Amtsblatt
der Europäischen Union

DE
Reihe L

2025/38

15.1.2025

VERORDNUNG (EU) 2025/38 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 19. Dezember 2024

über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (Cybersolidaritätsverordnung)

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 [4],

in Erwägung nachstehender Gründe:

(1) Die Nutzung und Abhängigkeit von Informations- und Kommunikationstechnologien sind mittlerweile aufgrund der ständig zunehmenden Verflechtung und gegenseitigen Abhängigkeit der öffentlichen Verwaltungen, Unternehmen und Bürger der Mitgliedstaaten branchen- und grenzübergreifend von grundlegender Bedeutung in allen Wirtschaftssektoren und Gesellschaftsbereichen, was gleichzeitig potenzielle Schwachstellen schafft.

(2) Die Tragweite, die Häufigkeit und die Auswirkungen von Cybersicherheitsvorfällen, einschließlich Angriffe auf die Lieferkette für die Zwecke von Cyberspionage, Ransomware oder Störungen, nehmen sowohl auf Unionsebene als auch weltweit zu. Sie stellen eine große Bedrohung für das Funktionieren von Netz- und Informationssystemen dar. Angesichts der sich wandelnden Bedrohungslandschaft ist wegen der Gefahr von potenziellen Cybersicherheitsvorfällen großen Ausmaßes, die erhebliche Störungen oder Schäden an kritischer Infrastruktur verursachen, eine erhöhte Abwehrbereitschaft des Cybersicherheitsrahmens der Union erforderlich. Diese Bedrohung geht über den Angriffskrieg Russlands gegen die Ukraine hinaus und wird angesichts der Vielzahl der Akteure, die an den derzeitigen geopolitischen Spannungen beteiligt sind, wahrscheinlich andauern. Solche Sicherheitsvorfälle können die Erbringung öffentlicher Dienstleistungen beeinträchtigen, da sich Cyberangriffe häufig gegen lokale, regionale oder nationale öffentliche Dienste und Infrastruktur richten, wobei lokale Behörden, auch aufgrund ihrer begrenzten Ressourcen, besonders anfällig sind. Ferner können sie — auch in Sektoren mit hoher Kritikalität oder sonstigen kritischen Sektoren — die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, erhebliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und den demokratischen Systemen der Union schweren Schaden zufügen und könnten sogar gesundheitliche oder lebensbedrohliche Folgen haben. Darüber hinaus sind Cybersicherheitsvorfälle unvorhersehbar, da sie oft schnell auftreten und sich fortentwickeln und nicht auf ein bestimmtes geografisches Gebiet beschränkt sind, sondern sich gleichzeitig in vielen Ländern ereignen oder sich rasch in anderen Ländern ausbreiten. Es bedarf einer engen Zusammenarbeit zwischen öffentlichem Sektor, Privatsektor, Hochschulen, Zivilgesellschaft und Medien.

(3) Es ist notwendig, die Wettbewerbsposition von Industrie und Dienstleistungen in der Union in der gesamten digitalen Wirtschaft zu stärken und ihren digitalen Wandel zu unterstützen, indem das Cybersicherheitsniveau im digitalen Binnenmarkt erhöht wird, wie es in drei verschiedenen Vorschlägen der Konferenz zur Zukunft Europas empfohlen wurde. Die Resilienz der Bürgerinnen und Bürger, der Unternehmen, einschließlich von Kleinstunternehmen, kleinen und mittleren Unternehmen und Start-up-Unternehmen, sowie von Einrichtungen, die kritische Infrastruktur betreiben, gegenüber den zunehmenden Cyberbedrohungen, die verheerende gesellschaftliche und wirtschaftliche Auswirkungen haben können, muss erhöht werden. Daher sind Investitionen in Infrastruktur und

[1] Stellungnahme vom 18. April 2023 (noch nicht im Amtsblatt veröffentlicht).
[2] ABl. C 349 vom 29.9.2023, S. 167.
[3] ABl. C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
[4] Standpunkt des Europäischen Parlaments vom 24. April 2024 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 2. Dezember 2024.

Dienste sowie der Aufbau von Fähigkeiten zur Entwicklung von Cybersicherheitskompetenzen erforderlich, die eine schnellere Erkennung von Cyberbedrohungen und Sicherheitsvorfällen und eine schnellere Reaktion darauf unterstützen. Darüber hinaus benötigen die Mitgliedstaaten Unterstützung bei der Verbesserung der Vorsorge für und der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes sowie Unterstützung in der Anfangsphase der Wiederherstellung nach solchen Sicherheitsvorfällen. Aufbauend auf den vorhandenen Strukturen sowie in enger Zusammenarbeit mit diesen sollte die Union ferner ihre Kapazitäten in diesen Bereichen ausbauen, insbesondere in Bezug auf die Erhebung und Analyse von Daten über Cyberbedrohungen und Sicherheitsvorfälle.

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

(5) Die zunehmenden Cybersicherheitsrisiken und eine insgesamt komplexe Bedrohungslandschaft mit der eindeutigen Gefahr einer raschen Ausbreitung von Sicherheitsvorfällen von einem Mitgliedstaat auf einen anderen sowie von Drittländern in die Union erfordern eine Stärkung der Solidarität auf Unionsebene, um die Erkennung von Cyberdrohungen und Sicherheitsvorfällen, die diesbezügliche Vorsorge und Reaktion sowie die anschließende Wiederherstellung zu verbessern, insbesondere durch eine Stärkung der Fähigkeiten vorhandener Strukturen. Darüber hinaus wurde die Kommission in den Schlussfolgerungen des Rates vom 23. Mai 2022 über die Einrichtung einer Cyberabwehr der Europäischen Union, aufgefordert, einen Vorschlag für einen neuen Notfallfonds für Cybersicherheit vorzulegen.

(6) In der Gemeinsamen Mitteilung der Kommission und des Hohen Vertreters der Union für Außen- und Sicherheitspolitik vom 10. November 2022 an das Europäische Parlament und den Rat über die EU-Cyberabwehrpolitik wurde eine EU-Initiative zur Cybersolidarität mit 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 Cyberreserve 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 Sicherheitsvorfälle als auch die Solidarität zu stärken, indem die Abwehrbereitschaft und die Fähigkeiten der Mitgliedstaaten und der Union zur Prävention von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes sowie zur Reaktion auf solche Sicherheitsvorfälle verbessert werden. Daher sollte ein europaweites Netz von Cyber-Hubs (im Folgenden „europäisches Warnsystem für Cybersicherheit“) geschaffen werden, um koordinierte Fähigkeiten zur Erkennung und Lageerfassung aufzubauen, damit die Fähigkeiten der Union zur Erkennung von Bedrohungen und zur Weitergabe von Informationen gestärkt werden; ein Cybernotfallmechanismus sollte eingerichtet werden, um die Mitgliedstaaten auf deren Antrag hin bei der Vorsorge für, der Bewältigung von und der Einleitung der Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes sowie andere Nutzer bei der Reaktion auf schwerwiegende Cybersicherheitsvorfälle und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfällen zu unterstützen; ferner sollte ein Europäischer Überprüfungsmechanismus für Cybersicherheitsvorfälle eingerichtet werden, um bestimmte schwerwiegende Cybersicherheitsvorfälle bzw. Cybersicherheitsvorfälle großen Ausmaßes zu überprüfen und zu bewerten. Die Maßnahmen, die gemäß dieser Verordnung ergriffen werden, sollten unter gebührender Berücksichtigung der Zuständigkeiten der Mitgliedstaaten durchgeführt werden und die Tätigkeiten des CSIRTs-Netzes, des Netzwerks der Verbindungsorganisationen für Cyberkrisen (im Folgenden „EU-CyCLONe“) oder der Kooperationsgruppe (im Folgenden „NIS-Kooperationsgruppe“), die alle gemäß der Richtlinie (EU) 2022/2555 eingerichtet wurden, ergänzen und nicht duplizieren. Diese Maßnahmen lassen Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unberührt.

([5]) 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).

([6]) 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).

([7]) 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).

([8]) 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).

(8) Um diese Ziele zu erreichen, ist es erforderlich, die Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates ([9]) in bestimmten Bereichen zu ändern. Insbesondere sollte mit dieser Verordnung die Verordnung (EU) 2021/694 dahin gehend geändert werden, dass neue operative Ziele im Zusammenhang mit dem europäischen Warnsystem für Cybersicherheit und dem Cybernotfallmechanismus 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 Cyberbedrohungen zu stärken und darauf zu reagieren und die grenzüberschreitende Zusammenarbeit und Koordination im Bereich der Cybersicherheit zu verbessern, hinzugefügt werden. Das europäische Warnsystem für Cybersicherheit könnte eine wichtige Rolle dabei spielen, die Mitgliedstaaten bei der Antizipation von und dem Schutz vor Cyberbedrohungen zu unterstützen, und die EU-Cybersicherheitsreserve in erheblichem Maße könnte dazu beitragen, die Mitgliedstaaten, die Organe, Einrichtungen und sonstigen Stellen der Union sowie die mit dem Programm „Digitales Europa" assoziierten Drittländer dabei zu unterstützen, auf schwerwiegende Cybersicherheitsvorfälle, Cybersicherheitsvorfälle großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle zu reagieren und deren Auswirkungen abzumildern. Diese Auswirkungen könnten erhebliche materielle oder immaterielle Schäden sowie ernsthafte Risiken für die öffentliche Sicherheit umfassen. Angesichts der besonderen Rolle, die das europäische Warnsystem für Cybersicherheit und die EU-Cybersicherheitsreserve spielen könnten, sollte mit der vorliegenden Verordnung die Verordnung (EU) 2021/694 in Bezug auf die Teilnahme von Rechtsträgern geändert werden, die ihren Sitz in der Union haben, aber aus Drittländern kontrolliert werden, und zwar für die Fälle, in denen ein reales Risiko besteht, dass die erforderlichen und ausreichenden Instrumente, Infrastrukturen und Dienste oder Technologien, Fachkenntnisse und Kapazitäten in der Union nicht zur Verfügung stehen und die Vorteile der Aufnahme solcher Rechtsträger die Sicherheitsrisiken überwiegen. Es sollten spezifische Bedingungen festgelegt werden, unter denen finanzielle Unterstützung für Maßnahmen zur Umsetzung des europäischen Warnsystems für Cybersicherheit und der EU-Cybersicherheitsreserve gewährt werden kann, und es sollten die Steuerungs- und Koordinierungsmechanismen bestimmt werden, 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 umfassen.

(9) Zur Stärkung der Reaktion der Union auf Cyberbedrohungen und Sicherheitsvorfälle ist eine Zusammenarbeit mit internationalen Institutionen sowie mit vertrauenswürdigen, gleich gesinnten internationalen Partnern von zentraler Bedeutung. In diesem Zusammenhang sollten solche Länder als vertrauenswürdige, gleich gesinnte internationale Partner verstanden werden, die die Grundprinzipien, die für die Entstehung der Union maßgebend waren, nämlich Demokratie, Rechtsstaatlichkeit, universelle Gültigkeit und Unteilbarkeit der Menschenrechte und Grundfreiheiten und Achtung der Menschenwürde sowie die Grundsätze der Gleichheit und der Solidarität und die Achtung der Grundsätze der Charta der Vereinten Nationen und des Völkerrechts teilen und die wesentlichen Sicherheitsinteressen der Union und ihrer Mitgliedstaaten nicht untergraben. Eine solche Zusammenarbeit könnte auch im Hinblick auf die gemäß dieser Verordnung ergriffenen Maßnahmen, insbesondere das europäische Warnsystem für Cybersicherheit und die EU-Cybersicherheitsreserve, von Vorteil sein. Die Verordnung (EU) 2021/694 sollte vorsehen, dass unter bestimmten Verfügbarkeits- und Sicherheitsbedingungen Ausschreibungen für das europäische Warnsystem für Cybersicherheit und die EU-Cybersicherheitsreserve unter dem Vorbehalt von Sicherheitsanforderungen Rechtsträgern offenstehen könnten, die aus Drittländern kontrolliert werden. Bei der Bewertung des mit einer solchen Öffnung von Ausschreibungen verbundenen Sicherheitsrisikos ist es wichtig, die Grundprinzipien und Werte zu berücksichtigen, die die Union mit gleich gesinnten internationalen Partnern teilt, sofern diese Grundprinzipien und Werte wesentliche Sicherheitsinteressen der Union betreffen. Darüber hinaus könnten bei der Prüfung solcher Sicherheitsanforderungen im Rahmen der Verordnung (EU) 2021/694 mehrere Elemente berücksichtigt werden, wie die Struktur und der Entscheidungsprozess der betreffenden Einrichtung, die Sicherheit von Daten und als Verschlusssache eingestuften oder vertraulichen Informationen, wobei sicherzustellen ist, dass die Ergebnisse der Maßnahme keiner Kontrolle und keinen Beschränkungen durch nicht förderfähige Drittländer unterliegen.

(10) Die Finanzierung von Maßnahmen im Rahmen der vorliegenden Verordnung sollte in der Verordnung (EU) 2021/694 geregelt werden, die weiterhin der einschlägige Basisrechtsakt für die im spezifischen Ziel 3 des Programms „Digitales Europa" verankerten Maßnahmen bleiben sollte. Die besonderen Teilnahmebedingungen für die einzelnen Maßnahmen sind gemäß der Verordnung (EU) 2021/694 in den einschlägigen Arbeitsprogrammen festzulegen.

(11) Auf diese Verordnung finden die vom Europäischen Parlament und dem Rat gemäß Artikel 322 AEUV erlassenen horizontalen Haushaltsvorschriften Anwendung. Diese Vorschriften sind in der Verordnung (EU, Euratom) 2024/2509 des Europäischen Parlaments und des Rates ([10]) festgelegt und regeln insbesondere das Verfahren für die Aufstellung und Ausführung des Haushaltsplans der Union sowie die Kontrolle der Verantwortung der

([9]) 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).

([10]) Verordnung (EU, Euratom) 2024/2509 des Europäischen Parlaments und des Rates vom 23. September 2024 über die Haushaltsordnung für den Gesamthaushaltsplan der Union (ABl. L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

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 ([11]) festgelegt ist.

(12) Zwar sind Präventionsmaßnahmen und Maßnahmen in Bezug auf die Abwehrbereitschaft von wesentlicher Bedeutung, um die Resilienz der Union beim Angehen von schwerwiegenden Cybersicherheitsvorfällen, Cybersicherheitsvorfällen großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfällen zu stärken, doch sind das Auftreten, der Zeitpunkt und das Ausmaß solcher Sicherheitsvorfälle naturgemäß unvorhersehbar. Die für eine angemessene Reaktion erforderlichen Finanzmittel können von Jahr zu Jahr erheblich variieren und sollten unverzüglich zur Verfügung gestellt werden können. Um den Haushaltsgrundsatz der Vorhersehbarkeit mit der Notwendigkeit einer raschen Reaktion auf neue Erfordernisse in Einklang zu bringen, muss die finanzielle Durchführung der Programme daher angepasst werden. Folglich ist es angezeigt, zusätzlich zu der Übertragung von gemäß Artikel 12 Absatz 4 der Verordnung (EU, Euratom) 2024/2509 genehmigten Mitteln die Übertragung nicht verwendeter Mittel zu gestatten, aber nur, wenn diese Mittelübertragung auf das folgende Haushaltsjahr beschränkt ist und die Mittel ausschließlich für die EU-Cybersicherheitsreserve und für Maßnahmen zur Unterstützung der Amtshilfe bestimmt sind.

(13) Um Cyberbedrohungen und Sicherheitsvorfälle wirksamer verhindern und bewerten zu können, wirksamer darauf reagieren und sich von diesen wirksamer erholen zu können, ist es notwendig, umfassendere Kenntnisse über die bestehenden Bedrohungen für kritische Anlagen und Infrastruktur im Gebiet der Union zu erlangen, einschließlich ihrer geografischen Verteilung, ihres Zusammenwirkens und ihrer potenziellen Auswirkungen im Falle von Cyberangriffen, die diese Infrastruktur betreffen. Eine vorausschauende Vorgehensweise zur Ermittlung, Minderung und Prävention von Cyberbedrohungen setzt erhöhte Kapazitäten auf dem Gebiet der fortgeschrittenen Erkennung voraus. Das europäische Warnsystem für Cybersicherheit sollte aus mehreren interoperativen grenzübergreifenden Cyber-Hubs bestehen, die jeweils drei oder mehr nationale Cyber-Hubs 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 fortschrittliche Instrumente für die Erhebung relevanter — gegebenenfalls anonymisierter — Daten und Informationen sowie für die Analyse nutzt, die Fähigkeiten zur koordinierten Erkennung und Bewältigung von Cyberangriffen verbessert und eine Echtzeit-Lageerfassung ermöglicht. Diese Infrastruktur sollte dazu dienen, die Cyberabwehr zu verbessern, indem die Erkennung, Aggregation und Analyse von Daten und Informationen verstärkt werden, um Cyberbedrohungen und Sicherheitsvorfällen vorzubeugen und somit die für das Cyberkrisenmanagement in der Union zuständigen Einrichtungen und Netze der Union, insbesondere das EU-CyCLONe, zu ergänzen und zu unterstützen.

(14) Die Teilnahme am europäischen Warnsystem für Cybersicherheit ist für die Mitgliedstaaten freiwillig. Jeder Mitgliedstaat sollte auf nationaler Ebene eine einzige Einrichtung benennen, die mit der Koordinierung von Tätigkeiten zur Erkennung von Cyberbedrohungen in diesem Mitgliedstaat betraut ist. Diese nationalen Cyber-Hubs sollten auf nationaler Ebene als Bezugspunkt und Zugangstor für die Beteiligung am europäischen Warnsystem für Cybersicherheit fungieren und sicherstellen, dass Informationen über Cyberbedrohungen von öffentlichen und privaten Einrichtungen auf nationaler Ebene wirksam und effizient ausgetauscht und gesammelt werden. Nationale Cyber-Hubs könnten die Zusammenarbeit und die Weitergabe von Informationen zwischen öffentlichen und privaten Einrichtungen stärken und ferner den Austausch relevanter Daten und Informationen mit einschlägigen sektoralen und sektorübergreifenden Gemeinschaften wie etwa einschlägigen sektorspezifischen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centers, im Folgenden „ISACs“) unterstützen. Eine enge und koordinierte Zusammenarbeit zwischen öffentlichen und privaten Einrichtungen ist für die Stärkung der Cyberresilienz der Union von zentraler Bedeutung. Diese Zusammenarbeit bietet insbesondere im Zusammenhang mit der Weitergabe von Erkenntnissen über Cyberbedrohungen zwecks Verbesserung des aktiven Cyberschutzes einen Mehrwert. Im Rahmen dieser Zusammenarbeit und dieser Weitergabe von Informationen könnten nationale Cyber-Hubs spezifische Informationen anfordern und erhalten. Diese nationalen Cyber-Hubs werden durch diese Verordnung weder verpflichtet noch befugt, entsprechende Ersuchen durchzusetzen. Sofern angezeigt und mit dem Unionsrecht und dem nationalen Recht vereinbar, könnten die angeforderten oder erhaltenen Informationen Telemetrie-, Sensor- und Protokolldaten von in Sektoren mit hoher Kritikalität tätigen Einrichtungen oder in sonstigen kritischen Sektoren tätigen Einrichtungen, in dem betreffenden Mitgliedstaat tätig sind, beispielsweise Anbietern verwalteter Sicherheitsdienste, umfassen, damit die rasche Erkennung potenzieller Cyberbedrohungen und Sicherheitsvorfälle bereits zu einem früheren Zeitpunkt verbessert wird, wodurch die Lageerfassung verbessert wird. Handelt es sich bei einem nationalen Cyber-Hub nicht um die von dem betreffenden Mitgliedstaat gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannte oder eingerichtete zuständige Behörde, ist es von entscheidender Bedeutung, dass sich dieser in Bezug auf die Anforderung und den Erhalt solcher Daten mit dieser zuständigen Behörde abstimmt.

(15) Im Rahmen des europäischen Warnsystems für Cybersicherheit sollte eine Reihe grenzübergreifender Cyber-Hubs eingerichtet werden. Diese grenzübergreifenden Cyber-Hubs sollten nationale Cyber-Hubs aus mindestens drei Mitgliedstaaten zusammenbringen, um sicherzustellen, dass die Vorteile der grenzübergreifenden Erkennung von Bedrohungen sowie der Weitergabe von Informationen und des Informationsmanagements voll ausgeschöpft

([11]) Verordnung (EU, Euratom) 2020/2092 des Europäischen Parlaments und des Rates vom 16. Dezember 2020 über eine allgemeine Konditionalitätsregelung zum Schutz des Haushalts der Union (ABl. L 433 I vom 22.12.2020, S. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

werden können. Das allgemeine Ziel grenzübergreifender Cyber-Hubs sollte darin bestehen, die Kapazitäten zur Analyse, Verhütung und Erkennung von Cyberdrohungen zu stärken und die Gewinnung hochwertiger Erkenntnisse über Cyberbedrohungen zu unterstützen, insbesondere durch die Weitergabe relevanter — gegebenenfalls anonymisierter — Informationen aus verschiedenen öffentlichen oder privaten Quellen in einem vertrauenswürdigen und sicheren Umfeld sowie durch die Weitergabe und die gemeinsame Nutzung modernster Instrumente und die gemeinsame Entwicklung von Erkennungs-, Analyse- und Präventionsfähigkeiten in einem vertrauenswürdigen und sicheren Umfeld. Die grenzübergreifenden Cyber-Hubs sollten neue zusätzliche Kapazitäten bereitstellen, die auf bestehenden SOCs, CSIRTs und anderen einschlägigen Akteuren, einschließlich des CSIRTs-Netzes, aufbauen und diese ergänzen.

(16) Ein Mitgliedstaat, der von dem durch die Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates ([12]) eingerichteten Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (im Folgenden „ECCC“) im Anschluss an einen Aufruf zur Interessenbekundung für die Einrichtung oder zum Ausbau der Fähigkeiten eines nationalen Cyber-Hubs ausgewählt wurde, sollte, gemeinsam mit dem ECCC, die einschlägigen Instrumente, Infrastruktur oder Dienste beschaffen. Ein solcher Mitgliedstaat sollte Finanzhilfen für die Verwendung der Instrumente, Infrastruktur oder Dienste erhalten können. Ein Aufnahmekonsortium, das aus mindestens drei Mitgliedstaaten besteht und das vom ECCC im Anschluss an einen Aufruf zur Interessenbekundung für die Einrichtung oder den Ausbau der Fähigkeiten eines grenzübergreifenden Cyber-Hubs ausgewählt wurde, sollte die einschlägigen Instrumente, Infrastruktur oder Dienste gemeinsam mit dem ECCC beschaffen. Das Aufnahmekonsortium sollte Finanzhilfen für die Verwendung der Instrumente, Infrastruktur oder Dienste erhalten können. Das Beschaffungsverfahren für die einschlägigen Instrumente, Infrastruktur und Dienste sollte vom ECCC und den zuständigen öffentlichen Auftraggebern in den Mitgliedstaaten, die im Anschluss an diese Aufrufe zur Interessenbekundung ausgewählt wurden, gemeinsam durchgeführt werden. Diese Beschaffung sollte Artikel 168 Absatz 2 der Verordnung (EU, Euratom) 2024/2509 und der Finanzordnung des ECCC entsprechen. Private Einrichtungen sollten daher nicht berechtigt sein, an den Aufrufen zur Interessenbekundung für die Beschaffung von Instrumenten, Infrastruktur oder Diensten gemeinsam mit dem ECCC teilzunehmen oder Finanzhilfen für die Verwendung dieser Instrumente, Infrastruktur oder Dienste zu erhalten. Die Mitgliedstaaten sollten jedoch in der Lage sein, private Einrichtungen gemäß dem Unionsrecht und dem nationalen Recht auf eine andere, von ihnen für angemessen erachtete Weise in die Einrichtung, den Ausbau und den Betrieb ihrer nationalen und grenzübergreifenden Cyber-Hubs einzubeziehen. Private Einrichtungen könnten ferner berechtigt sein, Unionsmittel gemäß der Verordnung (EU) 2021/887 zu erhalten, um nationale Cyber-Hubs zu unterstützen.

(17) Im Interesse einer besseren Erkennung von Cyberbedrohungen und einer besseren Lageerfassung in der Union sollten sich Mitgliedstaaten, die im Anschluss an einen Aufruf zur Interessenbekundung für die Einrichtung oder zum Ausbau der Fähigkeiten eines Cyber-Hubs ausgewählt wurde, verpflichten, einen Antrag auf Teilnahme an einem grenzübergreifenden Cyber-Hub zu stellen. Nimmt ein Mitgliedstaat binnen zwei Jahren ab dem Zeitpunkt, zu dem die Instrumente, Infrastruktur oder Dienste beschafft werden oder zu dem er Finanzhilfen erhält — je nachdem, welches Ereignis früher eintritt —, nicht an einem grenzübergreifenden Cyber-Hub teil, so sollte er nicht berechtigt sein, sich an weiteren Unterstützungsmaßnahmen der Union im Rahmen des Europäischen Warnsystems für Cybersicherheit zum Ausbau der Fähigkeiten seines nationalen Cyber-Hubs zu beteiligen. In solchen Fällen könnten Einrichtungen aus den Mitgliedstaaten weiterhin an Aufrufen zur Einreichung von Vorschlägen zu anderen Themen im Rahmen des Programms „Digitales Europa“ oder anderer Finanzierungsprogramme der Union teilnehmen, einschließlich Aufrufen in Bezug auf Kapazitäten für die Erkennung von Cyberbedrohungen und die Weitergabe von Informationen, sofern diese Einrichtungen die in diesen Programmen festgelegten Eignungskriterien erfüllen.

(18) Die CSIRTs tauschen innerhalb des CSIRTs-Netzes Informationen gemäß der Richtlinie (EU) 2022/2555 aus. Das europäische Warnsystem für Cybersicherheit sollte eine neue Fähigkeit bilden, die das CSIRTs-Netz ergänzt, indem sie zur Schaffung einer Lageerfassung in der Union beiträgt, durch die die Kapazitäten des CSIRTs-Netzes gestärkt werden können. Grenzübergreifende Cyber-Hubs sollten sich mit dem CSIRTs-Netz abstimmen und eng mit diesem zusammenarbeiten. Dabei sollten sie Daten über Cyberbedrohungen von öffentlichen und privaten Einrichtungen zusammenführen und entsprechende relevante — gegebenenfalls anonymisierte — Informationen weitergeben, den Wert solcher Daten und Informationen durch Expertenanalysen, gemeinsam beschaffte Infrastruktur und modernste Instrumente steigern und zur technologischen Souveränität, offenen strategischen Autonomie, Wettbewerbsfähigkeit und Resilienz der Union sowie zur Entwicklung ihrer Fähigkeiten beitragen.

(19) Die grenzübergreifenden Cyber-Hubs sollten als zentrale Stellen fungieren, die eine umfassende Zusammenführung einschlägiger Daten und Erkenntnisse über Cyberbedrohungen und die Verbreitung von Informationen über Bedrohungen in einem großen und vielfältigen Spektrum von Interessenträgern ermöglicht, beispielsweise Soforteinsatzteams für IT-Sicherheitsvorfälle (CERTs), CSIRTs, ISACs und Betreiber kritischer Infrastruktur. Die Mitglieder eines Aufnahmekonsortiums sollten die zwischen den Teilnehmern des betreffenden grenzüberschreitenden Cyberzentrums weiterzugebenden relevanten Informationen in der Konsortialvereinbarung festlegen. Der Informationsaustausch zwischen den Teilnehmern eines grenzübergreifenden Cyber-Hubs könnte beispielsweise Daten von Netzwerken und Sensoren, laufende Erkenntnisse über Bedrohungen, Kompromittierungsindikatoren und kontextualisierte Informationen über Sicherheitsvorfälle, Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen,

([12]) 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, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

Techniken und Verfahren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Erkennung von Cyberangriffen umfassen. Darüber hinaus sollten die grenzübergreifenden Cyber-Hubs auch untereinander Kooperationsvereinbarungen schließen. In diesen Kooperationsvereinbarungen sollten insbesondere die Grundsätze für die Informationsweitergabe und Aspekte im Zusammenhang mit der Interoperabilität festgelegt werden. Die Klauseln zur Interoperabilität, insbesondere in Bezug auf Formate und Protokolle für die Informationsweitergabe, sollten sich an den von der durch die Verordnung (EU) 2019/881 eingerichteten Agentur der Europäischen Union für Cybersicherheit (ENISA) herausgegebenen Interoperabilitätsleitlinien orientieren und diese daher als Ausgangspunkt nutzen. Diese Leitlinien sollten zeitnah herausgegeben werden, damit sichergestellt wird, dass sie von den grenzübergreifenden Cyber-Hubs frühzeitig berücksichtigt werden können. Sie sollten internationalen Standards und bewährten Verfahren sowie der Funktionsweise aller bestehenden grenzübergreifenden Cyber-Hubs Rechnung tragen.

(20) Grenzübergreifende Cyber-Hubs und das CSIRTs-Netz sollten eng zusammenarbeiten, um Synergien sowie eine Komplementarität der Tätigkeiten sicherzustellen. Zu diesem Zweck sollten sie Verfahrensmodalitäten für die Zusammenarbeit und die Weitergabe relevanter Informationen vereinbaren. Dies könnte die Weitergabe relevanter Informationen über Cyberbedrohungen und schwerwiegende Cybersicherheitsvorfälle und die Sicherstellung der Weitergabe von Erfahrungen mit in den grenzübergreifenden Cyber-Hubs verwendeten hochmodernen Instrumenten, insbesondere Technologien der künstlichen Intelligenz und der Datenanalyse, an das CSIRTs-Netz einschließen.

(21) 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 Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union wurde mit der Richtlinie (EU) 2022/2555 das EU-CyCLONe eingerichtet. Darüber hinaus wurde mit der Richtlinie (EU) 2022/2555 das CSIRTs-Netz eingerichtet, das der Förderung einer raschen und wirksamen operativen Zusammenarbeit zwischen allen Mitgliedstaaten dienen soll. Zur Sicherstellung der Lageerfassung und zur Stärkung der Solidarität sollten grenzübergreifende Cyber-Hubs, wenn sie Informationen in Bezug auf einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, dem CSIRTs-Netz relevante Informationen zur Verfügung stellen und diesbezüglich eine frühzeitige Warnung an das EU-CyCLONe richten. Je nach Lage könnten die weiterzugebenden 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 weitergegebenen Informationen gebührend Rechnung getragen werden. n der Richtlinie (EU) 2022/2555 werden auch die Zuständigkeiten der Kommission im Rahmen des mit dem Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates ([13]) eingerichteten Katastrophenschutzverfahrens der Union (UCPM) bekräftigt, sowie ihre Verantwortung für die Bereitstellung analytischer Berichte für die Integrierte EU-Regelung für die politische Reaktion auf Krisen (IPCR-Regelung) gemäß dem Durchführungsbeschluss (EU) 2018/1993 des Rates ([14]). Wenn grenzüberschreitende Cyber-Hubs relevante Informationen und Frühwarnungen in Bezug auf einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes an das EU-CyCLONe und das CSIRTs-Netz weitergeben, ist es unerlässlich, dass diese Informationen über die genannten Netze an die Behörden der Mitgliedstaaten sowie an die Kommission weitergegeben werden. In diesem Zusammenhang sieht die Richtlinie (EU) 2022/2555 vor, dass das EU-CyCLONe dem Zweck dient, das koordinierte Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene zu unterstützen und einen regelmäßigen Austausch relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union zu gewährleisten. Zu den Aufgaben des EU-CyCLONe gehört die Entwicklung einer gemeinsamen Lageerfassung für solche Sicherheitsvorfälle und Krisen. Es ist von größter Bedeutung, dass das EU-CyCLONe gemäß seinem Zweck und seinen Aufgaben dafür sorgt, dass diese Informationen unverzüglich den einschlägigen Vertretern der Mitgliedstaaten sowie der Kommission zur Verfügung gestellt werden. Zu diesem Zweck ist es von entscheidender Bedeutung, dass die Geschäftsordnung des EU-CyCLONe angemessene Bestimmungen enthält.

(22) Einrichtungen, die sich am europäischen Warnsystem für Cybersicherheit beteiligen, sollten ein hohes Maß an Interoperabilität untereinander sicherstellen, gegebenenfalls auch in Bezug auf Datenformate, Taxonomie, Datenverarbeitungs- und Datenanalyseinstrumente. Sie sollten auch sichere Kommunikationskanäle, ein Mindestmaß an Sicherheit auf Anwendungsebene, ein Lagebewusstsein und Indikatoren sicherstellen. Bei der Annahme einer gemeinsamen Taxonomie und der Entwicklung einer Vorlage für Lageberichte zur Beschreibung der Ursachen erkannter Cyberbedrohungen und -risiken sollten die bereits im Zusammenhang mit der Umsetzung der Richtlinie (EU) 2022/2555 erfolgten Arbeiten berücksichtigt werden.

([13]) 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

([14]) Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die integrierte EU-Regelung für die politische Reaktion auf Krisen (ABl. L 320 vom 17.12.2018, S. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

(23) Um den Austausch relevanter Daten und Informationen über Cyberbedrohungen aus verschiedenen Quellen in einem vertrauenswürdigen und sicheren Umfeld in großem Maßstab zu ermöglichen, sollten Einrichtungen, die sich am europäischen Warnsystem für Cybersicherheit beteiligen, mit modernsten, hochsicheren Instrumenten, Ausrüstungen und hochsicherer Infrastruktur sowie mit qualifiziertem Personal 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 Technologien der künstlichen Intelligenz und der Datenanalyse.

(24) Durch die Sammlung, die Analyse, die Weitergabe und den Austausch relevanter Daten und Informationen sollte das europäische Warnsystem für Cybersicherheit die technologische Souveränität der Union, ihre offene strategische Autonomie im Bereich der Cybersicherheit, ihre Wettbewerbsfähigkeit und ihre Resilienz stärken. Die Zusammenführung hochwertiger kuratierter Daten könnte auch zur Entwicklung fortgeschrittener Technologien der künstlichen Intelligenz und der Datenanalyse beitragen. Eine menschliche Aufsicht und im Hinblick darauf qualifizierte Arbeitskräfte sind für eine wirksame Zusammenführung hochwertiger Daten nach wie vor von wesentlicher Bedeutung.

(25) Obwohl das europäische Warnsystem für Cybersicherheit ein ziviles Projekt ist, könnten die Cyberabwehrkreise von besseren zivilen Fähigkeiten zur Erkennung und Lageerfassung profitieren, die für den Schutz kritischer Infrastruktur entwickelt werden.

(26) Bei der Weitergabe von Informationen zwischen den Teilnehmern des europäischen Warnsystems für Cybersicherheit 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, die die Rechte und Freiheiten der betroffenen Personen schützen und die Daten vernichten, sobald sie für den angegebenen Zweck nicht mehr erforderlich sind, und die Einrichtung, die die Daten zur Verfügung stellt, darüber informieren, dass die Daten vernichtet wurden.

(27) Die Wahrung der Vertraulichkeit und der Informationssicherheit ist für alle drei Säulen dieser Verordnung von größter Bedeutung, sei es für die Förderung der Weitergabe oder des Austauschs von Informationen im Rahmen des europäischen Warnsystems für Cybersicherheit, für die Wahrung der Interessen der Einrichtungen, die Unterstützung im Rahmen des Cybersicherheitsnotfallmechanismus beantragen, oder für die Sicherstellung, dass in Berichten im Rahmen des Europäischen Überprüfungsmechanismus für Cybersicherheitsvorfälle nützliche Schlussfolgerungen gezogen werden können, ohne dass die von diesen Sicherheitsvorfällen betroffenen Einrichtungen dadurch negativ beeinträchtigt würden. Die Teilnahme der Mitgliedstaaten und Einrichtungen an diesen Mechanismen setzt vertrauensbasierte Beziehungen zwischen den einzelnen Komponenten voraus. Sind Informationen gemäß Unions- oder nationalen Vorschriften vertraulich, so sollte ihre Weitergabe oder ihr Austausch im Rahmen dieser Verordnung auf den für den Zweck der Weitergabe oder des Austauschs relevanten und verhältnismäßigen Umfang beschränkt werden. Im Rahmen dieser Weitergabe oder Austauschs sollte auch die Vertraulichkeit der Informationen gewahrt werden, was auch den Schutz der Sicherheit und der geschäftlichen Interessen betreffender Einrichtungen umfasst. Die Weitergabe oder der Austausch von Informationen im Rahmen dieser Verordnung könnte unter Verwendung von Geheimhaltungsvereinbarungen oder Leitlinien für die Weitergabe von Informationen, wie beispielsweise dem Traffic Light Protocol (im Folgenden „TLP"), erfolgen. Das TLP ist als ein Mittel zu verstehen, um über etwaige Einschränkungen in Bezug auf die weitere Verbreitung von Informationen zu informieren. Es wird in fast allen CSIRTs sowie in einigen ISACs verwendet. Zusätzlich zu diesen allgemeinen Anforderungen sollten in Bezug auf das europäische Warnsystem für Cybersicherheit in Vereinbarungen über Aufnahmekonsortien spezifische Vorschriften in Bezug auf die Bedingungen für die Weitergabe von Informationen innerhalb des betreffenden grenzübergreifenden Cyber-Hubs festgelegt werden. Diese Vereinbarungen könnten konkret vorschreiben, dass Informationen nur gemäß dem Unionsrecht und dem nationalen Recht weitergegeben werden dürfen.

(28) Für den Einsatz der EU-Cybersicherheitsreserve sind spezifische Vorschriften in Bezug auf die Vertraulichkeit erforderlich. Die Beantragung, Prüfung und Bereitstellung von Unterstützung erfolgt in Krisensituationen und in Bezug auf in sensiblen Sektoren tätige Einrichtungen. Damit die EU-Cybersicherheitsreserve wirksam funktionieren kann, ist es von wesentlicher Bedeutung, dass Nutzer und Einrichtungen all jene Informationen, die die jeweiligen Einrichtungen zur Wahrnehmung ihrer Funktionen im Zusammenhang mit der Prüfung von Anträgen und der Bereitstellung von Unterstützung benötigen, unverzüglich weitergeben und zugänglich machen können. Dementsprechend sollte diese Verordnung vorsehen, dass alle diese Informationen nur dann verwendet oder weitergegeben werden, wenn dies für den Betrieb der EU-Cybersicherheitsreserve erforderlich ist, und dass Informationen, die gemäß Unions- oder nationalem Recht vertraulich oder als Verschlusssache eingestuft sind, nur gemäß diesem Recht zu verwenden und weiterzugeben sind. Darüber hinaus sollten die Nutzer in der Lage sein, gegebenenfalls Protokolle für die Weitergabe von Informationen wie etwa das TLP zu verwenden, um Einschränkungen genauer festzulegen. Zwar verfügen Nutzer diesbezüglich über einen Ermessensspielraum, doch ist es wichtig, dass sie bei der Anwendung solcher Einschränkungen die möglichen Folgen berücksichtigen, insbesondere im Hinblick auf Verzögerungen bei der Bewertung oder Bereitstellung der beantragten Dienste. Für die Effizienz der EU-Cybersicherheitsreserve ist es wichtig, dass der öffentliche Auftraggeber den Nutzer über solche Folgen aufklärt, bevor er einen Antrag stellt. Diese

Sicherheitsvorkehrungen beschränken sich auf die Beantragung und Bereitstellung von Diensten im Rahmen der EU-Cybersicherheitsreserve und wirken sich nicht auf den Austausch von Informationen in anderen Zusammenhängen, etwa bei Beschaffungen im Rahmen der EU-Cybersicherheitsreserve, aus.

(29) Angesichts der zunehmenden Risiken und der wachsenden Zahl von Sicherheitsvorfällen, von denen die Mitgliedstaaten betroffen sind, ist es erforderlich, ein Krisenhilfeinstrument, nämlich den Cybernotfallmechanismus einzurichten, um die Resilienz der Union gegenüber schwerwiegenden Cybersicherheitsvorfällen, Cybersicherheitsvorfällen großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfällen zu verbessern und die Maßnahmen der Mitgliedstaaten durch finanzielle Hilfe zur Unterstützung der Abwehrbereitschaft, Reaktion auf Sicherheitsvorfälle und anfänglichen Wiederherstellung wesentlicher Dienste zu ergänzen. Da eine vollständige Wiederherstellung nach einem Sicherheitsvorfall ein umfassender Prozess zur Wiederherstellung des vor diesem Sicherheitsvorfall verzeichneten Zustands der Funktionsfähigkeit der von dem Sicherheitsvorfall betroffenen Einrichtung ist und sich als langwierig und äußerst kostspielig erweisen könnte, sollte sich die Unterstützung aus der EU-Cybersicherheitsreserve auf die Anfangsphase des Wiederherstellungsprozesses beschränken und die Wiederherstellung der grundlegenden Funktionen der Systeme ermöglichen. Der Cybernotfallmechanismus sollte eine rasche und wirksame Hilfeleistung unter festgelegten Umständen und unter klaren Bedingungen sowie eine sorgfältige Überwachung und Bewertung der Verwendung der Ressourcen ermöglichen. Während die primäre Zuständigkeit für Prävention, Vorsorge und Bewältigung bei Sicherheitsvorfällen 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).

(30) Der Cybernotfallmechanismus sollte die Mitgliedstaaten in Ergänzung ihrer eigenen Maßnahmen und Ressourcen sowie anderer bestehender Unterstützungsoptionen — wie der von der ENISA gemäß ihrem Mandat bereitgestellten Dienste, der koordinierten Reaktion und der Unterstützung durch das CSIRTs-Netz, der Unterstützung der Eindämmung durch das EU-CyCLONe sowie der Amtshilfe zwischen den Mitgliedstaaten, auch im Zusammenhang mit Artikel 42 Absatz 7 EUV und der gemäß dem Beschluss (GASP) 2017/2315 des Rates eingerichteten Teams für die rasche Reaktion auf Cybervorfälle im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ) ([15]) — im Falle einer Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes sowie der anschließenden anfänglichen Wiederherstellung unterstützen. Er sollte der Notwendigkeit Rechnung tragen, dass spezialisierte Mittel zur Verfügung stehen müssen, um die Abwehrbereitschaft und die Reaktion auf diese Sicherheitsvorfälle sowie die anschließende Wiederherstellung in der gesamten Union und in mit dem Programm „Digitales Europa“ assoziierten Drittländern zu unterstützen.

(31) Diese Verordnung lässt die Verfahren und Rahmen für die Koordinierung der Krisenreaktion auf Unionsebene, insbesondere die Richtlinie (EU) 2022/2555, das mit dem Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates eingerichtete Katastrophenschutzverfahren der Union ([16]), die IPCR-Regelung und die Empfehlung (EU) 2017/1584 der Kommission ([17]), unberührt. Die Unterstützung im Rahmen des Cybernotfallmechanismus kann 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, wobei dem zivilen Charakter des Cybernotfallmechanismus Rechnung zu tragen ist. Die Unterstützung im Rahmen des Cybernotfallmechanismus kann Maßnahmen ergänzen, die im Zusammenhang mit Artikel 42 Absatz 7 EUV durchgeführt werden, einschließlich der Hilfe, die ein Mitgliedstaat einem anderen Mitgliedstaat leistet, die Teil der gemeinsamen Reaktion der Union und der Mitgliedstaaten sind oder die in den in Artikel 222 AEUV genannten Situationen durchgeführt werden. Die Umsetzung dieser Verordnung sollte gegebenenfalls auch mit der Umsetzung der Maßnahmen im Rahmen des Instrumentariums für die Cyberdiplomatie koordiniert werden.

(32) 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, der ENISA, den Mitgliedstaaten und gegebenenfalls dem ECCC gesorgt werden. Wenn Mitgliedstaaten Unterstützung im Rahmen des Cybernotfallmechanismus beantragen, sollten sie einschlägige Informationen bereitstellen, die den Unterstützungsbedarf begründen.

(33) 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, Fähigkeiten, 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 Krisen 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 Sicherheitsvorfällen nach einem genau festgelegten

([15]) Beschluss (GASP) 2017/2315 des Rates vom 11. Dezember 2017 über die Begründung der Ständigen Strukturierten Zusammenarbeit (SSZ) und über die Liste der daran teilnehmenden Mitgliedstaaten (ABl. L 331, 14.12.2017, S. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/oj).

([16]) 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).

([17]) 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).

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 Sicherstellung der Einhaltung der Verpflichtungen aus der Richtlinie (EU) 2022/2555 durch die Mitgliedstaaten unberührt. Im Rahmen des Cybernotfallmechanismus sollte Unterstützung für Maßnahmen zur Stärkung der Abwehrbereitschaft sowie für Maßnahmen zur Reaktion auf Sicherheitsvorfälle bereitgestellt werden, um die Auswirkungen von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes abzumildern, die anfängliche Wiederherstellung zu unterstützen oder die grundlegenden Funktionen von in Sektoren mit hoher Kritikalität tätigen Einrichtungen, oder von in sonstigen kritischen Sektoren tätigen Einrichtungen erbrachten Dienste wiederherzustellen.

(34) Im Rahmen der Maßnahmen in Bezug auf die Abwehrbereitschaft sollten — unter anderem durch Übungs- und Schulungsmaßnahmen — koordinierte Tests und eine koordinierte Bewertung der Cybersicherheit von in Sektoren mit hoher Kritikalität 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 nach Konsultation der ENISA, der NIS-Kooperationsgruppe und des EU-CyCLONe regelmäßig einschlägige Sektoren oder Teilsektoren festlegen, die für eine finanzielle Unterstützung für koordinierte Tests der Abwehrbereitschaft auf Unionsebene in Betracht kommen sollten. Die Sektoren oder Teilsektoren sollten aus den in Anhang I der Richtlinie (EU) 2022/2555 aufgeführten Sektoren mit hoher Kritikalität ausgewählt werden. Die koordinierten Tests der Abwehrbereitschaft sollten auf gemeinsamen Risikoszenarien und -methodiken beruhen. Bei der Auswahl der Sektoren und der Entwicklung von Risikoszenarien sollten einschlägige unionsweite Risikobewertungen und -szenarien — einschließlich der Notwendigkeit, Doppelarbeit zu vermeiden — berücksichtigt werden, beispielsweise die in den Schlussfolgerungen des Rates zur Entwicklung der Cyberabwehr der Europäischen Union geforderten Risikobewertungen und -szenarien durch die Kommission, den Hohen Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) und die NIS-Kooperationsgruppe in Abstimmung mit den einschlägigen zivilen und militärischen Einrichtungen und Agenturen sowie bestehenden Netzwerken, einschließlich des EU-CyCLONe, sowie die Risikobewertung von Kommunikationsnetzen und -infrastruktur, die im gemeinsamen Ministeraufruf von Nevers gefordert und von der NIS-Kooperationsgruppe mit Unterstützung der Kommission und der ENISA und in Zusammenarbeit mit dem durch die Verordnung (EU) 2018/1971 des Europäischen Parlaments und des Rates eingesetzten Gremium Europäischer Regulierungsstellen für elektronische Kommunikation ([18]) durchgeführt wird, die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 auf Unionsebene durchzuführenden koordinierten Risikobewertungen in Bezug auf die Sicherheit von kritischen Lieferketten und das Testen der digitalen operationalen Resilienz gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates ([19]). Bei der Auswahl der Sektoren sollte auch der Empfehlung des Rates für eine unionsweite koordinierte Vorgehensweise zur Stärkung der Resilienz kritischer Infrastruktur Rechnung getragen werden.

(35) Darüber hinaus sollte der Cybernotfallmechanismus Unterstützung für andere Maßnahmen in Bezug auf die Abwehrbereitschaft und die Abwehrbereitschaft in anderen Sektoren bieten, die nicht von den koordinierten Tests der Abwehrbereitschaft von in Sektoren mit hoher Kritikalität tätigen Einrichtungen oder in sonstigen kritischen Sektoren tätigen Einrichtungen erfasst werden. Diese Maßnahmen könnten verschiedene Arten nationaler Maßnahmen in Bezug auf die Abwehrbereitschaft umfassen.

(36) Erhalten die Mitgliedstaaten Finanzhilfen zur Unterstützung von Maßnahmen in Bezug auf die Abwehrbereitschaft, können sich in Sektoren mit hoher Kritikalität tätige Einrichtungen an diesen Maßnahmen auf freiwilliger Basis beteiligen. Es hat sich bewährt, dass teilnehmende Einrichtungen im Anschluss an solche Maßnahmen einen Abhilfeplan für die Umsetzung von sich möglicherweise daraus ergebenden Empfehlungen für spezifische Maßnahmen erstellen, um den größtmöglichen Nutzen aus der Maßnahme in Bezug auf die Abwehrbereitschaft zu ziehen. Zwar ist es wichtig, dass die Mitgliedstaaten teilnehmende Einrichtungen im Rahmen dieser Maßnahmen zur Erstellung und Umsetzung solcher Abhilfepläne auffordern, doch sind die Mitgliedstaaten aufgrund der vorliegenden Verordnung weder verpflichtet noch befugt, solche Forderungen durchzusetzen. Diese Forderungen lassen die Anforderungen an Einrichtungen sowie die Aufsichtsbefugnisse der zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 unberührt.

(37) Über den Cybernotfallmechanismus sollte auch Unterstützung für Maßnahmen zur Reaktion auf Sicherheitsvorfälle bereitgestellt werden, um die Auswirkungen von schwerwiegenden Cybersicherheitsvorfällen, Cybersicherheitsvorfällen großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle abzumildern, die anfängliche 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 Sicherheitsvorfällen für die Bürgerinnen und Bürger zu gewährleisten.

([18]) Verordnung (EU) 2018/1971 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Einrichtung des Gremiums europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und der Agentur zur Unterstützung des GEREK (GEREK-Büro), zur Änderung der Verordnung (EU) 2015/2120 und zur Aufhebung der Verordnung (EG) Nr. 1211/2009 (ABl. L 321 vom 17.12.2018, S. 1).

([19]) 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 (ABl. L 333 vom 27.12.2022, S. 1).

(38) Der Cybernotfallmechanismus sollte einen Mitgliedstaat bei der technischen Unterstützung eines anderen, von einem schwerwiegenden Cybersicherheitsvorfall oder Cybersicherheitsvorfall großen Ausmaßes betroffenen Mitgliedstaat helfen, auch mithilfe von CSIRTs gemäß Artikel 11 Absatz 3 Buchstabe f der Richtlinie (EU) 2022/2555. Mitgliedstaaten, die eine solche Unterstützung leisten, sollte es gestattet sein, 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.

(39) Da private Unternehmen bei der Erkennung von, der Abwehrbereitschaft gegenüber und der Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle eine wesentliche Rolle spielen, ist es wichtig, den Wert einer freiwilligen unentgeltlichen Zusammenarbeit mit solchen Unternehmen anzuerkennen, bei der diese Unternehmen bei Cybersicherheitsvorfällen und -krisen großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfällen sowie bei diesbezüglichen Krisen Dienste anbieten, ohne dafür eine Vergütung zu verlangen. Die ENISA könnte in Zusammenarbeit mit dem EU-CyCLONe die Entwicklung solcher unentgeltlichen Initiativen überwachen und deren Vereinbarkeit mit den gemäß dieser Verordnung für vertrauenswürdige Anbieter verwalteter Sicherheitsdienste geltenden Kriterien unterstützen, auch in Bezug auf die Vertrauenswürdigkeit und die Erfahrung von privaten Unternehmen und ihre Fähigkeit, sensible Informationen auf sichere Weise zu verarbeiten.

(40) Im Rahmen des Cybernotfallmechanismus sollte schrittweise eine EU-Cybersicherheitsreserve auf Unionsebene eingerichtet werden, die aus Diensten vertrauenswürdiger Anbieter verwalteter Sicherheitsdienste besteht, um die Reaktion und anfängliche Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen, Cybersicherheitsvorfällen großen Ausmaßes oder einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfällen mit Auswirkungen auf die Mitgliedstaaten, die Organe, Einrichtungen oder sonstigen Stellen der Union oder mit dem Programm „Digitales Europa“ assoziierte Drittländer zu unterstützen. Die EU-Cybersicherheitsreserve sollte die Verfügbarkeit und Einsatzbereitschaft der betroffenen Dienste gewährleisten. Sie sollte daher Dienste umfassen, die vorab zugesagt werden, darunter auch abrufbereite Kapazitäten, die kurzfristig eingesetzt werden können. Die Dienste der EU-Cybersicherheitsreserve sollten dazu dienen, den nationalen Behörden bei der Unterstützung betroffener in Sektoren mit hoher Kritikalität tätiger Einrichtungen oder betroffener in sonstigen kritischen Sektoren tätiger Einrichtungen ergänzend zu ihren eigenen Maßnahmen auf nationaler Ebene zu helfen. Die Dienste der EU-Cybersicherheitsreserve sollten auch dazu dienen können, die Organe, Einrichtungen und sonstigen Stellen der Union unter ähnlichen Bedingungen zu unterstützen. Die EU-Cybersicherheitsreserve könnte ferner dazu beitragen, die Wettbewerbsposition von Industrie und Dienstleistungen der Digitalwirtschaft in der Union, einschließlich Kleinstunternehmen, kleiner und mittlerer Unternehmen sowie Start-up-Unternehmen, zu stärken, unter anderem durch die Schaffung von Anreizen für Investitionen in Forschung und Innovation. Bei der Beschaffung der Dienste für die EU-Cybersicherheitsreserve ist es wichtig, den Europäischen Kompetenzrahmen für Cybersicherheit der ENISA zu berücksichtigen. Wenn die Nutzer Unterstützung aus der EU-Cybersicherheitsreserve beantragen, sollten sie ihrem Antrag angemessene Informationen über die betroffene Einrichtung und die potenziellen Auswirkungen, Informationen über die beantragten Dienste der EU-Cybersicherheitsreserve sowie Informationen darüber beifügen, welche Unterstützung die betroffene Einrichtung auf nationaler Ebene erhält, und dies sollte bei der Prüfung des Antrags des Antragstellers berücksichtigt werden. Zur Sicherstellung der Komplementarität mit anderen Formen der Unterstützung, die der betroffenen Einrichtung zur Verfügung stehen, sollte der Antrag, sofern diese verfügbar sind, auch Informationen über bestehende vertragliche Vereinbarungen über Sicherheitsvorfall-Notdienste und Dienste zur anfänglichen Wiederherstellung sowie Versicherungsverträge, die möglicherweise diese Art von Sicherheitsvorfällen abdecken, umfassen.

(41) Um die wirksame Verwendung von Unionsmitteln sicherzustellen, sollten vorab zugesagte Dienste im Rahmen der EU-Cybersicherheitsreserve gemäß dem entsprechenden Vertrag in Dienste in Bezug auf die Abwehrbereitschaft im Zusammenhang mit der Prävention von und der Reaktion auf Sicherheitsvorfälle umgewandelt werden, falls diese vorab zugesagten Dienste während des Zeitraums, für den sie vorab zugesagt wurden, nicht für die Reaktion auf Sicherheitsvorfälle in Anspruch genommen werden. Diese Dienste sollten die unter der Leitung des ECCC durchgeführten Maßnahmen in Bezug auf die Abwehrbereitschaft ergänzen und nicht duplizieren.

(42) Anträge auf Unterstützung aus der EU-Cybersicherheitsreserve, die von den für das Cyberkrisenmanagement zuständigen Behörden der Mitgliedstaaten und den CSIRTs oder vom CERT-EU im Namen der Organe, Einrichtungen und sonstigen Stellen der Union gestellt werden, sollten vom öffentlichen Auftraggeber geprüft werden. Wenn die ENISA mit der Verwaltung und dem Betrieb der EU-Cybersicherheitsreserve betraut wurde, ist der öffentliche Auftraggeber die ENISA. Von mit dem Programm „Digitales Europa“ assoziierten Drittländern gestellte Anträge auf Unterstützung sollten von der Kommission geprüft werden. Die ENISA könnte eine sichere Plattform einrichten, um die Einreichung und Prüfung von Anträgen auf Unterstützung zu erleichtern.

(43) Gehen mehrere Anträge gleichzeitig ein, so sollten diese gemäß den in der vorliegenden Verordnung festgelegten Kriterien priorisiert werden. Mit Blick auf die allgemeinen Ziele dieser Verordnung sollten diese Kriterien die Tragweite und Schwere des Sicherheitsvorfalls, die Art der betroffenen Einrichtung, die potenziellen Auswirkungen des Sicherheitsvorfalls auf betroffene Mitgliedstaaten und Nutzer, den potenziellen grenzüberschreitenden Charakter des Sicherheitsvorfalls und das Ausbreitungsrisiko sowie die vom Nutzer bereits ergriffenen Maßnahmen zur Unterstützung der Reaktion und der anfänglichen Wiederherstellung umfassen. Angesichts dieser Ziele und der

Tatsache, dass Anträge von Nutzern aus den Mitgliedstaaten ausschließlich darauf abzielen, dass unionsweit in Sektoren mit hoher Kritikalität tätige Einrichtungen oder in sonstigen kritischen Sektoren tätige Einrichtungen unterstützt werden, sollte den Anträgen von Nutzern aus den Mitgliedstaaten eine höhere Priorität eingeräumt werden, wenn zwei oder mehr Anträge auf der Grundlage der genannten Kriterien als gleichwertig eingestuft werden. Dies gilt unbeschadet etwaiger Verpflichtungen der Mitgliedstaaten im Rahmen einschlägiger Aufnahmevereinbarungen, Maßnahmen zum Schutz und zur Unterstützung der Organe, Einrichtungen und sonstigen Stellen der Union zu ergreifen.

(44) Die Kommission sollte die Gesamtverantwortung für die einwandfreie Umsetzung der EU-Cybersicherheitsreserve tragen. Angesichts der umfangreichen Erfahrungen, die die ENISA im Zusammenhang mit der Aktion zur Förderung der Cybersicherheit gesammelt hat, ist die ENISA die für die Umsetzung der EU-Cybersicherheitsreserve am besten geeignete Agentur. Deshalb sollte die Kommission die ENISA teilweise oder, sofern die Kommission dies für angezeigt hält, gänzlich mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve betrauen. Diese Betrauung sollte gemäß den geltenden Vorschriften der Verordnung (EU, Euratom) 2024/2509 erfolgen und insbesondere an die Erfüllung der einschlägigen Bedingungen für die Unterzeichnung einer Beitragsvereinbarung geknüpft sein. Alle Aspekte des Betriebs und der Verwaltung der EU-Cybersicherheitsreserve, mit denen die ENISA nicht betraut wurde, sollten direkt durch die Kommission verwaltet werden, auch vor der Unterzeichnung der Beitragsvereinbarung.

(45) Bei der Einrichtung und dem Einsatz der EU-Cybersicherheitsreserve sowie bei entsprechenden Nachbereitungen sollten die Mitgliedstaaten eine zentrale Rolle spielen. Da die Verordnung (EU) 2021/694 der einschlägige Basisrechtsakt für Maßnahmen zur Umsetzung der EU-Cybersicherheitsreserve ist, sollten die im Rahmen der EU-Cybersicherheitsreserve durchgeführten Maßnahmen in den in Artikel 24 der Verordnung (EU) 2021/694 genannten Arbeitsprogrammen vorgesehen werden. Gemäß Absatz 6 des genannten Artikels sind diese Arbeitsprogramme von der Kommission im Wege von Durchführungsrechtsakten nach dem Prüfverfahren anzunehmen. Darüber hinaus sollte die Kommission in Abstimmung mit der NIS-Kooperationsgruppe die Prioritäten sowie den weiteren Entwicklungsprozess der EU-Cybersicherheitsreserve festlegen.

(46) Die im Rahmen der EU-Cybersicherheitsreserve geschlossenen Verträge sollten die Geschäftsbeziehungen zwischen Unternehmen sowie die bestehenden Verpflichtungen zwischen der betroffenen Einrichtung bzw. den Nutzern und dem Diensteanbieter unberührt lassen.

(47) Im Hinblick auf die Auswahl privater Dienstleister für die Bereitstellung von Diensten im Rahmen der EU-Cybersicherheitsreserve muss eine Reihe von Mindestkriterien und -anforderungen festgelegt werden, die in die Ausschreibung für die Auswahl dieser Anbieter aufgenommen werden sollten, damit die Bedürfnisse der Behörden und der in Sektoren mit hoher Kritikalität tätigen Einrichtungen oder in sonstigen kritischen Sektoren tätigen Einrichtungen in den Mitgliedstaaten erfüllt werden. Um den besonderen Bedürfnissen der Mitgliedstaaten Rechnung zu tragen, sollte der öffentliche Auftraggeber bei der Beschaffung von Diensten für die EU-Cybersicherheitsreserve gegebenenfalls Auswahlkriterien und -anforderungen entwickeln, die über die in der vorliegenden Verordnung festgelegten Kriterien und Anforderungen hinausgehen. Es ist wichtig, die Beteiligung kleinerer, auf regionaler und lokaler Ebene tätiger Anbieter zu fördern.

(48) Bei der Auswahl von in die EU-Cybersicherheitsreserve einzubeziehenden Anbietern sollte der öffentliche Auftraggeber darauf abzielen sicherzustellen, dass die EU-Cybersicherheitsreserve insgesamt betrachtet Anbieter umfasst, die den sprachlichen Erfordernissen der Nutzer gerecht werden können. Zu diesem Zweck sollte sich der öffentliche Auftraggeber vor der Ausarbeitung von Ausschreibungsbedingungen erkundigen, ob die potenziellen Nutzer der EU-Cybersicherheitsreserve spezifische sprachliche Erfordernisse haben, damit die Unterstützungsdienste im Rahmen der EU-Cybersicherheitsreserve in einer der Amtssprachen der Organe der Union oder der Mitgliedstaaten erbracht werden können, die von dem Nutzer bzw. der betroffenen Einrichtung wahrscheinlich verstanden wird. Wenn ein Nutzer in Bezug auf Unterstützungsdienste im Rahmen der EU-Cybersicherheitsreserve mehr als eine Sprache benötigt und diese Dienste für diesen Nutzer in den entsprechenden Sprachen beschafft wurden, sollte der Nutzer in seinem Antrag auf Unterstützung aus der EU-Cybersicherheitsreserve angeben können, in welcher dieser Sprachen die Dienste in Bezug auf den spezifischen Sicherheitsvorfall, für den der Antrag gestellt wird, erbracht werden sollten.

(49) Zur Unterstützung der Einrichtung der EU-Cybersicherheitsreserve ist es wichtig, dass die Kommission die ENISA um die Ausarbeitung eines Schemas für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste gemäß der Verordnung (EU) 2019/881 in den vom Cybernotfallmechanismus abgedeckten Bereichen ersucht.

(50) 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 die Kommission oder das EU-CyCLONe die ENISA ersuchen können, mit Unterstützung des CSIRTs-Netzes und mit Zustimmung der betroffenen Mitgliedstaaten, Cyberbedrohungen, bekannte ausnutzbare 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 dem betroffenen Mitgliedstaat, den einschlägigen

Interessenträgern, einschließlich Vertretern des Privatsektors, der Kommission und anderer einschlägiger Organe, Einrichtungen und sonstiger Stellen der Union, einen Bericht über die Überprüfung des Sicherheitsvorfalls erstellen. Aufbauend auf der Zusammenarbeit mit Interessenträgern, einschließlich des Privatsektors, sollte der Bericht über die Überprüfung bestimmter Sicherheitsvorfälle darauf abzielen, die Ursachen, Auswirkungen und Maßnahmen zur Eindämmung eines Sicherheitsvorfalls nach seinem Auftreten zu bewerten. Besonderes Augenmerk sollte auf die Beiträge und Erkenntnisse gelegt werden, die von den Anbietern verwalteter Sicherheitsdienste übermittelt werden, die die in dieser Verordnung geforderten Bedingungen der größtmöglichen beruflichen Integrität, Unparteilichkeit und des erforderlichen technischen Fachwissens erfüllen. Der Bericht sollte an das EU-CyCLONe, das CSIRTs-Netz und die Kommission übermittelt werden und zur Information über deren Arbeit sowie die Arbeit der ENISA verwendet werden. Betrifft der Sicherheitsvorfall ein mit dem Programm „Digitales Europa" assoziiertes Drittland, so sollte die Kommission den Bericht auch an den Hohen Vertreter weiterleiten.

(51) Angesichts des unvorhersehbaren Charakters von Cyberangriffen 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 einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle zu reagieren, auch zum Schutz der Union als Ganzes bei, insbesondere ihres Binnenmarkts und ihrer Industrie. Durch derartige Aktivitäten könnte ein zusätzlicher Beitrag zur Cyberdiplomatie der Union geleistet werden. Daher sollten mit dem Programm „Digitales Europa" assoziierte Drittländer beantragen können, in ihrem gesamten Hoheitsgebiet oder in Teilen davon aus der EU-Cybersicherheitsreserve unterstützt zu werden, sofern dies in dem Abkommen über die Assoziierung des betreffenden Drittlands mit dem Programm „Digitales Europa" vorgesehen ist. Die Fördermittel für mit dem Programm „Digitales Europa" 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 anfänglichen Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfällen abdecken.

(52) Die in dieser Verordnung festgelegten Bedingungen für die EU-Cybersicherheitsreserve und für vertrauenswürdige Anbieter verwalteter Sicherheitsdienste sollten auch bei der Unterstützung der mit dem Programm „Digitales Europa" assoziierten Drittländer gelten. Mit dem Programm „Digitales Europa" assoziierte Drittländer sollten Unterstützung aus der EU-Cybersicherheitsreserve beantragen können, wenn es sich bei den betroffenen Einrichtungen, für die sie Unterstützung aus der EU-Cybersicherheitsreserve beantragen, um in Sektoren mit hoher Kritikalität tätige Einrichtungen oder in sonstigen kritischen Sektoren tätige Einrichtungen handelt, und wenn die festgestellten Sicherheitsvorfälle zu erheblichen operativen Störungen führen oder Ausbreitungseffekte der Union haben könnten. Mit dem Programm „Digitales Europa" assoziierte Drittländer sollten nur dann Unterstützung erhalten können, wenn eine solche Unterstützung in dem Abkommen über ihre Assoziierung mit dem Programm „Digitales Europa" ausdrücklich vorgesehen ist. Darüber hinaus sollten solche Drittländer nur dann weiterhin für Unterstützung in Betracht kommen, wenn drei Kriterien erfüllt sind. Erstens sollte das Drittland die einschlägigen Bestimmungen des genannten Abkommens uneingeschränkt einhalten. Zweitens sollte das Drittland angesichts des komplementären Charakters der EU-Cybersicherheitsreserve angemessene Schritte zur Vorbereitung auf schwerwiegende Cybersicherheitsvorfälle und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle unternommen haben. Drittens sollte die Bereitstellung von Unterstützung aus der EU-Cybersicherheitsreserve im Einklang mit der Politik der Union gegenüber dem betroffenen Land, ihren allgemeinen Beziehungen zu diesem Land sowie mit ihren anderweitigen Sicherheitsstrategien erfolgen. Bei der Überprüfung der Einhaltung dieses dritten Kriteriums sollte die Kommission den Hohen Vertreter konsultieren, um bezüglich der Gewährung einer solchen Unterstützung für eine Abstimmung mit der Gemeinsamen Außen- und Sicherheitspolitik zu sorgen.

(53) Die Unterstützung von mit dem Programm „Digitales Europa" assoziierten Drittländern kann Auswirkungen auf die Beziehungen zu Drittländern sowie auf die Sicherheitspolitik der Union haben, auch im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik und der Gemeinsamen Sicherheits- und Verteidigungspolitik. Daher sollten dem Rat Durchführungsbefugnisse in Bezug darauf übertragen werden, die Gewährung einer solchen Unterstützung zu genehmigen und den Zeitraum festzulegen, in dem die Unterstützung bereitgestellt werden kann. Der Rat sollte auf der Grundlage eines Vorschlags der Kommission tätig werden und dabei die Überprüfung der drei Kriterien durch die Kommission gebührend berücksichtigen. Gleiches sollte für Verlängerungen solcher Rechtsakte sowie für Vorschläge zu ihrer Änderung oder Aufhebung gelten. Ist der Rat in Ausnahmefällen der Auffassung, dass sich die Umstände in Bezug auf das dritte Kriterium erheblich geändert haben, so sollte er von sich aus — ohne die Vorlage eines Vorschlags durch die Kommission abzuwarten — tätig werden können, um einen Durchführungsrechtsakt zu ändern oder aufzuheben. Im Falle solcher erheblichen Änderungen ist es wahrscheinlich, dass dringendes Handeln erforderlich ist, dass es zu besonders weitreichenden Auswirkungen auf die Beziehungen zu Drittländern kommt und dass es keiner vorherigen eingehenden Überprüfung durch die Kommission bedarf. Darüber hinaus sollte die Kommission im Zusammenhang mit Anträgen auf Unterstützung, die von mit dem Programm „Digitales Europa" assoziierten Drittländern gestellten werden, und der Umsetzung der diesen Drittländern gewährten Unterstützung mit dem Hohen Vertreter zusammenarbeiten. Die Kommission sollte zudem etwaige Stellungnahmen der ENISA zu diesen Anträgen und der jeweiligen Unterstützung berücksichtigen. Die Kommission sollte den Rat über das Ergebnis der Prüfung der Anträge, einschließlich der diesbezüglichen einschlägigen Erwägungen, sowie über die erbrachten Dienste unterrichten.

(54) In der Mitteilung der Kommission vom 18. April 2023 über die Akademie für Cybersicherheitskompetenzen wird anerkannt, dass ein Mangel an qualifizierten Fachkräften herrscht. Solche Kompetenzen werden benötigt, damit die Ziele der vorliegenden Verordnung verfolgt werden können. Die Union braucht dringend Fachkräfte mit den Kompetenzen und Fähigkeiten, die nötig sind, um Cyberangriffe zu verhindern und zu entdecken und davon abzuschrecken, die Union einschließlich ihrer wichtigsten Infrastruktur dagegen zu verteidigen und ihre Resilienz sicherzustellen. Zu diesem Zweck ist es wichtig, die Zusammenarbeit zwischen den Interessenträgern, einschließlich aus dem Privatsektor, der Wissenschaft und dem öffentlichen Sektor, zu fördern. Ebenso wichtig ist es, dass in allen Gebieten der Union Synergien in Bezug auf Investitionen in die allgemeine und berufliche Bildung geschaffen werden, um die Konzipierung von Schutzvorkehrungen zu fördern, damit die Abwanderung hoch qualifizierter Kräfte verhindert wird und sich die Qualifikationslücke in gewissen Regionen nicht stärker vergrößert als in anderen. Es ist dringend erforderlich, die Qualifikationslücke auf dem Gebiet der Cybersicherheit zu schließen, wobei ein besonderer Schwerpunkt auf der Verringerung des Geschlechtergefälles bei den Fachkräften im Bereich der Cybersicherheit liegen sollte, damit die Präsenz von Frauen bei Gestaltungsprozessen im Bereich der digitalen Governance und ihre Beteiligung daran gestärkt wird.

(55) Für die Förderung der Innovation im digitalen Binnenmarkt ist es wichtig, die Forschung und Innovation auf dem Gebiet der Cybersicherheit zu stärken, um zur Stärkung der Resilienz der Mitgliedstaaten und zur offenen strategischen Autonomie der Union — zwei Ziele der vorliegenden Verordnung — beizutragen. Synergien sind von entscheidender Bedeutung, um die Zusammenarbeit und Koordinierung zwischen den verschiedenen Interessenträgern, einschließlich aus dem Privatsektor, der Zivilgesellschaft und der Wissenschaft, zu stärken.

(56) Die vorliegende Verordnung sollte den in der gemeinsamen Erklärung des Europäischen Parlaments, des Rates und der Kommission vom 26. Januar 2022 mit dem Titel „Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade“ vorgesehenen Verpflichtungen in Bezug auf den Schutz der Interessen der Demokratien, Bürgerinnen und Bürger, Unternehmen und öffentlichen Einrichtungen der Union vor Cybersicherheitsrisiken und Cyberkriminalität, darunter Datenschutzverletzungen und Identitätsdiebstahl bzw. -manipulation, Rechnung tragen.

(57) Zur Ergänzung bestimmter nicht wesentlicher Elemente dieser Verordnung sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, in denen die Art und die Anzahl der für die EU-Cybersicherheitsreserve benötigten Notfalldienste festgelegt werden. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([20]) niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(58) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse in Bezug darauf übertragen werden, die Verfahrensmodalitäten für die Zuweisung von Unterstützungsdiensten im Rahmen der EU-Cybersicherheitsreserve näher zu spezifizieren. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([21]) ausgeübt werden.

(59) Unbeschadet der Vorschriften über den Jahreshaushaltsplan der Union gemäß den Verträgen sollte die Kommission bei der Bewertung des Haushalts- und Personalbedarfs der ENISA den sich aus der vorliegenden Verordnung ergebenden Verpflichtungen Rechnung tragen.

(60) Die Kommission sollte die in dieser Verordnung festgelegten Maßnahmen regelmäßig einer Bewertung unterziehen. Die erste Bewertung sollte binnen zwei Jahren nach dem Tag des Inkrafttretens dieser Verordnung durchgeführt werden, und anschließende Bewertungen sollten mindestens alle vier Jahre erfolgen, wobei es den Zeitplan für die Überarbeitung des gemäß Artikel 312 AEUV aufgestellten mehrjährigen Finanzrahmens zu berücksichtigen gilt. Die Kommission sollte dem Europäischen Parlament und dem Rat einen Bericht über die erzielten Fortschritte übermitteln. Bei der Bewertung der verschiedenen erforderlichen Elemente, einschließlich des Umfangs der im Rahmen des europäischen Warnsystems für Cybersicherheit weitergegebenen Informationen, sollte sich die Kommission ausschließlich auf Informationen stützen, die ohne Weiteres verfügbar sind oder freiwillig bereitgestellt werden. Angesichts der geopolitischen Entwicklungen sowie zur Gewährleistung der Kontinuität und Weiterentwicklung der in dieser Verordnung vorgesehenen Maßnahmen in der Zeit nach 2027, ist es wichtig, dass die Kommission die Notwendigkeit prüft, im mehrjährigen Finanzrahmen für 2028 bis 2034 angemessene Haushaltsmittel vorzusehen.

([20]) ABl. L 123 vom 12.5.2016, S. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

([21]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) Das die Ziele dieser Verordnung, nämlich die Wettbewerbsposition von Industrie und Dienstleistungen der Digitalwirtschaft in der Union zu stärken und zur technologischen Souveränität und offenen strategischen Autonomie der Union im Bereich der Cybersicherheit beizutragen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 EUV verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Ziele

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

a) eines europaweiten Netzes von Cyber-Hubs (im Folgenden „europäisches Warnsystem für Cybersicherheit"), um Fähigkeiten zur koordinierten Erkennung und gemeinsamen Lageerfassung aufzubauen und zu verbessern;

b) eines Cybernotfallmechanismus zur Unterstützung der Mitgliedstaaten bei der Vorsorge für, Bewältigung und Eindämmung der Auswirkungen von und Einleitung der Wiederherstellung nach schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes und zur Unterstützung anderer Nutzer bei der Reaktion auf Cybersicherheitsvorfällen großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle;

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

(2) Mit dieser Verordnung werden die allgemeinen Ziele verfolgt, die Wettbewerbsposition von Industrie und Dienstleistungen der Digitalwirtschaft in der Union, einschließlich Kleinstunternehmen, kleiner und mittlerer Unternehmen sowie Start-up-Unternehmen, zu stärken und zur technologischen Souveränität und offenen strategischen Autonomie der Union im Bereich der Cybersicherheit beizutragen, unter anderem durch die Förderung von Innovationen im digitalen Binnenmarkt. Diese Ziele werden durch eine Stärkung der Solidarität auf Unionsebene, des Cybersicherheitsökosystems und der Cyberresilienz der Mitgliedstaaten sowie durch die Entwicklung der Fähigkeiten, des Fachwissens und der Kompetenzen von Fachkräften im Bereich der Cybersicherheit verfolgt.

(3) Zur Verwirklichung der in Absatz 2 genannten allgemeinen Ziele werden die folgenden spezifischen Ziele verfolgt:

a) Stärkung der gemeinsamen koordinierten Kapazitäten der Union zur Erkennung und gemeinsamen Lageerfassung im Bereich der Cyberbedrohungen und Sicherheitsvorfälle;

b) Stärkung der Abwehrbereitschaft der in Sektoren mit hoher Kritikalität tätigen Einrichtungen oder in sonstigen kritischen Sektoren tätigen Einrichtungen in der gesamten Union und Stärkung der Solidarität durch den Aufbau von Kapazitäten für koordinierte Tests der Abwehrbereitschaft, für die Reaktion auf schwerwiegende Cybersicherheitsvorfälle, Cybersicherheitsvorfälle großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle sowie für die anschließende Wiederherstellung, unter anderem durch die Möglichkeit, Unionsunterstützung für die Bewältigung von Cybersicherheitsvorfällen auch mit dem Programm „Digitales Europa" assoziierten Drittländern zur Verfügung zu stellen;

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

(4) Die Maßnahmen im Rahmen dieser Verordnung werden unter gebührender Berücksichtigung der Zuständigkeiten der Mitgliedstaaten durchgeführt und ergänzen die Tätigkeiten des CSIRTs-Netzes, des EU-CyCLONe und der NIS-Kooperationsgruppe.

(5) Diese Verordnung lässt die grundlegenden staatlichen Funktionen der Mitgliedstaaten, darunter auch die Wahrung der territorialen Unversehrtheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit, unberührt. Insbesondere die nationale Sicherheit fällt weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten.

(6) Die Weitergabe oder der Austausch von Informationen im Rahmen dieser Verordnung, die gemäß Unions- oder nationalen Vorschriften vertraulich sind, wird auf die Weitergabe und den Austausch solcher Daten beschränkt, die für den Zweck dieser Weitergabe oder dieses Austauschs relevant und verhältnismäßig sind. Bei der Weitergabe oder dem Austausch von Informationen werden die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen der betreffenden Einrichtungen geschützt. Dies umfasst nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:

1. „grenzübergreifender Cyber-Hub“ ist eine durch eine schriftliche Konsortialvereinbarung eingerichtete länderübergreifende Plattform, auf der nationale Cyber-Hubs aus mindestens drei Mitgliedstaaten in einer koordinierten Netzstruktur zusammenarbeiten und die dazu bestimmt ist, die Überwachung, Erkennung und Analyse von Cyberbedrohungen zu verbessern um Cybersicherheitsvorfälle zu verhindern und die Gewinnung von Erkenntnissen in Bezug auf Cyberbedrohungen zu unterstützen, insbesondere durch den Austausch relevanter — gegebenenfalls anonymisierter — Daten und Informationen sowie die gemeinsame Nutzung modernster Instrumente und die gemeinsame Entwicklung von Erkennungs-, Analyse-, Präventions- und Schutzfähigkeiten gegenüber Cyberangriffen in einem vertrauenswürdigen Umfeld;

2. „Aufnahmekonsortium“ ist ein Konsortium aus beteiligten Mitgliedstaaten, die vereinbart haben, einen grenzübergreifenden Cyber-Hub einzurichten und hierzu an der Beschaffung von Instrumenten, Infrastruktur oder Diensten sowie dessen Betrieb mitzuwirken;

3. „CSIRT“ ist ein gemäß Artikel 10 der Richtlinie (EU) 2022/2555 benanntes oder eingerichtetes Computer-Notfallteam (CSIRT);

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

5. „in Sektoren mit hoher Kritikalität tätige Einrichtungen“ sind die Arten von Einrichtungen, die in Anhang I der Richtlinie (EU) 2022/2555 aufgeführt sind;

6. „in sonstigen kritischen Sektoren tätige Einrichtungen“ sind die Arten von Einrichtungen, die in Anhang II der Richtlinie (EU) 2022/2555 aufgeführt sind;

7. „Risiko“ ist ein Risiko im Sinne des Artikels 6 Nummer 9 der Richtlinie (EU) 2022/2555;

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

9. „Sicherheitsvorfall“ ist ein Sicherheitsvorfall im Sinne des Artikels 6 Nummer 6 der Richtlinie (EU) 2022/2555;

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

11. „schwerwiegender Sicherheitsvorfall“ ist ein schwerwiegender Sicherheitsvorfall im Sinne des Artikels 3 Nummer 8 der Verordnung (EU, Euratom) 2023/2841 des Europäischen Parlaments und des Rates ([22]);

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

([22]) Verordnung (EU, Euratom) 2023/2841 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union (ABl. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13. „einem Cybersicherheitsvorfall großen Ausmaßes gleichwertiger Sicherheitsvorfall“ ist im Falle von Organen, Einrichtungen und sonstigen Stellen der Union ein schwerwiegender Sicherheitsvorfall und im Falle von mit dem Programm „Digitales Europa“ assoziierten Drittländern ein Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines mit dem Programm „Digitales Europa“ assoziierten betroffenen Drittlands übersteigt;

14. „mit dem Programm ‚Digitales Europa‘ assoziiertes Drittland“ ist ein Drittland, das mit der Union ein Abkommen geschlossen hat, die seine Teilnahme am Programm „Digitales Europa“ gemäß Artikel 10 der Verordnung (EU) 2021/694 ermöglicht;

15. „öffentlicher Auftraggeber“ ist die Kommission oder, insoweit die ENISA gemäß Artikel 14 Absatz 5 mit der Verwaltung und dem Betrieb der EU-Cybersicherheitsreserve betraut wurde, die ENISA;

16. „Anbieter verwalteter Sicherheitsdienste“ ist ein Anbieter verwalteter Sicherheitsdienste im Sinne des Artikels 6 Nummer 40 der Richtlinie (EU) 2022/2555;

17. „vertrauenswürdige Anbieter verwalteter Sicherheitsdienste“ sind Anbieter verwalteter Sicherheitsdienste, die gemäß Artikel 17 ausgewählt wurden, um in die EU-Cybersicherheitsreserve einbezogen zu werden.

KAPITEL II

DAS EUROPÄISCHE WARNSYSTEM FÜR CYBERSICHERHEIT

Artikel 3

Einrichtung des europäischen Warnsystems für Cybersicherheit

(1) Es wird ein europaweites Infrastrukturnetz aus freiwillig teilnehmenden nationalen und grenzübergreifenden Cyber-Hubs eingerichtet, das europäische Warnsystem für Cybersicherheit, um die Entwicklung fortgeschrittener Fähigkeiten in der Union zur Erkennung, Analyse und Datenverarbeitung in Bezug auf Cyberbedrohungen sowie die Prävention von Sicherheitsvorfällen in der Union zu unterstützen.

(2) Das europäische Warnsystem für Cybersicherheit hat folgende Aufgaben:

a) Leisten eines Beitrags zu einem besseren Schutz und einer besseren Reaktion auf Cyberbedrohungen durch die Unterstützung von und die Zusammenarbeit mit sowie die Verstärkung der Fähigkeiten der einschlägigen Einrichtungen, insbesondere CSIRTs, dem CSIRTs-Netz, dem EU-CyCLONe und den gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden;

b) Zusammenführung relevanter Daten und Informationen über Cyberbedrohungen und Sicherheitsvorfälle aus verschiedenen Quellen innerhalb der grenzübergreifenden Cyber-Hubs sowie Weitergabe analysierter oder aggregierter Informationen durch grenzübergreifende Cyber-Hubs, gegebenenfalls auch an das CSIRTs-Netz;

c) Sammlung und Unterstützung der Erstellung hochwertiger, handlungsrelevanter Informationen und Erkenntnisse über Cyberbedrohungen unter Nutzung modernster Instrumente und fortgeschrittener Technologien sowie Weitergabe solcher Informationen und Erkenntnisse über Cyberbedrohungen;

d) Leisten eines Beitrags zur Verbesserung der koordinierten Erkennung von Cyberbedrohungen und zur gemeinsamen Lageerfassung in der gesamten Union sowie zur Abgabe von Warnmeldungen, gegebenenfalls auch durch die Formulierung konkreter Empfehlungen an Einrichtungen;

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

(3) Maßnahmen zur Umsetzung des europäischen Warnsystems für Cybersicherheit werden mit Mitteln aus dem Programm „Digitales Europa“ (DEP) unterstützt und gemäß der Verordnung (EU) 2021/694, insbesondere deren spezifischen Ziel 3, durchgeführt.

Artikel 4

Nationale Cyber-Hubs

(1) Beschließt ein Mitgliedstaat, sich am europäischen Warnsystem für Cybersicherheit zu beteiligen, so benennt er für die Zwecke der vorliegenden Verordnung einen nationalen Cyber-Hub bzw. richtet einen solchen nationalen Cyber-Hub ein.

(2) Ein nationaler Cyber-Hub ist eine einzige Einrichtung, die der Aufsicht eines Mitgliedstaats untersteht. Dabei kann es sich um ein CSIRT oder gegebenenfalls um eine nationale Behörde für das Cyberkrisenmanagement, um eine andere gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannte bzw. eingerichtete zuständige Behörde oder um eine andere Einrichtung handeln. Der nationale Cyber-Hub,

a) verfügt über die Kapazität, als Bezugspunkt und Zugangstor zu anderen öffentlichen und privaten Organisationen auf nationaler Ebene für die Sammlung und Auswertung von Informationen über Cyberbedrohungen und Sicherheitsvorfälle zu fungieren und zu einem grenzübergreifenden Cyber-Hub gemäß Artikel 5 beizutragen, und

b) verfügt über die Fähigkeit, Daten und Informationen, die in Bezug auf Cyberbedrohungen und Sicherheitsvorfälle relevant sind, wie beispielsweise Erkenntnisse über Cyberbedrohungen, zu erkennen, zu aggregieren und zu analysieren, insbesondere unter Einsatz modernster Technologien, wobei das Ziel darin besteht, Sicherheitsvorfälle zu verhindern.

(3) Bei der Ausübung der in Absatz 2 des vorliegenden Artikels genannten Funktionen können nationale Cyber-Hubs mit Einrichtungen des Privatsektors zusammenarbeiten, um zwecks Erkennung und Prävention von Cyberbedrohungen und Sicherheitsvorfällen relevante Daten und Informationen auszutauschen, auch mit sektoralen und sektorübergreifenden Gemeinschaften wesentlicher und wichtiger Einrichtungen gemäß Artikel 3 der Richtlinie (EU) 2022/2555. Sofern angezeigt und mit dem Unionsrecht und dem nationalen Recht vereinbar können die von nationalen Cyber-Hubs angeforderten oder erhaltenen Informationen Telemetrie-, Sensor- und Protokolldaten umfassen.

(4) Ein gemäß Artikel 9 Absatz 1 ausgewählter Mitgliedstaat verpflichtet sich, für seinen nationalen Cyber-Hub einen Antrag auf Teilnahme an einem grenzübergreifenden Cyber-Hub zu stellen.

Artikel 5

Grenzübergreifende Cyber-Hubs

(1) Haben sich mindestens drei Mitgliedstaaten verpflichtet, die Zusammenarbeit ihrer nationalen Cyber-Hubs bei der Koordinierung ihrer Tätigkeiten zur Erkennung und Überwachung von Cyberbedrohungen sicherzustellen, können diese Mitgliedstaaten für die Zwecke der vorliegenden Verordnung ein Aufnahmekonsortium bilden.

(2) Ein Aufnahmekonsortium setzt sich aus mindestens drei beteiligten Mitgliedstaaten zusammen, die vereinbart haben, einen grenzübergreifenden Cyber-Hub gemäß Absatz 4 einzurichten und hierzu an der Beschaffung von Instrumenten, Infrastruktur oder Diensten sowie dessen Betrieb mitzuwirken.

(3) Wird ein Aufnahmekonsortium gemäß Artikel 9 Absatz 3 ausgewählt, schließen seine Mitglieder eine schriftliche Konsortialvereinbarung, in der

a) die internen Regelungen für die Durchführung der Aufnahme- und Nutzungsvereinbarung gemäß Artikel 9 Absatz 3 festgelegt werden,

b) das grenzübergreifende Cyber-Hubs des Aufnahmekonsortiums eingerichtet wird und

c) die gemäß Artikel 6 Absätze 1 und 2 erforderlichen spezifischen Klauseln enthalten sind.

(4) Ein grenzübergreifender Cyber-Hub ist eine länderübergreifende Plattform, die durch eine schriftliche Konsortialvereinbarung gemäß Absatz 3 eingerichtet wurde. In einem grenzübergreifenden Cyber-Hub arbeiten die nationalen Cyber-Hubs der Mitgliedstaaten des Aufnahmekonsortiums in einer koordinierten Netzstruktur zusammen. Er ist dazu bestimmt, die Überwachung, Erkennung und Analyse von Cyberbedrohungen zu verbessern, Sicherheitsvorfälle zu verhindern und die Gewinnung von Erkenntnissen in Bezug auf Cyberbedrohungen zu unterstützen, insbesondere durch den Austausch relevanter — und gegebenenfalls anonymisierter — Daten und Informationen sowie die gemeinsame Nutzung modernster Instrumente und die gemeinsame Entwicklung von Erkennungs-, Analyse-, Präventions- und Schutzfähigkeiten gegenüber Cyberangriffen in einem vertrauenswürdigen Umfeld.

(5) Ein grenzübergreifender Cyber-Hub wird zu rechtlichen Zwecken durch ein Mitglied des entsprechenden Aufnahmekonsortiums, das als Koordinierungsstelle fungiert, oder durch das Aufnahmekonsortium, falls es Rechtspersönlichkeit besitzt, vertreten. Die Verantwortung für die Einhaltung der vorliegenden Verordnung und der Aufnahme- und Nutzungsvereinbarung durch den grenzübergreifenden Cyber-Hub wird in der in Absatz 3 genannten schriftlichen Konsortialvereinbarung verteilt.

(6) Ein Mitgliedstaat kann mit Zustimmung der Mitglieder des Aufnahmekonsortiums einem bestehenden Aufnahmekonsortium beitreten. Die in Absatz 3 genannte schriftliche Konsortialvereinbarung und die Aufnahme- und Nutzungsvereinbarung werden entsprechend geändert. Die Eigentumsrechte des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) an den bereits gemeinsam mit diesem Aufnahmekonsortium beschafften Instrumenten, Infrastruktur oder Diensten bleiben davon unberührt.

Artikel 6

Zusammenarbeit und Weitergabe von Informationen in und zwischen grenzübergreifenden Cyber-Hubs

(1) Die Mitglieder eines Aufnahmekonsortiums stellen sicher, dass ihre nationalen Cyber-Hubs untereinander im grenzübergreifenden Cyber-Hub gemäß der in Artikel 5 Absatz 3 genannten schriftlichen Konsortialvereinbarung relevante Informationen, gegebenenfalls anonymisiert, weitergeben, darunter Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Erkennung von Cyberangriffen, sofern durch diese Weitergabe von Informationen

a) die Erkennung von Cyberbedrohungen unterstützt und verbessert und die Fähigkeiten des CSIRTs-Netzes, Sicherheitsvorfälle zu verhindern und darauf zu reagieren oder ihre Folgen einzudämmen, gestärkt werden,

b) das Cybersicherheitsniveau erhöht wird, beispielsweise indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die Fähigkeit solcher Bedrohungen, sich zu verbreiten, eingedämmt bzw. behindert wird und eine Reihe von Abwehrfähigkeiten, 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 von Informationen unter den Mitgliedern des Aufnahmekonsortiums gemäß Absatz 1 und die Bedingungen, unter denen diese Informationen weiterzugeben sind;

b) ein Governance-Rahmen, der Klarstellungen und Anreize in Bezug auf die Weitergabe von relevanten Informationen, gegebenenfalls anonymisiert, gemäß Absatz 1 durch alle Teilnehmer bietet;

c) Zielsetzungen für Beiträge zur Entwicklung fortgeschrittener Instrumente und Technologien, darunter auch Instrumente der künstlichen Intelligenz und der Datenanalyse.

In der schriftlichen Konsortialvereinbarung kann festgelegt werden, dass die in Absatz 1 genannten Informationen gemäß dem Unionsrecht und dem nationalen Recht weiterzugeben sind.

(3) Grenzübergreifende Cyber-Hubs schließen Kooperationsvereinbarungen miteinander, in denen die Grundsätze in Bezug auf die Interoperabilität und die Weitergabe von Informationen zwischen den grenzübergreifenden Cyber-Hubs festgelegt werden. Die grenzübergreifenden Cyber-Hubs unterrichten die Kommission über die geschlossenen Kooperationsvereinbarungen.

(4) Die Weitergabe von Informationen gemäß Absatz 1 zwischen grenzübergreifenden Cyber-Hubs wird durch ein hohes Maß an Interoperabilität sichergestellt. Zur Unterstützung dieser Interoperabilität gibt die ENISA unverzüglich und in jedem Fall bis zum 5. Februar 2026 in enger Abstimmung mit der Kommission Leitlinien zur Interoperabilität heraus, in denen insbesondere Formate und Protokolle für den Informationsaustausch festgelegt werden, die internationalen Standards und bewährten Verfahren sowie der Funktionsweise bestehender grenzübergreifender Cyber-Hubs Rechnung tragen. Die in Kooperationsvereinbarungen der grenzübergreifenden Cyber-Hubs festgelegten Interoperabilitätsanforderungen beruhen auf den von ENISA herausgegebenen Leitlinien.

Artikel 7

Zusammenarbeit und Weitergabe von Informationen mit Netzen auf Unionsebene

(1) Grenzübergreifende Cyber-Hubs und das CSIRTs-Netz arbeiten insbesondere zwecks Weitergabe von Informationen eng zusammen. Zu diesem Zweck vereinbaren sie Verfahrensregelungen für die Zusammenarbeit und die Weitergabe relevanter Informationen sowie — unbeschadet des Absatzes 2 — welche Arten von Informationen weiterzugeben sind.

(2) Wenn die grenzübergreifenden Cyber-Hubs Informationen über einen potenziellen oder andauernden Cybersicherheitsvorfall großen Ausmaßes erhalten, stellen sie zu Zwecken der gemeinsamen Lageerfassung sicher, dass den Behörden der Mitgliedstaaten und der Kommission über das EU-CyCLONe und das CSIRTs-Netz unverzüglich relevante Informationen und Frühwarnungen übermittelt werden.

Artikel 8

Sicherheit

(1) Die am europäischen Warnsystem für Cybersicherheit beteiligten Mitgliedstaaten sorgen für ein hohes Maß an Cybersicherheit, einschließlich Vertraulichkeit und Datensicherheit, sowie an physischer Sicherheit des Netzes des europäischen Warnsystems für Cybersicherheit und stellen sicher, dass das Netz angemessen verwaltet und kontrolliert wird, um es vor Bedrohungen zu schützen und seine Sicherheit sowie die Sicherheit der Systeme, einschließlich der über das Netz weitergegebenen Daten und Informationen, sicherzustellen.

(2) Die am europäischen Warnsystem für Cybersicherheit beteiligten Mitgliedstaaten stellen sicher, dass durch die Weitergabe von Informationen gemäß Artikel 6 Absatz 1 innerhalb des europäischen Warnsystems für Cybersicherheit an Einrichtungen, bei denen es sich nicht um eine Behörde oder öffentliche Stelle eines Mitgliedstaats handelt, die Sicherheitsinteressen der Union oder der Mitgliedstaaten nicht beeinträchtigt werden.

Artikel 9

Finanzierung des europäischen Warnsystems für Cybersicherheit

(1) Im Anschluss an eine Aufforderung zur Interessenbekundung für Mitgliedstaaten, die beabsichtigen, sich am europäischen Warnsystem für Cybersicherheit zu beteiligen, wählt der ECCC die Mitgliedstaaten aus, die sich mit dem ECCC an der gemeinsamen Beschaffung von Instrumenten, Infrastruktur oder Diensten beteiligen, um gemäß Artikel 4 Absatz 1 benannte oder eingerichtete Cyber-Hubs einzurichten oder deren Fähigkeiten auszubauen. Das ECCC kann den ausgewählten Mitgliedstaaten Finanzhilfen zur Finanzierung des Betriebs dieser Instrumente, Infrastruktur oder Dienste gewähren. Der Finanzbeitrag der Union deckt bis zu 50 % der Beschaffungskosten der Instrumente, Infrastruktur oder Dienste und bis zu 50 % der Betriebskosten. Die verbleibenden Kosten werden von den ausgewählten Mitgliedstaaten getragen. Bevor das Verfahren für die Beschaffung der Instrumente, Infrastruktur oder Dienste eingeleitet wird, schließen das ECCC und die ausgewählten Mitgliedstaaten eine Aufnahme- und Nutzungsvereinbarung, in der die Verwendung der Instrumente, Infrastruktur oder Dienste geregelt wird.

(2) Nimmt der nationale Cyber-Hub eines Mitgliedstaats binnen zwei Jahren ab dem Zeitpunkt, zu dem die Instrumente, Infrastruktur und Dienste beschafft wurden oder zu dem er Finanzhilfen erhalten hat — je nachdem, welches Ereignis früher eintritt —, nicht an einem grenzübergreifenden Cyber-Hub teil, so kommt der Mitgliedstaat nicht für weitere Unterstützung durch die Union im Rahmen des vorliegenden Kapitels infrage, bis er einem grenzübergreifenden Cyber-Hub beitritt.

(3) Im Anschluss an eine Aufforderung zu Interessenbekundung wählt das ECCC ein Aufnahmekonsortium zur Teilnahme an einer gemeinsamen Beschaffung von Instrumenten, Infrastruktur und Diensten mit dem ECCC aus. Das ECCC kann dem Aufnahmekonsortium eine Finanzhilfe zur Finanzierung des Betriebs der Instrumente, Infrastruktur oder Dienste gewähren. Der Finanzbeitrag der Union deckt bis zu 75 % der Beschaffungskosten der Instrumente, Infrastruktur oder Dienste und bis zu 50 % der Betriebskosten. Die verbleibenden Kosten werden von dem Aufnahmekonsortium getragen. Bevor das Verfahren für die Beschaffung der Instrumente, Infrastruktur oder Dienste eingeleitet wird, schließen das ECCC und das Aufnahmekonsortium eine Aufnahme- und Nutzungsvereinbarung, in der die Verwendung der Instrumente, Infrastruktur oder Dienste geregelt wird.

(4) Das ECCC arbeitet mindestens alle zwei Jahre eine Aufstellung der Instrumente, Infrastruktur oder Dienste von angemessener Qualität, die für die Einrichtung nationaler oder grenzübergreifender Cyber-Hubs oder den Ausbau ihrer Fähigkeiten erforderlich sind, sowie ihrer Verfügbarkeit aus, auch von Rechtsträgern, die in einem Mitgliedstaat niedergelassen sind oder als dort niedergelassen gelten und die von einem Mitgliedstaat oder von Staatsangehörigen eines Mitgliedstaats kontrolliert werden. Bei der Ausarbeitung dieser Aufstellung konsultiert das ECCC das CSIRTs-Netz, bestehende grenzübergreifende Cyber-Hubs, die ENISA und die Kommission.

KAPITEL III

CYBERNOTFALLMECHANISMUS

Artikel 10

Einrichtung des Cybernotfallmechanismus

(1) Ein Cybernotfallmechanismus wird eingerichtet, um die Verbesserung der Resilienz der Union gegenüber Cyberbedrohungen und die Vorbereitung auf schwerwiegende Cybersicherheitsvorfälle, Cybersicherheitsvorfälle großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle sowie Eindämmung deren kurzfristiger Auswirkungen im Geiste der Solidarität zu unterstützen.

(2) Im Falle der Mitgliedstaaten werden die im Rahmen des Cybernotfallmechanismus vorgesehenen Maßnahmen auf Antrag bereitgestellt; sie ergänzen die Bemühungen und Maßnahmen der Mitgliedstaaten zur Vorbereitung auf Sicherheitsvorfälle, die Reaktion darauf sowie die anschließende Wiederherstellung.

(3) Die Maßnahmen zur Umsetzung des Cybernotfallmechanismus werden mit Mitteln aus dem Programm „Digitales Europa“ unterstützt und gemäß der Verordnung (EU) 2021/694, insbesondere deren spezifischen Ziel 3, durchgeführt.

(4) Die Maßnahmen im Rahmen des Cybernotfallmechanismus werden in erster Linie durch das ECCC gemäß der Verordnung (EU) 2021/887 durchgeführt. Maßnahmen zur Umsetzung der EU-Cybersicherheitsreserve gemäß Artikel 11 Buchstabe b der vorliegenden Verordnung werden jedoch von der Kommission und der ENISA durchgeführt.

Artikel 11

Arten von Maßnahmen

Der Cybernotfallmechanismus unterstützt folgende Arten von Maßnahmen:

a) Maßnahmen in Bezug auf die Abwehrbereitschaft, und zwar

   i) koordinierte Tests der Abwehrbereitschaft von in Sektoren mit hoher Kritikalität tätigen Einrichtungen in der gesamten Union gemäß Artikel 12,

   ii) sonstige Maßnahmen in Bezug auf die Abwehrbereitschaft in Bezug auf in Sektoren mit hoher Kritikalität tätige Einrichtungen oder in sonstigen kritischen Sektoren tätige Einrichtungen gemäß Artikel 13;

b) Maßnahmen zur Unterstützung der Reaktion auf schwerwiegende Cybersicherheitsvorfälle, Cybersicherheitsvorfälle großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle sowie zur Einleitung der Wiederherstellung durch vertrauenswürdige Anbieter verwalteter Sicherheitsdienste, die sich an der gemäß Artikel 14 eingerichteten EU-Cybersicherheitsreserve beteiligen;

c) Maßnahmen zur Unterstützung der Amtshilfe gemäß Artikel 18.

Artikel 12

Koordinierte Tests der Abwehrbereitschaft von Einrichtungen

(1) Der Cybernotfallmechanismus unterstützt freiwillige koordinierte Tests der Abwehrbereitschaft von in Sektoren mit hoher Kritikalität tätigen Einrichtungen.

(2) Die koordinierten Tests der Abwehrbereitschaft können Maßnahmen in Bezug auf die Abwehrbereitschaft, wie Penetrationstests, und Bedrohungsanalysen umfassen.

(3) Die Unterstützung für Maßnahmen in Bezug auf die Abwehrbereitschaft nach dem vorliegenden Artikel wird den Mitgliedstaaten in erster Linie in Form von Finanzhilfen gewährt, wobei die in den einschlägigen Arbeitsprogrammen gemäß Artikel 24 der Verordnung (EU) 2021/694 festgelegten Bedingungen gelten.

(4) Zur Unterstützung der in Artikel 11 Buchstabe a Ziffer i der vorliegenden Verordnung genannten koordinierten Tests der Abwehrbereitschaft von Einrichtungen in der gesamten Union legt die Kommission nach Konsultation der NIS-Kooperationsgruppe, des EU-CyCLONe und der ENISA die betroffenen Sektoren oder Teilsektoren aus den in

Anhang I der Richtlinie (EU) 2022/2555 aufgeführten Sektoren mit hoher Kritikalität fest, für die ein Aufruf zur Einreichung von Vorschlägen für die Gewährung von Finanzhilfen veröffentlicht werden kann. Die Teilnahme der Mitgliedstaaten an diesen Aufrufen zur Einreichung von Vorschlägen ist freiwillig.

(5) Bei der Bestimmung der Sektoren bzw. Teilsektoren gemäß Absatz 4 berücksichtigt die Kommission koordinierte Risikobewertungen und Resilienztests auf Unionsebene sowie deren Ergebnisse.

(6) Die NIS-Kooperationsgruppe entwickelt in Zusammenarbeit mit der Kommission, dem Hohen Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) und der ENISA sowie — im Rahmen des Mandats des EU-CyCLONe — mit dem EU-CyCLONe gemeinsame Risikoszenarien und -methodiken für die Durchführung der koordinierten Tests der Abwehrbereitschaft gemäß Artikel 11 Buchstabe a Ziffer i bzw. gegebenenfalls für sonstige Maßnahmen in Bezug auf die Abwehrbereitschaft gemäß Absatz 1 Buchstabe a Ziffer ii des genannten Artikels.

(7) Beteiligt sich eine in einem Sektor mit hoher Kritikalität tätige Einrichtung freiwillig an koordinierten Tests der Abwehrbereitschaft und ergeben sich aus diesen Tests Empfehlungen für spezifische Maßnahmen, die von der teilnehmenden Einrichtung in einen Abhilfeplan aufgenommen werden könnten, so überprüft die für die koordinierten Tests der Abwehrbereitschaft zuständige Behörde des betreffenden Mitgliedstaats gegebenenfalls die Weiterverfolgung dieser Maßnahmen durch die teilnehmenden Einrichtungen zwecks Verbesserung der Abwehrbereitschaft.

Artikel 13

Sonstige Maßnahmen in Bezug auf die Abwehrbereitschaft

(1) Im Rahmen des Cybernotfallmechanismus werden überdies Maßnahmen in Bezug auf die Abwehrbereitschaft unterstützt, die nicht unter Artikel 12 fallen. Diese Maßnahmen umfassen Maßnahmen in Bezug auf die Abwehrbereitschaft in Bezug auf Einrichtungen, die in nicht für koordinierte Tests der Abwehrbereitschaft gemäß Artikel 12 bestimmten Sektoren tätig sind. Im Rahmen solcher Maßnahmen können die Überwachung von Schwachstellen und Risiken sowie Übungs- und Schulungsmaßnahmen unterstützt werden.

(2) Die Unterstützung für Maßnahmen in Bezug auf die Abwehrbereitschaft nach dem vorliegenden Artikel wird den Mitgliedstaaten auf Antrag in erster Linie in Form von Finanzhilfen gewährt, wobei die in den einschlägigen Arbeitsprogrammen gemäß Artikel 24 der Verordnung (EU) 2021/694 genannten Bedingungen gelten.

Artikel 14

Einrichtung der EU-Cybersicherheitsreserve

(1) Eine EU-Cybersicherheitsreserve wird eingerichtet, um den in Absatz 3 genannten Nutzern auf Antrag bei der Reaktion bzw. der Unterstützung der Reaktion auf schwerwiegende Cybersicherheitsvorfälle, Cybersicherheitsvorfälle großen Ausmaßes oder einem Cybersicherheitsvorfall großen Ausmaßes gleichwertiger Sicherheitsvorfälle und bei der Einleitung der Wiederherstellung nach solchen Sicherheitsvorfällen Hilfe zu leisten.

(2) Die EU-Cybersicherheitsreserve besteht aus Notdiensten vertrauenswürdiger Anbieter verwalteter Sicherheitsdienste, die nach den in Artikel 17 Absatz 2 festgelegten Kriterien ausgewählt wurden. Die EU-Cybersicherheitsreserve kann vorab zugesagte Dienste umfassen. Vorab zugesagte Dienste eines vertrauenswürdigen Anbieters verwalteter Sicherheitsdienste können in Dienste in Bezug auf die Abwehrbereitschaft im Zusammenhang mit der Prävention von und der Reaktion auf Sicherheitsvorfälle umgewandelt werden, wenn diese vorab zugesagten Dienste während des Zeitraums, für den sie vorab zugesagt wurden, nicht zwecks Reaktion auf Sicherheitsvorfälle in Anspruch genommen werden. Die EU-Cybersicherheitsreserve kann auf Antrag in allen Mitgliedstaaten, in Organen, Einrichtungen und sonstigen Stellen der Union und in mit dem Programm „Digitales Europa“ assoziierten Drittländern gemäß Artikel 19 Absatz 1 zum Einsatz kommen.

(3) Bei den Nutzern der von der EU-Cybersicherheitsreserve erbrachten Dienste handelt es sich um

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) CERT-EU gemäß Artikel 13 der Verordnung (EU, Euratom) 2023/2841,

c) zuständige Behörden wie Computer-Notfallteams oder Behörden für das Cyberkrisenmanagement von mit dem Programm „Digitales Europa“ assoziierten Drittländern gemäß Artikel 19 Absatz 8.

(4) Die Kommission trägt die Gesamtverantwortung für die Umsetzung der EU-Cybersicherheitsreserve. Die Kommission legt die Prioritäten und die Entwicklung der EU-Cybersicherheitsreserve in Abstimmung mit der NIS-Kooperationsgruppe und gemäß 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. Diese Prioritäten werden alle zwei Jahre überprüft und gegebenenfalls überarbeitet. Die Kommission informiert das Europäische Parlament und den Rat über diese Prioritäten und alle entsprechenden Überarbeitungen.

(5) Unbeschadet der Gesamtverantwortung der Kommission für die Umsetzung der EU-Cybersicherheitsreserve gemäß Absatz 4 des vorliegenden Artikels und vorbehaltlich einer Beitragsvereinbarung im Sinne von Artikel 2 Nummer 19 der Verordnung (EU, Euratom) 2024/2509 betraut die Kommission die ENISA ganz oder teilweise mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve. Aspekte, mit denen die ENISA nicht betraut wird, werden direkt durch die Kommission verwaltet.

(6) Die ENISA arbeitet mindestens alle zwei Jahre eine Aufstellung der von den in Absatz 3 Buchstaben a und b des vorliegenden Artikels genannten Nutzern benötigten Dienste aus. Diese Aufstellungen umfassen auch die Verfügbarkeit dieser Dienste, auch von Rechtsträgern, die in einem Mitgliedstaat niedergelassen sind oder als dort niedergelassen gelten und die von einem Mitgliedstaat oder von einem Staatsangehörigen eines Mitgliedstaats kontrolliert werden. Im Rahmen dieser Aufstellungen der Verfügbarkeit bewertet die ENISA die für die Ziele der EU-Cybersicherheitsreserve relevanten Kompetenzen und Kapazitäten der Fachkräfte der Union im Bereich der Cybersicherheit. Bei der Ausarbeitung der Aufstellungen konsultiert die ENISA die NIS-Kooperationsgruppe, das EU-CyCLONe, die Kommission und gegebenenfalls den gemäß Artikel 10 der Verordnung (EU, Euratom) 2023/2841 eingerichteten Interinstitutionellen Cybersicherheitsbeirat. Darüber hinaus konsultiert die ENISA bei der Ausarbeitung der Aufstellungen einschlägige Interessenträger der Cybersicherheitsbranche, einschließlich der Anbieter verwalteter Sicherheitsdienste. Nach Unterrichtung des Rates und nach Konsultation des EU-CyCLONe, der Kommission sowie gegebenenfalls des Hohen Vertreters arbeitet die ENISA eine ähnliche Aufstellung der Erfordernisse der in Absatz 3 Buchstabe c des vorliegenden Artikels genannten Nutzer aus.

(7) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 23 zu erlassen, um die vorliegende Verordnung durch die Festlegung der Art und der Anzahl der für die EU-Cybersicherheitsreserve erforderlichen Notdienste zu ergänzen. Bei der Ausarbeitung dieser delegierten Rechtsakte berücksichtigt die Kommission die in Absatz 6 des vorliegenden Artikels genannten Aufstellungen und kann sich mit der NIS-Kooperationsgruppe und der ENISA beraten und mit diesen zusammenarbeiten.

Artikel 15

Beantragung der Unterstützung aus der EU-Cybersicherheitsreserve

(1) Die in Artikel 14 Absatz 3 genannten Nutzer können Dienste der EU-Cybersicherheitsreserve beantragen, um die Reaktion auf schwerwiegende Cybersicherheitsvorfälle, Cybersicherheitsvorfälle großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle zu unterstützen und die anschließende Wiederherstellung einzuleiten.

(2) Um Unterstützung aus der EU-Cybersicherheitsreserve zu erhalten, ergreifen die in Artikel 14 Absatz 3 genannten Nutzer alle geeigneten Maßnahmen zur Eindämmung der Auswirkungen des Sicherheitsvorfalls, für den die Unterstützung beantragt wird, und stellen gegebenenfalls direkte technische Unterstützung und andere Ressourcen zur Unterstützung der Reaktion auf den Sicherheitsvorfall und der anschließenden Wiederherstellung bereit.

(3) Unterstützungsanträge werden dem öffentlichen Auftraggeber wie folgt übermittelt:

a) im Falle der in Artikel 14 Absatz 3 Buchstabe a der vorliegenden Verordnung genannten Nutzern über die gemäß Artikel 8 Absatz 3 der Richtlinie (EU) 2022/2555 benannte oder eingerichtete zentrale Anlaufstelle;

b) im Falle des in Artikel 14 Absatz 3 Buchstabe b genannten Nutzers durch diesen Nutzer;

c) im Falle der in Artikel 14 Absatz 3 Buchstabe c genannten Nutzern über die in Artikel 19 Absatz 9 genannte zentrale Anlaufstelle.

(4) Im Falle von Anträgen von in Artikel 14 Absatz 3 Buchstabe a genannten Nutzern unterrichten die Mitgliedstaaten das CSIRTs-Netz und gegebenenfalls das EU-CyCLONe über die Anträge ihrer Nutzer auf Sicherheitsvorfall-Notdienste und auf Unterstützung bei der anfänglichen Wiederherstellung nach diesem Artikel.

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

a) angemessene Informationen über die betroffene Einrichtung und die möglichen Auswirkungen des Sicherheitsvorfalls auf

   i) im Falle von in Artikel 14 Absatz 3 Buchstabe a genannten Nutzern, die betroffenen Mitgliedstaaten und Nutzer, einschließlich des Risikos einer Ausbreitung auf einen anderen Mitgliedstaat,

ii) im Falle des in Artikel 14 Absatz 3 Buchstabe b genannten Nutzers, betroffene Organe, Einrichtungen und sonstige Stellen der Union,

iii) im Falle von in Artikel 14 Absatz 3 Buchstabe c genannten Nutzern, die betroffenen mit dem Programm „Digitales Europa“ assoziierten Länder;

b) Informationen über die beantragten Dienste, zusammen mit der geplanten Verwendung der beantragten Unterstützung, einschließlich einer Bedarfsschätzung;

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

d) sofern angezeigt, verfügbare Informationen über andere Formen der Unterstützung, die der betroffenen Einrichtung zur Verfügung stehen.

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

(7) Die Kommission kann im Wege von Durchführungsrechtsakten die genauen Verfahrensmodalitäten für die Beantragung der Unterstützungsdienste der EU-Cybersicherheitsreserve und für die Beantwortung solcher Anträge gemäß dem vorliegenden Artikel, Artikel 16 Absatz 1 und Artikel 19 Absatz 10 festlegen, einschließlich der Modalitäten für die Einreichung dieser Anträge und die Übermittlung der Antworten sowie Vorlagen für die in Artikel 16 Absatz 9 genannten Berichte. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 24 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 16

Umsetzung der Unterstützung aus der EU-Cybersicherheitsreserve

(1) Im Falle von Anträgen von in Artikel 14 Absatz 3 Buchstaben a und b genannten Nutzern werden Anträge auf Unterstützung aus der EU-Cybersicherheitsreserve vom öffentlichen Auftraggeber geprüft. Eine Antwort wird den in Artikel 14 Absatz 3 Buchstaben a und b genannten Nutzern unverzüglich und in jedem Fall spätestens 48 Stunden nach Einreichung des Antrags übermittelt, damit die Wirksamkeit der Unterstützung sichergestellt ist. Der öffentliche Auftraggeber unterrichtet den Rat und die Kommission über die Ergebnisse des Verfahrens.

(2) In Bezug auf im Zuge der Beantragung und Bereitstellung der Dienste der EU-Cybersicherheitsreserve weitergegebene Informationen sind alle an der Anwendung der vorliegenden Verordnung beteiligten Parteien verpflichtet,

a) die Verwendung und Weitergabe dieser Informationen auf das zur Erfüllung ihrer Pflichten oder Aufgaben im Rahmen der vorliegenden Verordnung erforderliche Maß zu beschränken,

b) Informationen, die gemäß Unionsrecht und nationalem Recht vertraulich oder als Verschlusssache eingestuft sind, nur gemäß diesem Recht zu verwenden und weiterzugeben und

c) einen wirksamen, effizienten und sicheren Informationsaustausch, gegebenenfalls durch Verwendung und Einhaltung der einschlägigen Protokolle für die Weitergabe von Informationen, einschließlich des Traffic Light Protocol.

(3) Bei der Prüfung einzelner Anträge gemäß Artikel 16 Absatz 1 und Artikel 19 Absatz 10 prüft der öffentliche Auftraggeber bzw. die Kommission zunächst, ob die in Artikel 15 Absätze 1 und 2 genannten Kriterien erfüllt sind. Ist dies der Fall, prüft er bzw. sie die angemessene Dauer und die angemessene Art der Unterstützung unter Berücksichtigung des in Artikel 1 Absatz 3 Buchstabe b genannten Ziels und gegebenenfalls der im Folgenden genannten Kriterien:

a) Ausmaß und Schwere des Sicherheitsvorfalls,

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

c) potenzielle Auswirkungen des Sicherheitsvorfalls auf betroffene Mitgliedstaaten, Organe, Einrichtungen oder sonstige Stellen der Union oder mit dem Programm „Digitales Europa“ assoziierte Drittländer;

d) potenziell grenzüberschreitender Charakter des Sicherheitsvorfalls und Risiko einer Ausbreitung auf andere Mitgliedstaaten, Organe, Einrichtungen oder sonstige Stellen der Union oder mit dem Programm „Digitales Europa“ assoziierte Drittländer;

e) vom Nutzer ergriffene Maßnahmen zur Unterstützung der Reaktion und Bemühungen zur anfänglichen Wiederherstellung gemäß Artikel 15 Absatz 2.

(4) Im Falle mehrerer gleichzeitig eingehender Anträge von in Artikel 14 Absatz 3 genannten Nutzern werden — unbeschadet des Grundsatzes der loyalen Zusammenarbeit zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union — die in Absatz 3 des vorliegenden Artikels genannten Kriterien berücksichtigt, sofern sie relevant sind. Dabei wird Anträgen von Nutzern aus den Mitgliedstaaten eine höhere Priorität eingeräumt, wenn zwei oder mehr Anträge auf der Grundlage dieser Kriterien als gleichwertig eingestuft werden. Wurde gemäß Artikel 14 Absatz 5 die ENISA ganz oder teilweise mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve betraut, arbeiten die ENISA und die Kommission eng zusammen, um Anträge gemäß dem vorliegenden Absatz zu priorisieren.

(5) Die Bereitstellung der Dienste im Rahmen der EU-Cybersicherheitsreserve erfolgt nach besonderen Vereinbarungen zwischen dem vertrauenswürdigen Anbieter verwalteter Sicherheitsdienste und dem Nutzer, dem die Unterstützung aus der EU-Cybersicherheitsreserve gewährt wird. Die Bereitstellung dieser Dienste kann nach besonderen Vereinbarungen zwischen dem vertrauenswürdigen Anbieter verwalteter Sicherheitsdienste, dem Nutzer und der betroffenen Einrichtung erfolgen. Alle in dem vorliegenden Absatz genannten Vereinbarungen enthalten unter anderem Haftungsbedingungen.

(6) Die in Absatz 5 genannten Vereinbarungen beruhen auf Mustern, die von der ENISA nach Konsultation der Mitgliedstaaten und gegebenenfalls anderer Nutzer der EU-Cybersicherheitsreserve erstellt werden.

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

(8) Nutzer dürfen die auf Antrag gemäß Artikel 15 Absatz 1 bereitgestellten Dienste im Rahmen der EU-Cybersicherheitsreserve nur in Anspruch nehmen, um die Reaktion auf schwerwiegende Cybersicherheitsvorfälle, Cybersicherheitsvorfälle großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle zu unterstützen und die anschließende Wiederherstellung einzuleiten. Sie dürfen diese Dienste nur für in Bezug auf folgende Akteure in Anspruch nehmen:

a) in Sektoren mit hoher Kritikalität tätige Einrichtungen oder in sonstigen kritischen Sektoren tätige Einrichtungen im Falle von in Artikel 14 Absatz 3 Buchstabe a der vorliegenden Verordnung genannten Nutzern und gleichwertige Einrichtungen im Falle von in Artikel 14 Absatz 3 Buchstabe c der vorliegenden Verordnung genannten Nutzern und

b) Organe, Einrichtungen und sonstige Stellen der Union im Falle des in Artikel 14 Absatz 3 Buchstabe b genannten Nutzers.

(9) Binnen zwei Monaten nach Abschluss einer Unterstützung müssen die Nutzer, denen Unterstützung bereitgestellt wurde, einen zusammenfassenden Bericht über den erbrachten Dienst, die erzielten Ergebnisse und gewonnene Erkenntnisse vorlegen, und zwar:

a) der Kommission, der ENISA, dem CSIRTs-Netz und dem EU-CyCLONe im Falle der in Artikel 14 Absatz 3 Buchstabe a genannten Nutzern.

b) der Kommission, der ENISA und dem Interinstitutionellen Cybersicherheitsbeirat im Falle des in Artikel 14 Absatz 3 Buchstabe b genannten Nutzers.

c) der Kommission im Falle der in Artikel 14 Absatz 3 Buchstabe c genannten Nutzer.

Die Kommission leitet alle zusammenfassenden Berichte, die sie gemäß Unterabsatz 1 Buchstabe c des vorliegenden Absatzes von den in Artikel 14 Absatz 3 Buchstabe c genannten Nutzern erhält, an den Rat und den Hohen Vertreter weiter.

(10) Wurde gemäß Artikel 14 Absatz 5 der vorliegenden Verordnung die ENISA ganz oder teilweise mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve betraut, erstattet die ENISA der Kommission diesbezüglich regelmäßig Bericht und konsultiert sie. In diesem Zusammenhang leitet die ENISA der Kommission unverzüglich sämtliche Anträge, die sie von in Artikel 14 Absatz 3 Buchstabe c der vorliegenden Verordnung genannten Nutzern erhält, sowie, sofern dies für die Zwecke der Priorisierung gemäß dem vorliegenden Artikel erforderlich ist, sämtliche Anträge, die sie von in Artikel 14 Absatz 3 Buchstabe a oder b der vorliegenden Verordnung genannten Nutzern erhält, weiter. Die Verpflichtungen nach dem vorliegenden Absatz lassen Artikel 14 der Verordnung (EU) 2019/881 unbeschadet.

(11) Im Falle von in Artikel 14 Absatz 3 Buchstabe a oder b genannten Nutzern erstattet der öffentliche Auftraggeber der NIS-Kooperationsgruppe regelmäßig, mindestens jedoch zweimal jährlich, Bericht über die Inanspruchnahme und die Ergebnisse der Unterstützung.

(12) Im Falle des in Artikel 14 Absatz 3 Buchstabe c genannten Nutzers erstattet die Kommission dem Rat Bericht über die Inanspruchnahme und die Ergebnisse der Unterstützung und setzt den Hohen Vertreter darüber in Kenntnis; diese Berichterstattung und Inkenntnissetzung erfolgt regelmäßig, mindestens jedoch zweimal jährlich.

Artikel 17

Vertrauenswürdige Anbieter verwalteter Sicherheitsdienste

(1) In Beschaffungsverfahren zur Einrichtung der EU-Cybersicherheitsreserve handelt der öffentliche Auftraggeber gemäß den in der Verordnung (EU, Euratom) 2024/2509 festgelegten Grundsätzen und gemäß den folgenden Grundsätzen:

a) Sicherstellung, dass die von der EU-Cybersicherheitsreserve umfassten Dienste insgesamt betrachtet dazu führen, dass die EU-Cybersicherheitsreserve auch Dienste umfasst, die in allen Mitgliedstaaten durchgeführt werden können, wobei insbesondere nationale Anforderungen an die Erbringung solcher Dienste, auch in Bezug auf Sprache, Zertifizierung oder Akkreditierung, zu berücksichtigen sind;

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

c) Sicherstellung, dass die EU-Cybersicherheitsreserve einen Mehrwert für die Union 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 Union.

(2) Bei der Beschaffung von Diensten für die EU-Cybersicherheitsreserve nimmt der öffentliche Auftraggeber die folgenden Kriterien und Anforderungen in die Beschaffungsunterlagen auf:

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

b) der Anbieter sowie alle einschlägigen Tochterunternehmen und Unterauftragnehmer befolgen die geltenden Vorschriften zum Schutz von Verschlusssachen und verfügen über geeignete Vorkehrungen, darunter gegebenenfalls Vereinbarungen untereinander, um vertrauliche Informationen in Bezug auf den Dienst, insbesondere Beweismittel, Erkenntnisse und Berichte, zu schützen;

c) der Anbieter legt ausreichende Nachweise dafür vor, dass seine Leitungsstruktur transparent ist und dass es nicht wahrscheinlich ist, dass sie seine Unparteilichkeit und die Qualität seiner Dienstleistungen beeinträchtigt oder Interessenkonflikte verursacht;

d) der Anbieter verfügt über eine angemessene Sicherheitsüberprüfung, zumindest für das Personal, das für den Einsatz des Dienstes bestimmt ist, sofern ein Mitgliedstaat dies erfordert;

e) der Anbieter stellt das entsprechende Sicherheitsniveau für seine IT-Systeme sicher;

f) der Anbieter verfügt über die für die Unterstützung des beantragten Dienstes erforderliche Hardware und Software, welche keine bekannten ausnutzbaren Schwachstellen enthalten darf, im Hinblick auf sicherheitsbezogene Aspekte auf dem neuesten Stand ist und in jedem Fall allen geltenden Bestimmungen der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates ([23]) entspricht;

g) der Anbieter kann seine Erfahrung mit der Erbringung ähnlicher Dienste für einschlägige nationale Behörden, in Sektoren mit hoher Kritikalität tätige Einrichtungen oder in sonstigen kritischen Sektoren tätige Einrichtungen nachweisen;

h) der Anbieter kann den Dienst kurzfristig in den Mitgliedstaaten erbringen, in denen er ihn anbietet;

i) der Anbieter kann den Dienst in einer oder mehreren Amtssprachen der Organe der Union oder eines Mitgliedstaats erbringen, die gegebenenfalls von Mitgliedstaaten oder von in Artikel 14 Absatz 3 Buchstaben b und c genannten Nutzern verlangt werden, in denen bzw. für die der Anbieter den Dienst anbietet;

j) sobald ein europäisches System für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste gemäß der Verordnung (EU) 2019/881 besteht, wird der Anbieter innerhalb von zwei Jahren nach dem Tag der Anwendung des Systems nach diesem System zertifiziert;

([23]) Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

k) der Anbieter sieht in seinem Angebot die Bedingungen für die Umwandlung nicht in Anspruch genommener Sicherheitsvorfall-Notdienste vor, die in eng mit der Reaktion auf Sicherheitsvorfälle zusammenhängende Dienste in Bezug auf die Abwehrbereitschaft wie Übungen oder Schulungen umgewandelt können.

(3) Für die Zwecke der Beschaffung von Diensten für die EU-Cybersicherheitsreserve kann der öffentliche Auftraggeber in enger Zusammenarbeit mit den Mitgliedstaaten gegebenenfalls zusätzliche Kriterien und Anforderungen entwickeln, die über die in Absatz 2 genannten hinausgehen.

Artikel 18

Maßnahmen zur Unterstützung der Amtshilfe

(1) Im Rahmen des Cybernotfallmechanismus wird Hilfe für die Erbringung technischer Unterstützung durch einen Mitgliedstaat für einen anderen, von einem schwerwiegenden Cybersicherheitsvorfall oder einem Cybersicherheitsvorfall großen Ausmaßes betroffenen Mitgliedstaat geleistet, auch in Fällen gemäß Artikel 11 Absatz 3 Buchstabe f der Richtlinie (EU) 2022/2555.

(2) Die Unterstützung für technische Amtshilfe gemäß Absatz 1 des vorliegenden Artikels wird in Form von Finanzhilfen gewährt, wobei die in den einschlägigen Arbeitsprogrammen gemäß Artikel 24 der Verordnung (EU) 2021/694 genannten Bedingungen gelten.

Artikel 19

Unterstützung für mit dem Programm „Digitales Europa“ assoziierte Drittländer

(1) Ein mit dem Programm „Digitales Europa“ assoziiertes Drittland kann Unterstützung aus der EU-Cybersicherheitsreserve beantragen, sofern seine Teilnahme an der EU-Cybersicherheitsreserve in dem Abkommen über seine Assoziierung mit dem Programm „Digitales Europa“ vorgesehen ist. Dieses Abkommen enthält Bestimmungen, wonach das betreffende mit dem Programm „Digitales Europa“ assoziierte Drittland die in den Absätzen 2 und 9 des vorliegenden Artikels genannten Verpflichtungen erfüllen muss. Für die Zwecke der Teilnahme eines Drittlands an der EU-Cybersicherheitsreserve kann die teilweise Assoziierung eines Drittlands mit dem Programm „Digitales Europa“ eine auf das in Artikel 6 Absatz 1 Buchstabe g der Verordnung (EU) 2021/694 genannte operative Ziel beschränkte Assoziierung umfassen.

(2) Binnen drei Monaten nach Abschluss des in Absatz 1 genannten Abkommens und in jedem Fall vor dem Erhalt von Unterstützung aus der EU-Cybersicherheitsreserve, übermittelt ein mit dem Programm „Digitales Europa“ assoziiertes Drittland der Kommission Informationen über seine Cyberresilienz- und Risikomanagementfähigkeiten, darunter zumindest Informationen über nationale Maßnahmen, die zur Vorbereitung auf schwerwiegende Cybersicherheitsvorfälle oder einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle getroffen wurden, sowie Informationen über ihre zuständigen nationalen Stellen, einschließlich Computer-Notfallteams oder gleichwertige Einrichtungen, deren Fähigkeiten und die ihnen zugewiesenen Ressourcen. Die genannten Informationen werden von dem mit dem Programm „Digitales Europa“ assoziierten Drittland regelmäßig, mindestens jedoch einmal jährlich aktualisiert. Die Kommission leitet diese Informationen an den Hohen Vertreter und die ENISA weiter, um die Anwendung von Absatz 11 zu erleichtern.

(3) Die Kommission überprüft für jedes mit dem Programm „Digitales Europa“ assoziierte Drittland gemäß Absatz 1 regelmäßig, mindestens jedoch einmal jährlich die folgenden Kriterien:

a) ob das Land die Bedingungen des in Absatz 1 genannten Abkommens einhält, soweit sich diese Bedingungen auf die Teilnahme an der EU-Cybersicherheitsreserve beziehen;

b) ob das Land angemessene Schritte zur Vorbereitung auf schwerwiegende Cybersicherheitsvorfälle oder einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Sicherheitsvorfälle unternommen hat, wobei die in Absatz 2 genannten Informationen als Grundlage für die Prüfung dienen;

c) ob die Bereitstellung von Unterstützung gemäß der Politik der Union gegenüber dem Land und ihren allgemeinen Beziehungen zu diesem erfolgt und ob sie mit ihren anderweitigen Sicherheitsstrategien vereinbar ist.

Im Rahmen der Überprüfung gemäß Unterabsatz 1 konsultiert die Kommission in Bezug auf das unter Buchstabe c des genannten Unterabsatzes genannte Kriterium den Hohen Vertreter.

Gelangt die Kommission zu dem Schluss, dass ein mit dem Programm „Digitales Europa“ assoziiertes Drittland alle in Unterabsatz 4 genannten Bedingungen erfüllt, legt sie dem Rat einen Vorschlag für den Erlass eines Durchführungsrechtsakts gemäß Absatz 4 vor, mit dem die Bereitstellung von Unterstützung aus der EU-Cybersicherheitsreserve für dieses Land genehmigt wird.

(4) Der Rat kann die in Absatz 3 genannten Durchführungsrechtsakte erlassen. Diese Durchführungsrechtsakte gelten für höchstens ein Jahr. Ihre Geltungsdauer kann verlängert werden. Sie können eine mindestens 75 Tagen betragende Höchstdauer der Unterstützung vorsehen, die auf einen einzigen Antrag hin bereitgestellt werden kann.

Für die Zwecke des vorliegenden Artikels handelt der Rat zügig und erlässt in der Regel die im vorliegenden Absatz genannten Durchführungsrechtsakte binnen acht Wochen nach der Annahme des jeweiligen Vorschlags der Kommission gemäß Absatz 3 Unterabsatz 3.

(5) Der Rat kann einen gemäß Absatz 4 erlassenen Durchführungsrechtsakt jederzeit auf Vorschlag der Kommission ändern oder aufheben.

Ist der Rat der Auffassung, dass sich in Bezug auf das in Absatz 3 Unterabsatz 1 Buchstabe c genannte Kriterium wesentliche Änderungen ergeben haben, so kann er einen gemäß Absatz 4 erlassenen Durchführungsrechtsakt auf ordnungsgemäß begründete Initiative eines oder mehrerer Mitgliedstaaten ändern oder aufheben.

(6) Bei der Ausübung seiner Durchführungsbefugnisse nach dem vorliegenden Artikel wendet der Rat die in Absatz 3 Unterabsatz 1 genannten Kriterien an und legt erläutert seine Überprüfung dieser Kriterien. Insbesondere legt der Rat, wenn er gemäß Absatz 5 Unterabsatz 2 auf eigene Initiative handelt, Erläuterungen zu den in jenem Unterabsatz genannten wesentlichen Änderungen vor.

(7) Die Unterstützung eines mit dem Programm „Digitales Europa“ assoziierten Drittlands aus der EU-Cybersicherheitsreserve unterliegt allen besonderen Bedingungen, die in dem in Absatz 1 genannten Abkommen festgelegt sind.

(8) Zu den Nutzern aus mit dem Programm „Digitales Europa“ assoziierten Drittländern, die Dienste aus der EU-Cybersicherheitsreserve in Anspruch nehmen können, gehören zuständige Behörden wie Computer-Notfallteams oder gleichwertige Einrichtungen und Behörden für das Cyberkrisenmanagement.

(9) Jedes mit dem Programm „Digitales Europa“ assoziierte Drittland, das Unterstützung aus der EU-Cybersicherheitsreserve in Anspruch nehmen kann, benennt eine Behörde als zentrale Anlaufstelle für die Zwecke der vorliegenden Verordnung.

(10) Anträge auf Unterstützung aus der EU-Cybersicherheitsreserve nach dem vorliegenden Artikel werden von der Kommission geprüft. Der öffentliche Auftraggeber darf einem Drittland nur dann Unterstützung gewähren, wenn und solange ein gemäß Absatz 4 des vorliegenden Artikels erlassener Durchführungsrechtsakt des Rates in Kraft ist, der eine solche Unterstützung dieses Landes genehmigt. Eine Antwort wird den in Artikel 14 Absatz 3 Buchstabe c genannten Nutzern unverzüglich übermittelt.

(11) Nach Eingang eines Antrags auf Unterstützung nach dem vorliegenden Artikel unterrichtet die Kommission unverzüglich den Rat. Die Kommission übermittelt dem Rat aktuelle Informationen über die Prüfung des Antrags. Die Kommission arbeitet in Bezug auf die eingegangenen Anträge und die Umsetzung der mit dem Programm „Digitales Europa“ assoziierten Drittländern aus der EU-Cybersicherheitsreserve gewährten Unterstützung ferner mit dem Hohen Vertreter zusammen. Die Kommission berücksichtigt zudem etwaige Stellungnahmen der ENISA in Bezug auf solche Anträge.

Artikel 20

Koordinierung mit Krisenmanagementmechanismen der Union

(1) Wenn ein schwerwiegender Cybersicherheitsvorfall, ein Cybersicherheitsvorfall großen Ausmaßes oder ein einem Cybersicherheitsvorfall großen Ausmaßes gleichwertiger Sicherheitsvorfall von einer Katastrophe im Sinne des Artikels 4 Nummer 1 des Beschlusses Nr. 1313/2013/EU verursacht wird oder zu einer solche Katastrophe führt, ergänzt die im Rahmen der vorliegenden Verordnung geleistete Unterstützung der Reaktion auf solche Sicherheitsvorfälle die Maßnahmen im Rahmen des genannten Beschlusses, der davon unberührt bleibt.

(2) Im Falle eines Cybersicherheitsvorfalls großen Ausmaßes oder eines einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfalls, bei dem die Integrierte EU-Regelung für die politische Reaktion auf Krisen gemäß dem Durchführungsbeschluss (EU) 2018/1993 (IPCR-Regelung) aktiviert wird, erfolgt die im Rahmen der vorliegenden Verordnung geleistete Unterstützung der Reaktion auf einen solchen Sicherheitsvorfall gemäß den einschlägigen Verfahren der IPCR-Regelung.

KAPITEL IV

EUROPÄISCHER ÜBERPRÜFUNGSMECHANISMUS FÜR CYBERSICHERHEITSVORFÄLLE

Artikel 21

Europäischer Überprüfungsmechanismus für Cybersicherheitsvorfälle

(1) Auf Ersuchen der Kommission oder des EU-CyCLONe nimmt die ENISA mit Unterstützung des CSIRTs-Netzes und mit Zustimmung der betroffenen Mitgliedstaaten eine Überprüfung und Bewertung von Cyberbedrohungen, bekannten ausnutzbaren 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 EU-CyCLONe, dem CSIRTs-Netz, den betroffenen Mitgliedstaaten und der Kommission einen Bericht über die Überprüfung des Sicherheitsvorfalls vor, der darauf abzielt, zwecks Vermeidung oder Eindämmung künftiger Sicherheitsvorfälle gewonnene Erkenntnisse festzuhalten, um die genannten Adressaten des Berichts bei der Wahrnehmung ihrer Aufgaben — insbesondere der in den Artikeln 15 und 16 der Richtlinie (EU) 2022/2555 festgelegten Aufgaben — zu unterstützen. Hat ein Sicherheitsvorfall Auswirkungen auf ein mit dem Programm „Digitales Europa“ assoziiertes Drittland, leitet die ENISA den Bericht auch dem Rat weiter. In solchen Fällen leitet die Kommission den Bericht an den Hohen Vertreter weiter.

(2) Bei der Erstellung des in Absatz 1 des vorliegenden Artikels genannten Berichts über die Überprüfung des Sicherheitsvorfalls arbeitet die ENISA mit allen einschlägigen Interessenträgern zusammen und holt Rückmeldungen von diesen ein, darunter Vertreter der Mitgliedstaaten, die Kommission, andere einschlägige Organe, Einrichtungen und sonstige Stellen der Union sowie die Branche, einschließlich Anbieter verwalteter Sicherheitsdienste, und Nutzer von Cybersicherheitsdiensten. Soweit dies angemessen ist, arbeitet die ENISA in Kooperation mit CSIRTs sowie gegebenenfalls mit gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden auch mit Einrichtungen zusammen, die von schwerwiegenden Cybersicherheitsvorfällen oder Cybersicherheitsvorfällen großen Ausmaßes betroffen sind. Befragte Vertreter müssen etwaige Interessenkonflikte offenlegen.

(3) Der in Absatz 1 des vorliegenden Artikels genannte Bericht über die Überprüfung des Sicherheitsvorfalls enthält eine Überprüfung und Analyse des konkreten schwerwiegenden Cybersicherheitsvorfalls oder Cybersicherheitsvorfalls großen Ausmaßes, einschließlich der Hauptursachen, der bekannten ausnutzbaren Schwachstellen und der gewonnenen Erkenntnisse. Die ENISA stellt sicher, dass der Bericht den Rechtsvorschriften der Union oder den nationalen Rechtsvorschriften über den Schutz vertraulicher oder als Verschlusssache eingestufter Informationen entspricht. Wenn die betreffenden Mitgliedstaaten oder andere in Artikel 14 Absatz 3 genannte Nutzer, die von dem Sicherheitsvorfall betroffen sind, dies verlangen, werden die in dem Bericht enthaltenen Daten und Informationenanonymisiert. Der Bericht darf keine Angaben über aktiv ausgenutzte Schwachstellen enthalten, die noch nicht behoben wurden.

(4) Gegebenenfalls enthält der Bericht über die Überprüfung des Sicherheitsvorfalls Empfehlungen zur Verbesserung der Cyberabwehr der Union und kann bewährte Verfahren und gewonnene Erkenntnisse einschlägiger Interessenträger umfassen.

(5) Die ENISA kann eine öffentlich zugängliche Fassung des Berichts über die Überprüfung des Sicherheitsvorfalls herausgeben. Diese Fassung des Berichts darf nur zuverlässige öffentliche Informationen oder andere zuverlässige Informationen nur mit Zustimmung der betreffenden Mitgliedstaaten bzw. — bei Informationen über einen in Artikel 14 Absatz 3 Buchstabe b oder c genannten Nutzer — nur mit Zustimmung dieses Nutzers enthalten.

KAPITEL V

SCHLUSSBESTIMMUNGEN

Artikel 22

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:

      i) Folgender Buchstabe wird eingefügt:

„aa) Unterstützung des Aufbaus des mit Artikel 3 der Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates (*) eingerichteten europäischen Warnsystems für Cybersicherheit (im Folgenden ‚europäisches Warnsystem für Cybersicherheit'), einschließlich der Entwicklung, der Einführung und des Betriebs nationaler und grenzübergreifender Cyber-Hubs, die zur Lageerfassung in der Union und zur Erweiterung der Kapazitäten der Union zur Gewinnung von Erkenntnissen über Cyberbedrohungen beitragen;

(*) Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität für und der Kapazitäten in der Union für die Erkennung von, Vorsorge und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (Cybersolidaritätsverordnung) (ABl. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).“

ii) Folgender Buchstabe wird angefügt:

„g) Einrichtung und Betrieb des mit Artikel 10 der Verordnung (EU) 2025/38 eingerichteten Cybernotfallmechanismus, einschließlich der mit Artikel 14 der genannten Verordnung eingerichteten EU-Cybersicherheitsreserve (im Folgenden ‚EU-Cybersicherheitsreserve'), zur Unterstützung der Mitgliedstaaten bei der Vorbereitung und Reaktion auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes, ergänzend zu nationalen Ressourcen und Fähigkeiten und anderen auf Unionsebene verfügbaren Formen der Unterstützung, und zur Unterstützung anderer Nutzer bei der Reaktion auf erhebliche Cybersicherheitsvorfälle und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertige Vorfälle.“

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 (*) durchgeführt. Die EU-Cybersicherheitsreserve wird jedoch von der Kommission und, gemäß Artikel 14 Absatz 6 der Verordnung (EU) 2025/38, von der ENISA durchgeführt.

(*) 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).“

2. Artikel 9 wird wie folgt geändert:

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

„b) 1 760 806 000 EUR für das spezifische Ziel 2 — Künstliche Intelligenz;

c) 1 372 020 000 EUR für das spezifische Ziel 3 — Cybersicherheit und Vertrauen;

d) 482 640 000 EUR für das spezifische Ziel 4 — Fortgeschrittene digitale Kompetenzen;“

b) Folgender Absatz wird angefügt:

„(8) Abweichend von Artikel 12 Absatz 1 der Haushaltsordnung werden nicht verwendete Mittel für Verpflichtungen und Zahlungen, die für im Zusammenhang mit der Umsetzung der EU-Cybersicherheitsreserve und der Maßnahmen zur Unterstützung der Amtshilfe gemäß der Verordnung (EU) 2025/38 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. Das Europäische Parlament und der Rat werden gemäß Artikel 12 Absatz 6 Haushaltsordnung über die übertragenen Mittel informiert.“

3. Artikel 12 wird wie folgt geändert:

a) Folgende Absätze werden eingefügt:

„(5a) Im Falle von Rechtsträgern mit Sitz in der Union, die aber aus Drittländern kontrolliert werden, findet Absatz 5 auf Maßnahmen zur Umsetzung des europäischen Warnsystems für Cybersicherheit keine Anwendung, wenn in Bezug auf die betreffende Maßnahme die beiden folgenden Bedingungen erfüllt sind:

a) unter Berücksichtigung der Ergebnisse der gemäß Artikel 9 Absatz 4 der Verordnung (EU) 2025/38 erstellten Aufstellung besteht ein reales Risiko, dass die Instrumente, Infrastruktur oder Dienste, die erforderlich und ausreichend dafür sind, dass die betreffende Maßnahme angemessen zu den Zielen des europäischen Warnsystems für Cybersicherheit beitragen kann, von Rechtsträgern, die in einem Mitgliedstaat niedergelassen sind oder als dort niedergelassen gelten und die von einem Mitgliedstaat oder von einem Staatsangehörigen eines Mitgliedstaats kontrolliert werden, nicht zur Verfügung gestellt werden können;

b) das mit einer Beschaffung über solche Rechtsträger im Rahmen des europäischen Warnsystems für Cybersicherheit einhergehende Sicherheitsrisiko steht in einem angemessenen Verhältnis zu den damit verbundenen Vorteilen und steht den grundlegenden Sicherheitsinteressen der Union und ihrer Mitgliedstaaten nicht entgegen.

(5b) Im Falle von Rechtsträgern mit Sitz in der Union, die aber aus Drittländern kontrolliert werden, findet Absatz 5 auf Maßnahmen zur Umsetzung der EU-Cybersicherheitsreserve keine Anwendung, wenn in Bezug auf die betreffende Maßnahme die beiden folgenden Bedingungen erfüllt sind:

a) unter Berücksichtigung der Ergebnisse der gemäß Artikel 14 Absatz 6 der Verordnung (EU) 2025/38 erstellten Aufstellung besteht ein reales Risiko, dass die Technologien, Fachkenntnisse oder Kapazitäten, die erforderlich und ausreichend dafür sind, dass die EU-Cybersicherheitsreserve ihre Funktionen angemessen ausüben kann, von Rechtsträgern, die in einem Mitgliedstaat niedergelassen sind oder als dort niedergelassen gelten und die von einem Mitgliedstaat oder von einem Staatsangehörigen eines Mitgliedstaats kontrolliert werden, nicht zur Verfügung gestellt werden können;

b) das mit einer Aufnahme solcher Rechtsträger in die EU-Cybersicherheitsreserve einhergehende Sicherheitsrisiko steht in einem angemessenen Verhältnis zu den damit verbundenen Vorteilen und steht den grundlegenden Sicherheitsinteressen der Union und ihrer Mitgliedstaaten nicht entgegen.“

b) Absatz 6 erhält folgende Fassung:

„6. Wenn dies aus Sicherheitsgründen hinreichend gerechtfertigt ist, kann im Arbeitsprogramm auch vorgesehen werden, dass sich Rechtsträger mit Sitz in assoziierten Ländern und Rechtsträger mit Sitz in der Union, die aber aus Drittländern kontrolliert werden, an einigen oder allen Maßnahmen im Rahmen der spezifischen Ziele 1 und 2 nur dann beteiligen dürfen, wenn sie den von diesen Rechtsträgern zu erfüllenden Anforderungen genügen, damit der Schutz der grundlegenden Sicherheitsinteressen der Union und der Mitgliedstaaten gewährleistet und für den Schutz von Informationen in Verschlusssachen gesorgt ist. Die entsprechenden Anforderungen sind im Arbeitsprogramm enthalten.

Im Falle von Rechtsträgern mit Sitz in der Union, die aber aus Drittländern kontrolliert werden, findet Unterabsatz 1 auch Anwendung in Bezug auf Maßnahmen im Rahmen des spezifischen Ziels 3

a) zur Umsetzung des europäischen Warnsystems für Cybersicherheit in Fällen, in denen Absatz 5a Anwendung findet und

b) zur Umsetzung der EU-Cybersicherheitsreserve in Fällen, in denen Absatz 5b Anwendung findet.“

4. 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 (*) und 2014/25/EU (**) 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 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 der vorliegenden Verordnung zu vergeben. Die Kommission und die ENISA können auch als Großhändler auftreten, und zwar durch den Ankauf, die Lagerung und den Weiterverkauf oder die Spende von

Lieferungen und Dienstleistungen, einschließlich Mieten, zugunsten dieser Drittländer. Abweichend von Artikel 168 Absatz 3 der Verordnung (EU, Euratom) 2024/2509 des Europäischen Parlaments und des Rates (***) reicht hierzu der Antrag eines einzigen Drittlands als Handlungsauftrag für die Kommission oder die ENISA aus.

Bei der Durchführung von Vergabeverfahren für die 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 ein Großhändler auftreten, und zwar durch den Ankauf, die Lagerung und den Weiterverkauf oder die Spende von Lieferungen und Dienstleistungen, einschließlich Mieten, zugunsten der Organe, Einrichtungen und oder sonstigen Stellen der Union. Abweichend von Artikel 168 Absatz 3 der Verordnung (EU, Euratom) 2024/2509 reicht hierzu der Antrag eines einzigen Organs, einer einzigen Einrichtung oder einer einzigen 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.

(*) 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).

(**) Richtlinie 2014/25/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die Vergabe von Aufträgen durch Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste und zur Aufhebung der Richtlinie 2004/17/EG (ABl. L 94 vom 28.3.2014, S. 243).

(***) Verordnung (EU, Euratom) 2024/2509 des Europäischen Parlaments und des Rates vom 23. September 2024 über die Haushaltsordnung für den Gesamthaushaltsplan der Union (ABl. L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).“

5. Folgender Artikel wird eingefügt:

„*Artikel 16a*

Normenkonflikte

Für Maßnahmen zur Umsetzung des europäischen Warnsystems für Cybersicherheit gelten die Regeln in den Artikeln 4, 5 und 9 der Verordnung (EU) 2025/38. Im Falle eines Konflikts zwischen den Bestimmungen der vorliegenden Verordnung und den Artikeln 4, 5 und 9 der Verordnung (EU) 2025/38 gehen Letztere vor und finden auf diese spezifischen Maßnahmen Anwendung.

In Bezug auf die EU-Cybersicherheitsreserve sind in Artikel 19 der Verordnung (EU) 2025/38 spezifische Regeln für die Teilnahme von mit dem Programm assoziierten Drittländern festgelegt. Im Falle eines Konflikts zwischen den Bestimmungen der vorliegenden Verordnung und Artikel 19 der Verordnung (EU) 2025/38 geht Letzterer vor und findet auf diese spezifischen Maßnahmen Anwendung.“

6. Artikel 19 erhält folgende Fassung:

„*Artikel 19*

Finanzhilfen

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 gemäß Artikel 9 der Verordnung (EU) 2025/38 ausgewählten Mitgliedstaaten und dem in Artikel 5 der Verordnung (EU) 2025/38 genannten Aufnahmekonsortium nach 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 Cybernotfallmechanismus kann den Mitgliedstaaten nach Artikel 195 Absatz 1 Buchstabe d der Haushaltsordnung ohne Aufforderung zur Einreichung von Vorschlägen vom ECCC direkt gewährt werden.

In Bezug auf Maßnahmen zur Unterstützung der Amtshilfe gemäß Artikel 18 der Verordnung (EU) 2025/38 unterrichtet das ECCC die Kommission und die ENISA über Anträge der Mitgliedstaaten auf Gewährung direkter Finanzhilfen ohne Aufforderung zur Einreichung von Vorschlägen.

In Bezug auf Maßnahmen zur Unterstützung der Amtshilfe gemäß Artikel 18 der Verordnung (EU) 2025/38 können die Kosten gemäß 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."

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

Artikel 23

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 14 Absatz 7 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 5. Februar 2025 übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(3) Die Befugnisübertragung gemäß Artikel 14 Absatz 7 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 14 Absatz 7 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 24

Ausschussverfahren

(1) Die Kommission wird von dem in Artikel 31 Absatz 1 der Verordnung (EU) 2021/694 genannten 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 25

Bewertung und Überarbeitung

(1) Bis zum 5. Februar 2027 und danach mindestens alle vier Jahre bewertet die Kommission die Funktionsweise der in dieser Verordnung festgelegten Maßnahmen und übermittelt dem Europäischen Parlament und dem Rat einen Bericht.

(2) Im Rahmen der in Absatz 1 genannten Bewertung wird insbesondere Folgendes geprüft:

a) die Anzahl der eingerichteten nationalen Cyber-Hubs und grenzübergreifenden Cyber-Hubs, der Umfang der weitergegebenen Informationen, soweit möglich einschließlich der Auswirkungen auf die Arbeit des CSIRTs-Netzes und das Ausmaß, in dem diese Maßnahmen zur Stärkung der gemeinsamen Erkennung und Lageerfassung der Union in Bezug auf Cyberbedrohungen und Sicherheitsvorfälle und zur Entwicklung von Spitzentechnologien beigetragen haben; die Verwendung von Mitteln aus dem Programm „Digitales Europa" für gemeinsam beschaffte Instrumente, Infrastruktur

oder, Dienste im Bereich der Cybersicherheit; sowie — sofern diese Informationen verfügbar sind — das Ausmaß der Zusammenarbeit zwischen nationalen Cyber-Hubs und sektoralen und sektorübergreifenden Gemeinschaften wesentlicher und wichtiger Einrichtungen, wie in Artikel 3 der Richtlinie (EU) 2022/2555 genannt;

b) die Nutzung und Wirksamkeit von Maßnahmen im Rahmen des Cybernotfallmechanismus zur Unterstützung der Abwehrbereitschaft, einschließlich Schulungen, zur Unterstützung der Reaktion auf und anfänglichen Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen, Cybersicherheitsvorfällen großen Ausmaßes und einem Cybersicherheitsvorfall großen Ausmaßes gleichwertigen Sicherheitsvorfällen, einschließlich der Verwendung von Mitteln aus dem Programm „Digitales Europa“, sowie die bei der Umsetzung des Cybernotfallmechanismus gewonnenen Erkenntnisse und die sich daraus ergebenden Empfehlungen;

c) die Nutzung und Wirksamkeit der EU-Cybersicherheitsreserve in Bezug auf die Art der Nutzer, einschließlich der Verwendung von Mitteln aus dem Programm „Digitales Europa“, die Inanspruchnahme von Diensten, einschließlich der Art der Dienste, die durchschnittliche Zeit für die Beantwortung von Anträgen und für den Einsatz der EU-Cybersicherheitsreserve, den prozentualen Anteil der Dienste, die in Dienste in Bezug auf die Abwehrbereitschaft im Zusammenhang mit der Prävention von und der Reaktion auf Sicherheitsvorfälle umgewandelt wurden, sowie die bei der Umsetzung der EU-Cybersicherheitsreserve gewonnenen Erkenntnisse und die sich daraus ergebenden Empfehlungen;

d) der Beitrag der vorliegenden Verordnung zur Stärkung der Wettbewerbsposition von Industrie und Dienstleistungen der Digitalwirtschaft in der Union, einschließlich Kleinstunternehmen, kleiner und mittlerer Unternehmen sowie Start-up-Unternehmen, sowie der Beitrag zu dem übergeordneten Ziel der Stärkung der Kompetenzen und Kapazitäten von Fachkräften im Bereich der Cybersicherheit.

(3) Die Kommission legt dem Europäischen Parlament und dem Rat auf der Grundlage der in Absatz 1 genannten Berichte gegebenenfalls einen Legislativvorschlag zur Änderung dieser Verordnung vor.

Artikel 26

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 Brüssel am 19. Dezember 2024.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	BÓKA J.

ANHANG

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

1. In Anhang I erhält der Abschnitt „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 -infrastruktur 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 Cyber-Hubs und der grenzübergreifenden Cyber-Hubs, die das europäische Warnsystem für Cybersicherheit 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 unter Berücksichtigung eines ausgewogenen Geschlechterverhältnisses, beispielsweise 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 und Cybersicherheitsvorfällen großen Ausmaßes durch eine grenzüberschreitende Einführung von Cybersicherheitsdiensten, einschließlich der Unterstützung der Amtshilfe zwischen Behörden und der Einrichtung einer Reserve vertrauenswürdiger Anbieter verwalteter Sicherheitsdienste auf Unionsebene.“

2. In Anhang II erhält der Abschnitt „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, auch im Rahmen des europäischen Warnsystems für Cybersicherheit

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“.

Zu diesem Rechtsakt wurde eine Erklärung abgegeben, die in ABl. C, C/2025/308, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/308/oj, zu finden ist.