen ohne Aufforderung zur Einreichung von Vorschlägen.

Im Falle der Unterstützung der gegenseitigen Amtshilfe bei der Reaktion auf einen schwerwiegenden Cybersicherheitsvorfall oder einen Cybersicherheitsvorfall großen Ausmaßes gemäß Artikel 10 Buchstabe c der Verordnung (EU) XXXX können die Kosten im Einklang mit Artikel 193 Absatz 2 Unterabsatz 2 Buchstabe a der Haushaltsordnung in hinreichend begründeten Fällen auch dann als förderfähig betrachtet werden, wenn sie vor der Einreichung des Finanzhilfeantrags entstanden sind.“

6. Die Anhänge I und II werden gemäß dem Anhang der vorliegenden Verordnung geändert.

Artikel 20

Bewertung

Bis zum [vier Jahre nach dem Datum des Geltungsbeginns dieser Verordnung] legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor.

Artikel 21

Ausschussverfahren

(1) Die Kommission wird von dem durch die Verordnung (EU) 2021/694 eingesetzten Koordinierungsausschuss für das Programm Digitales Europa unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Artikel 22

Inkrafttreten

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.

Geschehen zu Straßburg am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident/Die Präsidentin*

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

1.2. Politikbereich(e)

1.3. Der Vorschlag/Die Initiative betrifft

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

1.4.2. Einzelziel(e)

1.4.3. Erwartete Ergebnisse und Auswirkungen

1.4.4. Leistungsindikatoren

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größere Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union“ den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

1.7. Vorgeschlagene Haushaltsvollzugsart(en)

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

2.3. Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

3.2.3.1. Geschätzter Personalbedarf

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

3.2.5. Finanzierungsbeteiligung Dritter

3.3. Geschätzte Auswirkungen auf die Einnahmen

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Verordnung des Europäischen Parlaments und des Rates über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen

1.2. Politikbereich(e)

Ein Europa für das digitale Zeitalter

Strategische Investitionen der EU

Tätigkeit: Gestaltung der digitalen Zukunft Europas

1.3. Der Vorschlag/Die Initiative betrifft

☒ eine neue Maßnahme

☐ eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme[33]

☐ die Verlängerung einer bestehenden Maßnahme

☐ die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

Das Cybersolidaritätsgesetz soll die Solidarität auf Unionsebene stärken, um die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen zu verbessern. Seine Ziele sind die Folgenden:

a) Stärkung der gemeinsamen Erkennung und Lageerfassung der EU im Bereich der Cyberbedrohungen und -vorfälle;

b) Stärkung der Abwehrbereitschaft kritischer Einrichtungen in der gesamten EU und Stärkung der Solidarität durch den Aufbau gemeinsamer Kapazitäten für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, indem u. a. die Unterstützung für die Bewältigung auch Drittländern, die mit dem Programm Digitales Europa (DEP) assoziiert sind, zur Verfügung gestellt wird;

c) Stärkung der Abwehrfähigkeit der Union und Leistung eines Beitrags zu einer wirksamen Bewältigung durch die Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes, einschließlich der Gewinnung von Erkenntnissen und gegebenenfalls der Formulierung von Empfehlungen.

[33] Im Sinne des Artikels 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

1.4.2. Einzelziel(e)

Die Ziele des Cybersolidaritätsgesetzes werden durch folgende Maßnahmen verwirklicht:

a) Aufbau einer europaweiten Infrastruktur von Sicherheitseinsatzzentren („europäischer Cyberschutzschild“), um gemeinsame Fähigkeiten zur Erkennung und Lageerfassung aufzubauen und zu verbessern;

b) Schaffung eines Cybernotfallmechanismus zur Unterstützung der Mitgliedstaaten bei der Vorsorge für, Bewältigung von und sofortigen Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes. Auch die Organe, Einrichtungen und sonstigen Stellen der Union werden Unterstützung für die Bewältigung von Vorfällen erhalten.

Diese Maßnahmen werden durch Mittel aus dem Programm Digitales Europa gefördert, das durch dieses Rechtsinstrument geändert wird, um die oben genannten Maßnahmen festzulegen, finanzielle Unterstützung für ihre Entwicklung bereitzustellen und die Bedingungen für die Inanspruchnahme der finanziellen Unterstützung zu präzisieren.

c) Einrichtung eines europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle zur Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes.

1.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppe auswirken dürfte.

Die vorgeschlagene Verordnung würde den verschiedenen Beteiligten erhebliche Vorteile bringen. Der Europäische Cyberschutzschild wird die Fähigkeiten der Mitgliedstaaten zur Erkennung von Cyberbedrohungen verbessern. Der Cybernotfallmechanismus wird die Maßnahmen der Mitgliedstaaten durch eine Soforthilfe bei der Abwehrbereitschaft, Reaktion und sofortigen Wiederherstellung bzw. Wiederaufnahme des Betriebs wesentlicher Dienste ergänzen.

Diese Maßnahmen sollen die Wettbewerbsposition der Branche und der Unternehmen in der gesamten digitalisierten Wirtschaft in Europa stärken und ihren digitalen Wandel vorantreiben, indem das Cybersicherheitsniveau im digitalen Binnenmarkt erhöht wird. Die Verordnung zielt insbesondere darauf ab, die Widerstandsfähigkeit der Bürgerinnen und Bürger, der Unternehmen und der in kritischen oder hochkritischen Sektoren tätigen Einrichtungen gegenüber den zunehmenden Bedrohungen der Cybersicherheit zu erhöhen, die verheerende gesellschaftliche und wirtschaftliche Auswirkungen haben können. Dazu sind insbesondere Investitionen in Instrumente vorgesehen, die eine schnellere Erkennung von Cybersicherheitsbedrohungen und -vorfällen und eine schnellere Reaktion darauf unterstützen; gleichzeitig wird den Mitgliedstaaten geholfen ihre Vorsorgemaßnahmen und ihre Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes zu verbessern. Dies wird auch dazu beitragen, dass die Union ihre Kapazitäten in diesen Bereichen ausbaut, insbesondere in Bezug auf die Erhebung und Analyse von Daten über Cybersicherheitsbedrohungen und -vorfälle.

1.4.4. Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Fortschritte und Ergebnisse verfolgen lassen.

Im Hinblick auf die Förderung der Solidarität auf Unionsebene könnten mehrere Indikatoren berücksichtigt werden:

1. Anzahl der gemeinsam beschafften Cybersicherheitsinfrastrukturen oder -werkzeuge oder beider
2. Anzahl der Maßnahmen zur Unterstützung der Abwehrbereitschaft und der Reaktion auf Cybersicherheitsvorfälle im Rahmen des Cybernotfallmechanismus.

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

Die Verordnung soll kurz nach ihrer Annahme, also am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union uneingeschränkt in Kraft treten.

1.5.2. Mehrwert aufgrund des Tätigwerdens der Union (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größere Wirksamkeit oder Komplementarität). Für die Zwecke dieser Nummer bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der Union" den Wert, der sich aus dem Tätigwerden der Union ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

Aufgrund des ausgeprägten grenzübergreifenden Charakters von Cybersicherheitsbedrohungen im Allgemeinen und der zunehmenden Zahl der Risiken und Sicherheitsvorfälle, die sich über Grenzen, Sektoren und Produkte hinweg auswirken, können die Ziele der vorliegenden Maßnahme von den Mitgliedstaaten allein nicht wirksam erreicht werden und erfordern ein gemeinsames Vorgehen und Solidarität auf Unionsebene. Die Erfahrungen mit der Abwehr von Cyberbedrohungen, die sich aus dem Krieg gegen die Ukraine ergeben, sowie die Lehren aus einer unter französischem Ratsvorsitz durchgeführten Cybersicherheitsübung (EU CyCLES) haben gezeigt, dass konkrete Mechanismen zur gegenseitigen Unterstützung, insbesondere für die Zusammenarbeit mit dem Privatsektor, entwickelt werden sollten, um Solidarität auf EU-Ebene zu erreichen. Vor diesem Hintergrund wurde die Kommission in den Schlussfolgerungen des Rates vom 23. Mai 2022 zur Entwicklung der Cyberabwehr der Europäischen Union aufgefordert, einen Vorschlag für einen neuen Cybersicherheits-Notfallfonds vorzulegen. Unterstützung und Maßnahmen zur besseren Erkennung von Cybersicherheitsbedrohungen auf Unionsebene und zur Erhöhung der Abwehrbereitschaft und Reaktionskapazitäten stellen einen Mehrwert dar, da so Doppelarbeit in der gesamten Union und in den Mitgliedstaaten vermieden werden kann. Dies würde zu einer besseren Nutzung der vorhandenen Ressourcen, einer besseren Koordinierung und einem besseren Informationsaustausch über gewonnene Erkenntnisse führen.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

In Bezug auf die Lageerfassung und Erkennung unter dem europäischen Cyberschutzschild wurden im Rahmen des Arbeitsprogramms des DEP für Cybersicherheit 2021–2022 eine Aufforderung zur Interessenbekundung für die gemeinsame Beschaffung von Instrumenten und Infrastrukturen für die Einrichtung grenzübergreifender SOCs und eine Aufforderung zur Beantragung von Finanzhilfen für den Kapazitätsaufbau der SOCs, die im Dienste öffentlicher und privater Organisationen stehen, durchgeführt.

Im Hinblick auf die Abwehrbereitschaft und die Bewältigung von Vorfällen hat die Kommission ein kurzfristiges Unterstützungsprogramm für die Mitgliedstaaten aufgestellt und der ENISA zusätzliche Mittel zugewiesen, um die Abwehrbereitschaft und Reaktionsfähigkeit bei großen Cybersicherheitsvorfällen unverzüglich zu stärken. Die Unterstützungsdienste im Rahmen des Programms umfassen Vorsorgemaßnahmen, wie Penetrationstests kritischer Einrichtungen zur Ermittlung von Schwachstellen. Außerdem sieht das Programm zusätzliche Möglichkeiten vor, um Mitgliedstaaten im Falle eines schwerwiegenden Sicherheitsvorfalls bei einer kritischen Einrichtung zu unterstützen. Die Umsetzung dieses kurzfristigen Programms durch die ENISA ist im Gange und hat bereits wertvolle einschlägige Erkenntnisse hervorgebracht, die bei der Ausarbeitung dieser Verordnung berücksichtigt wurden.

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

Das Cybersolidaritätsgesetz wird auf Maßnahmen aufbauen, die bereits von der Union und den Mitgliedstaaten unterstützt werden, um die Lageerfassung und die Erkennung von Cyberbedrohungen zu verbessern und auf grenzüberschreitende Cybersicherheitsvorfälle großen Ausmaßes zu reagieren. Darüber hinaus steht das Instrument im Einklang mit anderen Krisenmanagementrahmen wie der Integrierten Regelung für die politische Reaktion auf Krisen (IPCR), der Gemeinsamen Sicherheits- und Verteidigungspolitik, einschließlich der Teams für die rasche Reaktion auf Cybervorfälle, und der Unterstützung, die ein Mitgliedstaat einem anderen Mitgliedstaat im Rahmen des Artikels 42 Absatz 7 des Vertrags über die Europäische Union gewährt. Der neue Vorschlag würde auch Strukturen ergänzen und unterstützen, die im Rahmen anderer Cybersicherheitsinstrumente wie der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) oder der Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit) aufgebaut worden sind.

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

Das Management der Handlungsbereiche, die der ENISA zugewiesen werden, passt zu ihrem bestehenden Mandat und gehört zu ihren bestehenden allgemeinen Aufgaben. Diese Handlungsbereiche machen möglicherweise spezifische Profile oder neue Aufgabenstellungen erforderlich, die sich aber mit den vorhandenen Ressourcen der ENISA durch Neuzuweisungen oder Verknüpfungen verschiedener Aufgaben abdecken lassen. Die ENISA führt derzeit ein kurzfristiges Programm durch, das im Jahr 2022 von der Kommission aufgestellt wurde, um die Abwehrbereitschaft und Reaktionsfähigkeit bei großen Cybersicherheitsvorfällen unverzüglich zu stärken. Die vorgesehenen Dienste bieten Möglichkeiten, um Mitgliedstaaten im Falle eines schwerwiegenden Sicherheitsvorfalls bei einer

kritischen Einrichtung zu unterstützen. Die Umsetzung dieses kurzfristigen Programms durch die ENISA ist im Gange und hat bereits wertvolle einschlägige Erkenntnisse hervorgebracht, die bei der Ausarbeitung dieser Verordnung berücksichtigt wurden. Die für das kurzfristige Programm zugewiesenen Ressourcen könnten auch im Zusammenhang mit dieser Verordnung verwendet werden.

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

☒ **befristete Laufzeit**

– ☒ gilt ab dem Datum der Annahme des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zur Stärkung der Solidarität und der Kapazitäten in der Union zur Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen („Cybersolidaritätsgesetz“)

– ☒ Finanzielle Auswirkungen auf die Mittel für Verpflichtungen von 2023 bis 2027 und auf die Mittel für Zahlungen von 2023 bis 2031[34]

☐ **unbefristete Laufzeit**

– Anlaufphase von JJJJ bis JJJJ,

– anschließend reguläre Umsetzung.

1.7. Vorgeschlagene Haushaltsvollzugsart(en)[35]

☒ **Direkte Mittelverwaltung** durch die Kommission

– ☒ durch ihre Dienststellen, einschließlich ihres Personals in den Delegationen der Union

– ☐ durch Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

☒ **Indirekte Mittelverwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

– ☐ Drittländer oder die von ihnen benannten Einrichtungen

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

– ☐ die EIB und den Europäischen Investitionsfonds

– ☒ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

– ☐ öffentlich-rechtliche Körperschaften

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern ihnen ausreichende finanzielle Garantien bereitgestellt werden

– ☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und denen ausreichende finanzielle Garantien bereitgestellt werden

---

34 Die in der Verordnung vorgesehenen Maßnahmen sollten auch durch den nächsten mehrjährigen Finanzrahmen getragen werden.

35 Erläuterungen zu den Haushaltsvollzugsarten und Verweise auf die Haushaltsordnung finden sich auf der Website BUDGpedia (in englischer Sprache): https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

– ☐ Einrichtungen oder Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der GASP im Rahmen des Titels V EUV betraut und in dem maßgeblichen Basisrechtsakt benannt sind

– *Falls mehrere Methoden der Mittelverwaltung angegeben werden, ist dies unter „Bemerkungen" näher zu erläutern.*

Bemerkungen

Die Maßnahmen in Bezug auf den europäischen Cyberschutzschild werden vom ECCC durchgeführt. Bis das ECCC in der Lage ist, seinen eigenen Haushalt auszuführen, wird die Europäische Kommission die Maßnahmen in direkter Mittelverwaltung im Namen des ECCC durchführen. Das ECCC kann auf der Grundlage von Aufforderungen zur Interessenbekundung Einrichtungen zur Teilnahme an der gemeinsamen Beschaffung von Instrumenten auswählen. Das ECCC kann Finanzhilfen für den Betrieb dieser Instrumente gewähren.

Darüber hinaus kann das ECCC Finanzhilfen für Vorsorgemaßnahmen im Rahmen des Cybernotfallmechanismus gewähren.

Die Kommission trägt die Gesamtverantwortung für die Umsetzung der EU-Cybersicherheitsreserve. Die Kommission kann die ENISA ganz oder teilweise im Wege von Beitragsvereinbarungen mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve betrauen. Die der ENISA mit dieser Verordnung übertragenen Maßnahmen stehen im Einklang mit ihrem bestehenden Mandat. Diese Maßnahmen umfassen Folgendes: i) Unterstützung der NIS-Kooperationsgruppe bei der Entwicklung der Vorsorgemaßnahmen entsprechend den Risikobewertungen; ii) Unterstützung der Kommission bei der Einrichtung und Überwachung der Umsetzung der EU-Cybersicherheitsreserve, einschließlich der Entgegennahme und Bearbeitung von Unterstützungsanträgen; iii) Ausarbeitung von Musterformularen zur leichteren Beantragung von Unterstützung aus der EU-Cybersicherheitsreserve und von Mustervereinbarungen zwischen dem Diensteanbieter und dem Nutzer, dem die Unterstützung aus der EU-Cybersicherheitsreserve gewährt werden soll; iv) Überprüfung und Bewertung von Bedrohungen, Schwachstellen und Eindämmungsmaßnahmen im Zusammenhang mit einem bestimmten schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes und Erstellung entsprechender Berichte.

Der Umfang aller dieser Aufträge wird auf etwa 7 VZÄ geschätzt, die aus den bestehenden Ressourcen der ENISA bereitzustellen sind, wobei auf vorhandenes Fachwissen und vorbereitende Arbeiten zurückgegriffen wird, die von der ENISA im Pilotprojekt für die Soforthilfe bei der Abwehrbereitschaft und Bewältigung von Vorfällen bereits durchgeführt werden.

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Die Kommission wird die Durchführung, Anwendung und Einhaltung dieser neuen Bestimmungen überwachen, um auch deren Wirksamkeit zu bewerten. Spätestens vier Jahre nach dem Geltungsbeginn dieser Verordnung wird die Kommission dem Europäischen Parlament und dem Rat einen Bericht über ihre Bewertung und Überprüfung vorlegen.

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Methode(n) der Mittelverwaltung, des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

Mit der Verordnung wird ein Rahmen für die Verwendung von EU-Mitteln geschaffen, um die Resilienz im Bereich der Cybersicherheit durch Maßnahmen zur Verbesserung der Erkennungs-, Reaktions- und Wiederherstellungsfähigkeiten bei schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu verbessern. Die für diesen Politikbereich zuständigen Referate der GD CNECT werden die Umsetzung der Richtlinie verwalten.

Um den neuen Aufgaben gerecht zu werden, müssen die Dienststellen der Kommission angemessen mit Ressourcen ausgestattet werden. Für die Durchsetzung der neuen Verordnung werden schätzungsweise 6 VZÄ (3 AD und 3 VB) benötigt, um folgende Aufgaben wahrzunehmen:

- Festlegung von Vorsorgemaßnahmen entsprechend den Risikobewertungen;
- Gewährleistung der Interoperabilität zwischen grenzübergreifenden SOC-Plattformen;
- Ausarbeitung möglicher Durchführungsrechtsakte (zwei für SOCs und zwei für den Cybernotfallmechanismus);
- Verwaltung der Aufnahme- und Nutzungsvereinbarungen für SOCs;
- Einrichtung und Verwaltung der EU-Cybersicherheitsreserve, entweder direkt oder über eine Beitragsvereinbarung mit der ENISA; im Falle einer Beitragsvereinbarung mit der ENISA: Ausarbeitung und Überwachung der Durchführung der Beitragsvereinbarung für die der ENISA übertragenen Aufgaben;
- Mitarbeit in den von der ENISA einberufenen Konsultationsgruppen zur Überprüfung und Bewertung von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfälle großen Ausmaßes und zur Vorbereitung der Berichte.

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

Ein für den europäischen Cyberschutzschild ermitteltes Risiko besteht darin, dass die Mitgliedstaaten innerhalb der grenzübergreifenden SOC-Plattformen oder zwischen grenzübergreifenden Plattformen und anderen einschlägigen Einrichtungen auf EU-

Ebene keine Informationen über Cyberbedrohungen in ausreichender Menge austauschen. Um diesem Risiko entgegenzuwirken, erfolgt die Mittelzuweisung im Anschluss an eine Aufforderung zur Interessenbekundung, bei der sich die Mitgliedstaaten verpflichten müssen, eine bestimmte Menge an Informationen an die EU-Ebene weiterzugeben. Diese Verpflichtung wird dann in einer Aufnahme- und Nutzungsvereinbarung formalisiert, die dem ECCC die Befugnis gibt, Prüfungen durchzuführen, damit die gemeinsam beschafften Instrumente und Infrastrukturen im Einklang mit der Vereinbarung verwendet werden. Die Verpflichtung zu einem umfangreichen Informationsaustausch innerhalb der grenzübergreifenden SOCs wird in einer Konsortialvereinbarung formalisiert.

Ein Risiko für den Cybernotfallmechanismus besteht darin, dass die am Mechanismus beteiligten Nutzer nicht genügend Maßnahmen ergreifen, um die Abwehrbereitschaft gegenüber Cyberangriffen zu gewährleisten. Deshalb müssen die Nutzer solche Vorsorgemaßnahmen ergreifen, um Unterstützung aus der EU-Cybersicherheitsreserve erhalten zu können. Bei der Beantragung der Unterstützung aus der EU-Cybersicherheitsreserve müssen die Nutzer erläutern, welche Maßnahmen bereits ergriffen wurden, um auf Vorfälle zu reagieren, was dann bei der Bewertung der Anträge an die EU-Cybersicherheitsreserve berücksichtigt wird.

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

Da die für die Unterstützung nach dem Cybersolidaritätsgesetz geltenden Regeln für die Beteiligung am Programm Digitales Europa denen ähneln, die die Kommission in ihren Arbeitsprogrammen anwenden wird, und die Gruppe der Empfänger ein ähnliches Risikoprofil wie bei Programmen mit direkter Mittelverwaltung aufweist, kann davon ausgegangen werden, dass die Fehlermarge in etwa derjenigen entspricht, die die Kommission für das Programm Digitales Europa vorgesehen hat (d. h. dass hinreichend Gewähr dafür besteht, dass das Fehlerrisiko über den gesamten mehrjährigen Ausgabenzeitraum zwischen 2 und 5 % jährlich liegen wird), wobei letztlich angestrebt wird, zum Abschluss der mehrjährigen Programme eine Restfehlerquote möglichst nahe bei 2 % zu erreichen, nachdem die finanziellen Auswirkungen aller Audits sowie Korrektur- und Erstattungsmaßnahmen berücksichtigt worden sind.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen, z. B. im Rahmen der Betrugsbekämpfungsstrategie, bereits bestehen oder angedacht sind.

Im Falle des Europäischen Cyberschutzschilds wird das ECCC befugt sein, Prüfungen in Bezug auf gemeinsam beschaffte Instrumente und Infrastrukturen anhand des Zugangs zu Informationen und mithilfe von Vor-Ort-Kontrollen entsprechend der zwischen dem Aufnahmekonsortium und dem ECCC zu unterzeichnenden Aufnahme- und Nutzungsvereinbarung durchzuführen.

Die für die Organe, Einrichtungen und sonstigen Stellen der Union geltenden Betrugsbekämpfungsmaßnahmen gelten auch für die zusätzlichen Mittel, die für diese Verordnung erforderlich werden.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

- Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer	GM/ NGM[36]	von EFTA-Ländern[37]	von Kandidatenländern und potenziellen Kandidaten[38]	von anderen Drittländern	andere zweckgebundene Einnahmen
1	02 04 01 10 – Programm Digitales Europa – Cybersicherheit	GM	JA	JA	NEIN	NEIN
1	02 04 01 11 – Programm Digitales Europa – Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung	GM	JA	JA	NEIN	NEIN
1	02 04 03 – Programm Digitales Europa – Künstliche Intelligenz	GM	JA	JA	NEIN	NEIN
1	02 04 04 – Programm Digitales Europa – Kompetenzen	GM	JA	JA	NEIN	NEIN
1	02 01 30 – Unterstützungsausgaben für das Programm Digitales Europa	NGM	JA	JA	NEIN	NEIN

[36] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.
[37] EFTA: Europäische Freihandelsassoziation.
[38] Kandidatenländer und gegebenenfalls potenzielle Kandidaten.

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

– ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	Nummer	1 **Binnenmarkt, Innovation und Digitales**

Durch den Vorschlag wird die Gesamthöhe der Verpflichtungen im Rahmen des Programms Digitales Europa nicht erhöht. Der Beitrag zu dieser Initiative ergibt sich aus einer Umverteilung der Mittelbindungen für die spezifischen Ziele SO2 und SO4 zur Aufstockung der Haushaltsmittel für das spezifische Ziel SO3 und das ECCC. Jede Erhöhung der Mittel für Verpflichtungen im Rahmen des Programms Digitales Europa, die sich aus einer Überarbeitung des MFR ergibt, könnte für die Zwecke dieser Initiative verwendet werden.

GD CONNECT			Jahr **2025**	Jahr **2026**	Jahr **2027**	Jahr **2028+**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			**INSGESAMT**
○ Operative Mittel										
Haushaltslinie[39] 02 04 01 10 (Umverteilung von 02 04 03 und 02 04 04)	Verpflichtungen	(1a)	15,000	15,000	6,000	z. E.				**36,000**
	Zahlungen	(2a)	15,000	15,000	6,000					**36,000**
Haushaltslinie 02 04 01 11 02 (Umverteilung von 02 04 03 und 02 04 04)	Verpflichtungen	(1b)	13,000	23,000	28,000	z. E.				**64,000**
	Zahlungen	(2b)	8,450	18,200	25,250	12,100				**64,000**
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben[40]										
Haushaltslinie 02 01 30		(3)	0,150	0,150	0,150	z. E.				0,450
Mittel INSGESAMT	Verpflichtungen	=1a+1b +3	**28,150**	**38,150**	**34,150**	**z. E.**				**100,450**

[39] Gemäß dem offiziellen Eingliederungsplan.

[40] Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

für die GD CONNECT	Zahlungen	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ Operative Mittel INSGESAMT	Verpflichtungen	(4)	28,000	38,000	34,000	z. E.				**100,000**
	Zahlungen	(5)	23,450	33,200	31,250	12,100				**100,000**
○ Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)	0,150	0,150	0,150	z. E.				**0,450**
Mittel INSGESAMT unter der RUBRIK 1 des Mehrjährigen Finanzrahmens	Verpflichtungen	=4+6	**28,150**	**38,150**	**34,150**	**z. E.**				**100,450**
	Zahlungen	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Wenn der Vorschlag/die Initiative mehrere operative Rubriken betrifft, ist der vorstehende Abschnitt zu wiederholen:

○ Operative Mittel INSGESAMT (alle operativen Rubriken)	Verpflichtungen	(4)	28,000	38,000	34,000	z. E.				**100,000**
	Zahlungen	(5)	23,450	33,200	31,250	12,100				**100,000**
○ Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT (alle operativen Rubriken)		(6)	0,150	0,150	0,150					**0,450**
Mittel INSGESAMT unter den RUBRIKEN 1 bis 6 des Mehrjährigen Finanzrahmens (Referenzbetrag)	Verpflichtungen	=4+6	**28,150**	**38,150**	**34,150**	**z. E.**				**100,450**
	Zahlungen	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Rubrik des Mehrjährigen Finanzrahmens	7	Verwaltungsausgaben

Zum Ausfüllen dieses Teils ist die „Tabelle für Verwaltungsausgaben“ zu verwenden, die zuerst in den Anhang des Finanzbogens zu Rechtsakten (Anhang 5 des Beschlusses der Kommission über die internen Vorschriften für die Ausführung des Einzelplans Kommission des Gesamthaushaltsplans der Europäischen Union), der für die dienststellenübergreifende Konsultation in DECIDE hochgeladen wird, aufgenommen wird.

in Mio. EUR (3 Dezimalstellen)

		Jahr **2025**	Jahr **2026**	Jahr **2027**	Jahr **2028+**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			**INSGESAMT**
GD CONNECT									
○ Personal		0,786	0,786	0,786	z. E.				**2,358**
○ Sonstige Verwaltungsausgaben		0,035	0,035	0,035	z. E.				**0,105**
GD CONNECT INSGESAMT	Mittel	**0,821**	**0,821**	**0,821**					**2,463**

Mittel INSGESAMT unter der RUBRIK 7 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	**0,821**	**0,821**	**0,821**					**2,463**

in Mio. EUR (3 Dezimalstellen)

		Jahr **2025**	Jahr **2026**	Jahr **2027**	Jahr **2028+**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			**INSGESAMT**
Mittel INSGESAMT unter den RUBRIKEN 1 bis 7 des Mehrjährigen Finanzrahmens	Verpflichtungen	**28,971**	**38,971**	**34,971**	**z. E.**				**102,913**
	Zahlungen	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse angeben ⇩			Jahr **N**		Jahr **N+1**		Jahr **N+2**		Jahr **N+3**		Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.						**INSGESAMT**	
	ERGEBNISSE																	
	Art[41]	Durch-schnitts kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamt-zahl	Gesamt-kosten
EINZELZIEL Nr. 1[42] …																		
– Ergebnis																		
– Ergebnis																		
– Ergebnis																		
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2 …																		
– Ergebnis																		
Zwischensumme für Einzelziel Nr. 2																		
INSGESAMT																		

[41] Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Zahl der Austauschstudenten, gebaute Straßenkilometer…).

[42] Wie unter 1.4.2. „Einzelziel(e)…“ beschrieben.

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

– ☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr 2025	Jahr 2026	Jahr 2027	Jahr N+3	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			**INSGESAMT**
RUBRIK 7 des Mehrjährigen Finanzrahmens								
Personal	0,786	0,786	0,786					**2,358**
Sonstige Verwaltungsausgaben	0,035	0,035	0,035					**0,105**
Zwischensummer der RUBRIK 7 des Mehrjährigen Finanzrahmens	**0,821**	**0,821**	**0,821**					**2,463**

Außerhalb der RUBRIK 7[43] des Mehrjährigen Finanzrahmens								
Personal								
Sonstige Verwaltungsausgaben	0,150	0,150	0,150					**0,450**
Zwischensumme außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens	**0,150**	**0,150**	**0,150**					**0,450**

INSGESAMT	**0,971**	**0,971**	**0,971**					**2,913**

Der Mittelbedarf für Personal- und sonstige Verwaltungsausgaben wird durch der Verwaltung der Maßnahme zugeordnete Mittel der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

[43] Technische und/oder administrative Hilfe und Ausgaben zur Unterstützung der Durchführung von Programmen bzw. Maßnahmen der EU (vormalige BA-Linien), indirekte Forschung, direkte Forschung.

3.2.3.1. Geschätzter Personalbedarf

– ☐ Für den Vorschlag/die Initiative wird kein Personal benötigt.

– ☒ Für den Vorschlag/die Initiative wird folgendes Personal benötigt:

Schätzung in Vollzeitäquivalenten

		Jahr **2025**	Jahr **2026**	Jahr 2027	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
○ Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)								
20 01 02 01 (am Sitz und in den Vertretungen der Kommission)		3	3	3				
20 01 02 03 (in den Delegationen)								
01 01 01 01 (indirekte Forschung)								
01 01 01 11 (direkte Forschung)								
Sonstige Haushaltslinien (bitte angeben)								
○ Externes Personal (in Vollzeitäquivalenten – VZÄ)[44]								
20 02 01 (VB, ANS und LAK der Globaldotation)		3	3	3				
20 02 03 (VB, ÖB, ANS, LAK und JFD in den Delegationen)								
XX 01 xx **yy zz** [45]	– am Sitz							
	– in den Delegationen							
01 01 01 02 (VB, ANS und LAK der indirekten Forschung)								
01 01 01 12 (VB, ANS und LAK der direkten Forschung)								
Sonstige Haushaltslinien (bitte angeben)								
INSGESAMT		**6**	**6**	**6**				

XX steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumschichtung gedeckt. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

Beamte und Bedienstete auf Zeit	- Festlegung von Vorsorgemaßnahmen entsprechend den Risikobewertungen (Artikel 11), - Ausarbeitung möglicher Durchführungsrechtsakte (zwei für SOCs und zwei für den Cybernotfallmechanismus), - Verwaltung der Aufnahme- und Nutzungsvereinbarungen für SOCs, - Einrichtung und Verwaltung der EU-Cybersicherheitsreserve, entweder direkt oder über eine Beitragsvereinbarung mit der ENISA.
Externes Personal	unter der Aufsicht eines Beamten, - Festlegung von Vorsorgemaßnahmen entsprechend den Risikobewertungen (Artikel 11), - Ausarbeitung möglicher Durchführungsrechtsakte (zwei für SOCs und zwei für den Cybernotfallmechanismus), - Verwaltung der Aufnahme- und Nutzungsvereinbarungen für SOCs, - Einrichtung und Verwaltung der EU-Cybersicherheitsreserve, entweder direkt oder über eine Beitragsvereinbarung mit der ENISA.

[44] VB = Vertragsbedienstete, ÖB = örtliche Bedienstete, ANS = abgeordnete nationale Sachverständige, LAK = Leiharbeitskräfte, JFD = Juniorfachkräfte in Delegationen.

[45] Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

3.2.4. *Vereinbarkeit mit dem Mehrjährigen Finanzrahmen*

Der Vorschlag/Die Initiative

– [X] kann durch Umschichtungen innerhalb der entsprechenden Rubrik des Mehrjährigen Finanzrahmens (MFR) in voller Höhe finanziert werden.

Bitte erläutern Sie die erforderliche Neuprogrammierung unter Angabe der betreffenden Haushaltslinien und der entsprechenden Beträge. Bitte legen Sie im Falle einer größeren Neuprogrammierung eine Excel-Tabelle vor.

	2023	2024	2025	2026	2027	Insgesamt
SO1	16.232.897	20.528.765	17.406.899	16.223.464	10.022.366	80.414.391
SO2 anfänglich	226.316.819	295.067.000	195.649.000	221.809.000	246.608.000	1.185.449.819
Für CYBER-Initiative			18.000.000	28.000.000	19.000.000	65.000.000
NEU SO2	**226.316.819**	**295.067.000**	**177.649.000**	**193.809.000**	**227.608.000**	**1.120.449.819**
SO3 DB 24	24.361.553	35.596.172	3.638.000	3.638.000	11.175.000	78.408.725
Von SO2-SO4			15.000.000	15.000.000	6.000.000	36.000.000
NEU SO3	**24.361.553**	**35.596.172**	**18.638.000**	**18.638.000**	**17.175.000**	**114.408.725**
ECCC anfänglich	176.222.303	208.374.879	104.228.130	90.704.986	84.851.497	664.381.795
Von SO2-SO4			13.000.000	23.000.000	28.000.000	64.000.000
NEU ECCC	**176.222.303**	**208.374.879**	**117.228.130**	**113.704.986**	**112.851.497**	**728.381.795**
SO4 anfänglich	66.902.708	64.892.032	56.577.977	70.477.245	72.107.201	330.957.163
Für CYBER-Initiative			10.000.000	10.000.000	15.000.000	35.000.000
NEU SO4	**66.902.708**	**64.892.032**	**46.577.977**	**60.477.245**	**57.107.201**	**295.957.163**

– [ ] erfordert die Inanspruchnahme des verbleibenden Spielraums unter der einschlägigen Rubrik des MFR und/oder den Einsatz der besonderen Instrumente im Sinne der MFR-Verordnung.

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien, der entsprechenden Beträge und der vorgeschlagenen einzusetzenden Instrumente.

– [ ] erfordert eine Revision des MFR.

Bitte erläutern Sie den Bedarf unter Angabe der betreffenden Rubriken und Haushaltslinien sowie der entsprechenden Beträge.

3.2.5. *Finanzierungsbeteiligung Dritter*

Der Vorschlag/Die Initiative

– [X] sieht keine Kofinanzierung durch Dritte vor.

– [ ] sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr **N**[46]	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			Insgesamt
Kofinanzierende Einrichtung								
Kofinanzierung INSGESAMT								

3.3. Geschätzte Auswirkungen auf die Einnahmen

– ☒ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

– ☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar

  – ☐ auf die Eigenmittel

  – ☐ auf die übrigen Einnahmen

  – Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugewiesen sind. ☐

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[47]						
		Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
Artikel …								

Bitte geben Sie für die zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

[…]

Sonstige Anmerkungen (bei der Ermittlung der Auswirkungen auf die Einnahmen verwendete Methode/Formel oder weitere Informationen).

[…]

46 Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird. Bitte ersetzen Sie „N“ durch das voraussichtlich erste Jahr der Umsetzung (z. B. 2021). Dasselbe gilt für die folgenden Jahre.

47 Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.

EUROPÄISCHE
KOMMISSION

Straßburg, den 18.4.2023
COM(2023) 209 final

ANNEX

ANHANG

der

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen

ANHANG

Die Verordnung (EU) 2021/694 wird wie folgt geändert:

1. In Anhang I erhält der Abschnitt/das Kapitel „Spezifisches Ziel 3 – Cybersicherheit und Vertrauen“ folgende Fassung:

„Spezifisches Ziel 3 – Cybersicherheit und Vertrauen

Das Programm regt die Verstärkung, den Aufbau und den Erwerb grundlegender Kapazitäten zur Sicherung der digitalen Wirtschaft, Gesellschaft und Demokratie in der Union an, indem es das industrielle Potenzial und die Wettbewerbsfähigkeit der Union im Bereich der Cybersicherheit stärkt und die Kapazitäten der Privatwirtschaft und des öffentlichen Sektors zum Schutz der Bürger und Unternehmen vor Cyberbedrohungen verbessert, einschließlich durch Unterstützung bei der Umsetzung der Richtlinie (EU) 2016/1148.

Die anfänglichen und gegebenenfalls nachfolgenden Maßnahmen im Rahmen dieses Ziels umfassen Folgendes:

1. Koinvestitionen mit Mitgliedstaaten in fortgeschrittene Cybersicherheitsausrüstung und -infrastrukturen sowie Know-how im Bereich der Cybersicherheit, die für den Schutz kritischer Infrastrukturen und des digitalen Binnenmarkts insgesamt von wesentlicher Bedeutung sind. Solche Koinvestitionen könnten Investitionen in Quantencomputeranlagen und Datenressourcen für Cybersicherheit, die Lageerfassung im Cyberraum, ***einschließlich der nationalen SOCs und der grenzübergreifenden SOCs, die den europäischen Cyberschutzschild bilden***, sowie weitere Instrumente umfassen, die dem öffentlichen Sektor und der Privatwirtschaft in ganz Europa zugänglich zu machen sind;

2. Ausweitung der vorhandenen technologischen Kapazitäten und Vernetzung der Kompetenzzentren in den Mitgliedstaaten sowie Sicherstellung, dass diese Kapazitäten dem Bedarf des öffentlichen Sektors und der Industrie entsprechen, einschließlich durch Produkte und Dienstleistungen zur Stärkung der Cybersicherheit und des Vertrauens in den digitalen Binnenmarkt;

3. Sicherstellung einer breiten Einführung wirksamer moderner cybersicherheits- und vertrauensfördernder Lösungen in allen Mitgliedstaaten. Zu einer solchen Einführung gehört auch die Stärkung der Produktsicherheit vom Design bis zur Kommerzialisierung der Produkte;

4. Unterstützung bei der Schließung der Kompetenzlücke im Bereich der Cybersicherheit, z. B. durch die Angleichung der entsprechenden Qualifikationsprogramme, ihre Anpassung an die sektorspezifischen Bedürfnisse und die Erleichterung des Zugangs zu gezielten spezialisierten Schulungen.

5. ***Förderung der Solidarität zwischen den Mitgliedstaaten bei der Vorbereitung und Reaktion auf schwerwiegende Cybersicherheitsvorfälle durch eine grenzüberschreitende Einführung von Cybersicherheitsdiensten, einschließlich der Unterstützung der Amtshilfe zwischen Behörden und der Einrichtung einer Reserve vertrauenswürdiger Cybersicherheitsanbieter auf Unionsebene.***“

2. In Anhang II erhält der Abschnitt/das Kapitel „Spezifisches Ziel 3 – Cybersicherheit und Vertrauen“ folgende Fassung:

„Spezifisches Ziel 3 – Cybersicherheit und Vertrauen

3.1. Anzahl der gemeinsam beschafften Cybersicherheitsinfrastrukturen oder -werkzeuge oder beider[1]

3.2. Anzahl der Nutzer und Nutzergemeinschaften, die Zugang zu europäischen Cybersicherheitseinrichtungen erhalten

3.3. Anzahl der Maßnahmen zur Unterstützung der Abwehrbereitschaft und der Reaktion auf Cybersicherheitsvorfälle im Rahmen des Cybernotfallmechanismus“.