EUROPÄISCHE
KOMMISSION

Brüssel, den 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

(Text von Bedeutung für den EWR)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Dieser Vorschlag ist Teil eines Pakets von Maßnahmen, mit denen die Resilienz und die Kapazitäten zur Reaktion auf Sicherheitsvorfälle öffentlicher und privater Einrichtungen, zuständiger Behörden und der Union als Ganzer auf dem Gebiet der Cybersicherheit und des Schutzes kritischer Infrastrukturen weiter verbessert werden sollen. Er steht im Einklang mit den Prioritäten der Kommission, Europa für das digitale Zeitalter zu rüsten und eine zukunftsfähige Wirtschaft zu schaffen, die im Dienste des Menschen steht. Cybersicherheit ist eine Priorität in der Reaktion der Kommission auf die COVID-19-Krise. Das Paket umfasst eine neue Cybersicherheitsstrategie, die die strategische Autonomie der Union stärken soll, um ihre Resilienz und kollektive Reaktion zu verbessern und ein offenes und globales Internet zu errichten. Das Paket umfasst ferner einen Vorschlag für eine Richtlinie über die Resilienz von Betreibern wesentlicher Dienste, die physische Bedrohungen von diesen Betreibern abwenden soll.

Dieser Vorschlag baut auf der Richtlinie (EU) 2016/1148 über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) auf, die der erste EU-Rechtsakt über Cybersicherheit ist und Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vorsieht. Gleichzeitig wird die NIS-Richtlinie mit diesem Vorschlag aufgehoben. Die NIS-Richtlinie hat 1) zur Verbesserung der Cybersicherheitskapazitäten auf nationaler Ebene beigetragen, weil sie vorsieht, dass die Mitgliedstaaten nationale Cybersicherheitsstrategien aufstellen und Cybersicherheitsbehörden benennen; 2) für mehr Zusammenarbeit zwischen den Mitgliedstaaten auf Unionsebene gesorgt, weil verschiedene Foren errichtet wurden, die den Austausch von strategischen und operativen Informationen erleichtern; und 3) die Cyberresilienz öffentlicher und privater Einrichtungen in sieben Sektoren (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastrukturen) und in drei digitalen Dienstleistungsbereichen (Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste) verbessert, weil die Mitgliedstaaten gemäß der Richtlinie dafür sorgen müssen, dass Betreiber wesentlicher Dienste und Anbieter digitaler Dienste Cybersicherheitsanforderungen einführen und Sicherheitsvorfälle melden.

Mit dem Vorschlag wird der bestehende Rechtsrahmen modernisiert unter Berücksichtigung der zunehmenden Digitalisierung des Binnenmarkts in den letzten Jahren und der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit. Beide Entwicklungen haben seit Beginn der COVID-19-Krise noch an Intensität gewonnen. Der Vorschlag behebt auch verschiedene Schwächen der NIS-Richtlinie, die die Freisetzung ihres gesamten Potenzials verhindert haben.

Mit der NIS-Richtlinie wurden zwar beachtliche Ergebnisse erzielt, und sie hat in vielen Mitgliedstaaten ein erhebliches Umdenken in Bezug auf das institutionelle und regulatorische Cybersicherheitskonzept bewirkt, aber sie stößt auch an Grenzen. Mit dem zunehmenden digitalen Wandel der Gesellschaft, der durch die COVID-19-Krise noch an Tempo gewonnen hat, haben auch die Bedrohungen für die Cybersicherheit zugenommen. Dies bringt neue Herausforderungen mit sich, die entsprechende, innovative Antworten erfordern. Die Zahl der Cyberangriffe steigt weiter, und die Angriffe von verschiedensten Seiten innerhalb und außerhalb der EU werden immer komplexer.

Die Bewertung der Wirksamkeit der NIS-Richtlinie, die für die Zwecke der Folgenabschätzung vorgenommen wurde, ergab folgende Schwachstellen: 1) niedriges

Cyberresilienzniveau bei Unternehmen, die in der EU tätig sind; 2) unterschiedliche Resilienz von Mitgliedstaat zu Mitgliedstaat und von Sektor zu Sektor; 3) schwach ausgeprägte gemeinsame Lageerfassung und mangelnde gemeinsame Krisenreaktion. Wenn z. B. in einem Mitgliedstaat bestimmte große Krankenhäuser nicht unter die NIS-Richtlinie fallen, müssen sie die entsprechenden Sicherheitsmaßnahmen nicht ergreifen, während die NIS-Sicherheitsanforderungen in einem anderen Mitgliedstaat praktisch für alle Gesundheitsdienstleister gelten.

Da es sich um eine Initiative im Rahmen des Programms zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung (REFIT) handelt, sollen mit dem Vorschlag der Regelungsaufwand für die zuständigen Behörden verringert und die Befolgungskosten für öffentliche und private Einrichtungen gesenkt werden. Erreicht wird dies vor allem durch die Streichung der Verpflichtung der zuständigen Behörden, die Betreiber wesentlicher Dienste zu ermitteln, und durch eine stärkere Harmonisierung der Sicherheits- und Berichterstattungsanforderungen, um Einrichtungen, die grenzüberschreitende Dienste erbringen, die Einhaltung der Vorschriften zu erleichtern. Gleichzeitig wird den zuständigen Behörden eine Reihe neuer Aufgaben übertragen, darunter die Überwachung von Einrichtungen in Sektoren, die bisher nicht unter die NIS-Richtlinie fallen.

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

Dieser Vorschlag ist Teil eines umfassenderen Pakets bestehender Rechtsinstrumente und geplanter Initiativen auf Unionsebene, mit denen die Widerstandsfähigkeit öffentlicher und privater Einrichtungen gegenüber Bedrohungen erhöht werden soll.

Im Bereich Cybersicherheit sind dies hauptsächlich die Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation (deren cybersicherheitsbezogene Bestimmungen durch die Bestimmungen des vorliegenden Vorschlags ersetzt werden) und der Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (COM(2020) 595 final), die als *lex specialis* zum vorliegenden Vorschlag angesehen wird, sobald beide Rechtsakte in Kraft getreten sind.

Im Bereich physische Sicherheit ergänzt der vorliegende Vorschlag den Vorschlag für eine Richtlinie über die Resilienz kritischer Einrichtungen, mit der die Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (EKI-Richtlinie) überarbeitet wird und die ein Unionsverfahren zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und ein Konzept zur Verbesserung ihres Schutzes vorsieht. Im Juli 2020 verabschiedete die Kommission die EU-Strategie für die Sicherheitsunion[1], in der die zunehmenden Verflechtungen und gegenseitigen Abhängigkeiten zwischen physischen und digitalen Infrastrukturen anerkannt wurden. In der Strategie wurde hervorgehoben, dass ein kohärenterer Ansatz zwischen der EKI-Richtlinie und der Richtlinie (EU) 2016/1148 in Bezug auf Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union notwendig ist.

Der Vorschlag ist daher eng abgestimmt mit dem Vorschlag für eine Richtlinie über die Resilienz kritischer Einrichtungen, mit der die Resilienz kritischer Einrichtungen gegen physische Bedrohungen in einer Vielzahl von Sektoren verbessert werden soll. Der Vorschlag soll sicherstellen, dass die zuständigen Behörden auf der Grundlage beider Rechtsakte sich

[1] COM(2020)605 final.

ergänzende Maßnahmen treffen und Informationen austauschen zur cyberbezogenen gegebenenfalls und zur nicht cyberbezogenen Resilienz und dass für besonders kritische Betreiber in den Sektoren, die nach dem vorliegenden Vorschlag als „wesentlich“ eingestuft werden, auch allgemeinere resilienzfördernde Verpflichtungen mit einem Schwerpunkt auf nicht cyberbezogenen Risiken gelten.

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

Wie in der Mitteilung der Kommission zur Gestaltung der digitalen Zukunft Europas[2] dargelegt, ist es für Europa von entscheidender Bedeutung, dass das Potenzial des digitalen Zeitalters vollständig ausgeschöpft und die europäische Industrie und Innovationskapazität gestärkt werden, ohne bei Sicherheit und Ethik Abstriche zu machen. Die europäische Datenstrategie setzt auf vier Säulen – Datenschutz, Grundrechte, Sicherheit und Cybersicherheit – als wesentliche Voraussetzungen dafür, dass die Gesellschaft Vorteile aus der Nutzung von Daten ziehen kann.

In einer Entschließung vom 12. März 2019 forderte das Europäische Parlament *„[…] die Kommission auf zu prüfen, ob der Anwendungsbereich der Richtlinie über Netz- und Informationssysteme auf andere kritische Bereiche und Dienstleistungen ausgeweitet werden muss, die nicht von branchenspezifischen Rechtsvorschriften erfasst sind“*.[3] Der Rat begrüßte in seinen Schlussfolgerungen vom 9. Juni 2020 *„[…] die Pläne der Kommission, für kohärente Vorschriften für die Marktteilnehmer zu sorgen und einen sicheren, soliden und angemessenen Informationsaustausch über Bedrohungen sowie Zwischenfälle zu erleichtern – auch durch eine Überprüfung der Richtlinie über die Sicherheit von Netz-und Informationssystemen (NIS-Richtlinie) –, um Optionen nachzugehen, mit denen unter Wahrung der Zuständigkeiten der Mitgliedstaaten, einschließlich der Verantwortung für ihre nationale Sicherheit, die Widerstandsfähigkeit gegen Cyberangriffe – insbesondere auf wesentliche wirtschaftliche und gesellschaftliche Tätigkeiten – verbessert wird und wirksamere Reaktionen auf sie ermöglicht werden.“*[4] Der vorgeschlagene Rechtsakt berührt nicht die Anwendung der im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) festgelegten Wettbewerbsregeln.

Da nicht wenige Cybersicherheitsbedrohungen ihren Ursprung außerhalb der EU haben, bedarf es eines kohärenten Konzepts für die internationale Zusammenarbeit. Diese Richtlinie wird als Referenzmodell dienen, für das im Rahmen der Zusammenarbeit der EU mit Drittländern und insbesondere bei der Bereitstellung externer technischer Hilfe geworben werden soll.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- **Rechtsgrundlage**

Die Rechtsgrundlage der NIS-Richtlinie ist Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der vorsieht, dass das Europäische Parlament und der Rat Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten erlassen, die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben.

[2] COM(2020)67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_DE.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/de/pdf

Der Gerichtshof der EU stellte in seinem Urteil in der Rechtssache C-58/08, Vodafone u. a., fest, dass die Wahl von Artikel 114 AEUV als Rechtsgrundlage gerechtfertigt ist, wenn Unterschiede zwischen den nationalen Vorschriften vorliegen, die sich unmittelbar auf das Funktionieren des Binnenmarkts auswirken. Ferner befand der Gerichtshof, dass, wenn ein auf Artikel 114 AEUV gestützter Rechtsakt bereits jedes Handelshemmnis auf dem von ihm harmonisierten Gebiet beseitigt hat, der Unionsgesetzgeber im Hinblick auf seine Aufgabe, über den Schutz der im Vertrag anerkannten allgemeinen Interessen zu wachen, nicht daran gehindert sein kann, diesen Rechtsakt den Umständen oder neuen Erkenntnissen anzupassen. Außerdem entschied der Gerichtshof, dass der Ausdruck „Maßnahmen zur Angleichung“ in Artikel 114 AEUV nach Maßgabe des allgemeinen Kontextes und der speziellen Umstände der zu harmonisierenden Materie einen Ermessensspielraum hinsichtlich der zur Erreichung eines angestrebten Ergebnisses am besten geeigneten Angleichungstechnik einräumen soll. Der vorgeschlagene Rechtsakt würde Hindernisse für den Binnenmarkt beseitigen und seine Errichtung und sein Funktionieren verbessern durch klare und allgemeingültige Bestimmungen über den Anwendungsbereich der NIS-Richtlinie, mit denen die geltenden Regeln im Bereich Cybersicherheitsrisikomanagement und Meldung von Sicherheitsvorfällen harmonisiert werden. Die derzeitigen Unterschiede in diesem Bereich auf legislativer und aufsichtsrechtlicher Ebene sowie auf nationaler und EU-Ebene sind Hindernisse für den Binnenmarkt, da für grenzüberschreitend tätige Einrichtungen unterschiedliche und sich möglicherweise überschneidende rechtliche Anforderungen gelten und/oder angewendet werden, was sie in ihrer Ausübung der Niederlassungs- und Dienstleistungsfreiheit behindern könnte. Unterschiedliche Regeln wirken sich auch negativ auf die Wettbewerbsbedingungen im Binnenmarkt aus, wenn sie Einrichtungen derselben Art in verschiedenen Mitgliedstaaten betreffen.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

Die unionsweite Cybersicherheitsresilienz kann nicht wirksam sein, wenn sie in nationalen oder regionalen Silos uneinheitlich angegangen wird. Die NIS-Richtlinie hat diesen Mangel durch die Errichtung eines Rahmens für die Sicherheit der Netz- und Informationssysteme auf der Ebene der Mitgliedstaaten und auf Unionsebene zum Teil behoben. Aber ihre Übernahme in die nationalen Rechtsordnungen und ihre Umsetzung haben inhärente Mängel und Grenzen einiger Bestimmungen und Ansätze ans Licht gebracht, wie z. B. die unklare Abgrenzung des Anwendungsbereichs der Richtlinie, die in der Praxis zu erheblichen Unterschieden in Umfang und Tiefe des Tätigwerdens der EU auf der Ebene der Mitgliedstaaten führt. Hinzu kommt, dass die europäische Wirtschaft seit Beginn der COVID-19-Krise noch stärker von Netz- und Informationssystemen abhängig ist als je zuvor und Sektoren und Dienste immer enger miteinander verflochten sind. Ein Tätigwerden der EU über die geltenden Maßnahmen der NIS-Richtlinie hinaus ist hauptsächlich aus folgenden Gründen gerechtfertigt: i) Die NIS-bezogenen Bedrohungen und Herausforderungen sind zunehmend grenzüberschreitender Art, ii) die Union kann dazu beitragen, die Wirksamkeit und Koordinierung nationaler Politiken zu verbessern und zu fördern, und iii) konzertierte und kooperative politische Maßnahmen können zu einem wirksamen Schutz von personenbezogenen Daten und Privatsphäre beitragen.

- **Verhältnismäßigkeit**

Die in dieser Richtlinie vorgeschlagenen Regeln gehen nicht über das für die zufriedenstellende Verwirklichung der spezifischen Ziele erforderliche Maß hinaus. Die vorgesehene Angleichung und Vereinheitlichung von Sicherheitsmaßnahmen und

Meldepflichten entsprechen den Forderungen von Mitgliedstaaten und Unternehmen nach einer Verbesserung des geltenden Rahmens.

In dem Vorschlag wird der bereits bestehenden Praxis in den Mitgliedstaaten Rechnung getragen. Ein höheres Schutzniveau, dass durch diese vereinheitlichten und abgestimmten Anforderungen erreicht wird, steht im Verhältnis zu den immer höheren Risiken, einschließlich jener mit einem grenzüberschreitenden Element; sie sind vertretbar und entsprechen allgemein den Interessen der betroffenen Einrichtungen, da sie die Kontinuität und die Qualität von deren Dienstleistungen gewährleisten. Die Kosten für die Gewährleistung einer systematischen Zusammenarbeit zwischen den Mitgliedstaaten sind gering im Vergleich zu den Verlusten und Schäden, die Wirtschaft und Gesellschaft durch Cybersicherheitsvorfälle entstehen, Außerdem haben die Konsultationen der Interessenträger, die im Zuge der Überprüfung der NIS-Richtlinie durchgeführt wurden, einschließlich der Konsultation der Öffentlichkeit und der gezielten Erhebungen, ergeben, dass eine Überarbeitung der NIS-Richtlinie in diesem Sinne befürwortet wird.

- **Wahl des Instruments**

Mit dem Vorschlag werden die Pflichten von Unternehmen weiter angepasst und stärker harmonisiert. Zugleich soll der Vorschlag den Mitgliedstaaten die erforderliche Flexibilität einräumen, besondere nationale Gegebenheiten zu berücksichtigen, indem er z. B. die Möglichkeit vorsieht, über den im Rechtsakt festgelegten Ausgangswert hinaus zusätzliche wesentliche oder wichtige Einrichtungen zu ermitteln. Bei dem geplanten Rechtsakt sollte es sich daher um eine Richtlinie handeln, weil dieses Rechtsinstrument sowohl eine gezielte Harmonisierung als auch ein bestimmtes Maß an Flexibilität für die zuständigen Behörden ermöglicht.

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

- **Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften**

Die Kommission hat eine Bewertung der Funktionsweise der Richtlinie vorgenommen.[5] Sie hat ihre Relevanz, ihren EU-Mehrwert sowie ihre Kohärenz und ihre Wirksamkeit analysiert. Diese Analyse hat im Wesentlichen Folgendes ergeben:

- Der Anwendungsbereich der NIS-Richtlinie ist zu begrenzt, was die Zahl der erfassten Sektoren angeht, vor allem wegen i) der zunehmenden Digitalisierung in den letzten Jahren und eines höheren Vernetzungsgrads sowie ii) der Tatsache, dass der Anwendungsbereich der NIS-Richtlinie nicht mehr alle digitalisierten Sektoren erfasst, die grundlegende Dienstleistungen für die Wirtschaft und Gesellschaft als Ganze anbieten.
- Die NIS-Richtlinie bietet keine hinreichende Klarheit, was den Anwendungsbereich für Betreiber wesentlicher Dienste angeht, und ihre Bestimmungen sind nicht klar genug hinsichtlich der nationalen Zuständigkeit für Anbieter digitaler Dienste. Infolgedessen wurden bestimmte Arten von Einrichtungen nicht in allen Mitgliedstaaten ermittelt und müssen daher weder Sicherheitsvorkehrungen treffen noch Sicherheitsvorfälle melden.

[5] [Anhang 5 der Folgenabschätzung]

- Die NIS-Richtlinie hat den Mitgliedstaaten großen Ermessensspielraum bei der Festlegung von Sicherheitsanforderungen und Meldepflichten für Betreiber wesentlicher Dienste eingeräumt. Die Bewertung hat ergeben, dass die Mitgliedstaaten diese Anforderungen in einigen Fällen auf sehr unterschiedliche Weise umgesetzt haben, was für Unternehmen, die in mehr als einem Mitgliedstaat tätig sind, mit zusätzlichem Aufwand verbunden ist.
- Die Aufsichts- und Durchsetzungsregeln der NIS-Richtlinie sind nicht wirksam. Die Mitgliedstaaten zögern beispielsweise sehr, Sanktionen gegen Einrichtungen zu verhängen, die keine Sicherheitsanforderungen festlegen oder Sicherheitsvorfälle nicht melden. Dies kann nachteilige Auswirkungen auf die Cyberresilienz einzelner Einrichtungen haben.
- Bei den finanziellen und personellen Ressourcen, die die Mitgliedstaaten für die Erfüllung ihrer Aufgaben (wie die Ermittlung von Betreibern wesentlicher Dienste oder auch die Aufsicht) vorsehen, gibt es große Unterschiede, und folglich variiert auch die Erfahrung im Umgang mit Cybersicherheitsrisiken stark. Dies vertieft die Unterschiede in der Cyberresilienz zwischen den Mitgliedstaaten weiter.
- Die Mitgliedstaaten tauschen nicht systematisch Informationen aus, was sich vor allem nachteilig auf die Wirksamkeit der Cybersicherheitsmaßnahmen und die gemeinsame Lageerfassung auf EU-Ebene auswirkt. Dies gilt auch für die Weitergabe von Informationen zwischen privaten Einrichtungen und für die Zusammenarbeit zwischen den Kooperationsstrukturen auf EU-Ebene und privaten Einrichtungen.

- **Konsultation der Interessenträger**

Die Kommission hat eine Vielzahl verschiedener Interessenträger konsultiert. Mitgliedstaaten und Interessenträger wurden aufgefordert an der Konsultation der Öffentlichkeit teilzunehmen sowie an den Erhebungen und Workshops, die von Wavestone, CEPS und ICF organisiert wurden, bei denen die Kommission eine Studie zur Unterstützung der Überprüfung der NIS-Richtlinie in Auftrag gegeben hat. Zu den konsultierten Interessenträgern zählten die zuständigen nationalen Behörden, die mit Cybersicherheit befassten Unionsgremien, Betreiber wesentlicher Dienste, Anbieter digitaler Dienste, Einrichtungen, die nicht unter die jetzige NIS-Richtlinie fallende Dienste anbieten, Handelsverbände und Verbraucherorganisationen sowie die Bürgerinnen und Bürger.

Außerdem steht die Kommission fortwährend in Kontakt mit den Behörden, die für die Umsetzung der NIS-Richtlinie zuständig sind. Die Kooperationsgruppe hat sich ausführlich mit verschiedenen Aspekten der Umsetzung auf sektorübergreifender und sektoraler Ebene befasst. Und während ihrer NIS-Länderbesuche 2019 und 2020 hat die Kommission 154 öffentliche und private Einrichtungen sowie 117 zuständige Behörden befragt.

- **Einholung und Nutzung von Expertenwissen**

Die Kommission hat ein Konsortium mit Wavestone, CEPS und ICF unter Vertrag genommen, die sie bei der Überprüfung der NIS-Richtlinie unterstützen sollen.[6] Das Konsortium hat sich nicht nur an die von der NIS-Richtlinie unmittelbar betroffenen

[6] Studie zur Unterstützung der Überprüfung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) – Nr. 2020-665, Wavestone, CEPS und ICF.

Interessenträger im Wege von gezielten Erhebungen und Workshops gewandt, sondern auch verschiedenste Sachverständige für Cybersicherheit wie Forscher und Fachleute der Cybersicherheitsbranche konsultiert.

- **Folgenabschätzung**

Diesem Vorschlag ist eine Folgenabschätzung[7] beigefügt, die dem Ausschuss für Regulierungskontrolle am 23. Oktober 2020 vorgelegt wurde. Der Ausschuss für Regulierungskontrolle gab am 20. November 2020 eine positive Stellungnahme mit Anmerkungen ab. Der Ausschuss empfahl Verbesserungen in einigen Bereichen, damit 1) der Bedeutung von grenzüberschreitenden Spillover-Effekten bei der Problemanalyse besser Rechnung getragen wird, 2) besser erläutert wird, wie Erfolg für die Initiative aussehen würde, 3) die Liste politischer Optionen ausführlicher begründet wird und 4) die Kosten der vorgeschlagenen Maßnahmen genauer dargelegt werden. Die Folgenabschätzung wurde angepasst, um diesen Punkten und detaillierteren Anmerkungen des Ausschusses Folge zu leisten. Sie beinhaltet nun ausführlichere Erläuterungen zur Bedeutung von grenzüberschreitenden Spillover-Effekten auf dem Gebiet der Cybersicherheit, einen klareren Überblick darüber, woran sich der Erfolg messen lässt, ausführlichere Erläuterungen zum Konzept und zur Logik hinter den verschiedenen politischen Optionen und zu den Maßnahmen, die im Rahmen dieser Optionen in Betracht gezogen werden, eine eingehendere Erläuterung der im Zusammenhang mit dem sektoralen Anwendungsbereich der NIS-Richtlinie analysierten Aspekte und weitere Präzisierungen zu den Kosten.

Die Kommission prüfte verschiedene Optionen für die Verbesserung des Rechtsrahmens im Bereich der Cyberresilienz und Reaktion auf Sicherheitsvorfälle:

- „Nicht tätig werden“: Die NIS-Richtlinie würde unverändert bleiben, und es würden auch keine nicht legislativen Maßnahmen ergriffen, um die im Rahmen der Bewertung der NIS-Richtlinie festgestellten Probleme auszuräumen.
- Option 1: Die Rechtsvorschriften würden nicht geändert. Stattdessen würde die Kommission – in Absprache mit der Kooperationsgruppe, der EU-Agentur für Cybersicherheit (ENISA) und ggf. dem Netz der Soforteinsatzteams für IT-Sicherheitsvorfälle (CSIRTs) – Empfehlungen und Leitlinien (z. B. für die Ermittlung von Betreibern wesentlicher Dienste, Sicherheitsanforderungen, Verfahren zur Meldung und Überwachung von Sicherheitsvorfällen) herausgeben.
- Option 2: Diese Option sieht gezielte Änderungen der NIS-Richtlinie vor, darunter eine Ausweitung des Anwendungsbereichs und verschiedene weitere Änderungen, die bestimmte Sofortlösungen für ermittelte Probleme gewährleisten sollen und so mehr Klarheit und eine weitere Harmonisierung bringen würden (z. B. Bestimmungen zur Harmonisierung der Schwellenwerte bei der Ermittlung). Die Struktur, der Ansatz und die Rationale der NIS-Richtlinie blieben jedoch erhalten.
- Option 3: Dieses Szenario sieht systemische und strukturelle Änderungen der NIS-Richtlinie vor (im Wege einer neuen Richtlinie) mit einem grundlegenden Richtungswechsel hin zur Abdeckung eines größeren Segments der Volkswirtschaften in der gesamten Union, aber zugleich mit einer gezielteren Beaufsichtigung großer und wesentlicher Akteure. Ferner sind eine Straffung und umfassendere Harmonisierung der Verpflichtungen von Unternehmen sowie die

[7] **[Links to final document and to the summary sheet to be added.]**

Schaffung eines effektiveren Umfelds für operative Aspekte und einer klaren Grundlage für eine größere gemeinsame Verantwortung und Rechenschaftspflicht verschiedener Interessenträger bei Cybersicherheitsmaßnahmen vorgesehen.

In der Folgenabschätzung wird der Schluss gezogen, dass Option 3 (systemische und strukturelle Änderungen des NIS-Rahmens) der Vorzug zu geben ist. Im Interesse der Wirksamkeit würde bei der bevorzugten Option der Anwendungsbereich der NIS-Richtlinie eindeutig festgelegt werden und sich auf einen repräsentativeren Teil der Volkswirtschaften und Gesellschaften der EU erstrecken, Anforderungen würden vereinheitlicht und die Aufsichts- und Durchsetzungsvorschriften präzisiert, um die Einhaltung zu verbessern. Außerdem sind Maßnahmen vorgesehen, die die Herangehensweisen an die Politikgestaltung auf der Ebene der Mitgliedstaaten verbessern und zu einem Paradigmenwechsel in diesem Bereich führen sollen, indem neue Rahmen für das Risikomanagement der Beziehungen zwischen den Anbietern und die koordinierte Offenlegung von Schwachstellen gefördert werden. Gleichzeitig wird mit der bevorzugten Option eine klare Grundlage für eine gemeinsame Verantwortung und Rechenschaftspflicht geschaffen, und es sind Mechanismen vorgesehen, die mehr Vertrauen zwischen den Mitgliedstaaten seitens der Behörden und seitens der Industrie fördern, Anreize zum Austausch von Informationen und einen operativeren Ansatz gewährleisten sollen, wie z. B. der Amtshilfe- und der Peer-Review-Mechanismus. Diese Option würde auch einen EU-Krisenmanagementrahmen bieten, der auf dem unlängst errichteten operativen EU-Netz aufbaut, und würde eine stärkere Mitwirkung der ENISA, im Rahmen ihres aktuellen Mandats, an einem aktuellen und genauen Überblick über die Cybersicherheitslage in der Union gewährleisten.

Was die Effizienz angeht, so würde die bevorzugte Option zwar zusätzliche Einhaltungs- und Durchsetzungskosten für Unternehmen und Mitgliedstaaten mit sich bringen, aber sie würde auch zu wirksamen Kompromissen und Synergien führen, und laut der Analyse der Optionen verfügt sie über das größte Potenzial, unionsweit ein höheres und einheitliches Cyberresilienzniveau wesentlicher Einrichtungen zu gewährleisten, das schließlich zu Kosteneinsparungen für Unternehmen und für die Gesellschaft führen würde. Diese Option würde eine gewisse zusätzliche Verwaltungslast und höhere Befolgungskosten für die Behörden in den Mitgliedstaaten mit sich bringen. Unterm Strich würde die Option aber mittel- bis langfristig erhebliche Vorteile bringen durch eine verstärkte Zusammenarbeit der Mitgliedstaaten auch auf der operativen Ebene und durch Amtshilfe, Peer-review-Mechanismen sowie einen besseren Überblick über und eine bessere Interaktion mit wesentlichen Unternehmen Anreize für einen Ausbau der Cybersicherheitskapazitäten auf nationaler und regionaler Ebene geben. Die bevorzugte Option würde auch für eine weitgehende Kohärenz mit anderen Rechtsvorschriften, Initiativen und Maßnahmen, darunter auch sektorspezifische *Lex specialis*, sorgen.

Wenn die gegenwärtig unzulängliche Vorsorge im Bereich der Cybersicherheit auf mitgliedstaatlicher Ebene und auf der Ebene von Unternehmen und anderen Organisationen angegangen würde, wären Effizienzgewinne möglich und die durch Cybersicherheitsvorfälle verursachten Zusatzkosten könnten sinken.

- Für wesentliche und wichtige Einrichtungen könnte eine bessere Vorsorge im Bereich der Cybersicherheit dazu beitragen, die potenziellen Einnahmeeinbußen aufgrund von Störungen – auch durch Industriespionage – abzufedern und die hohen Kosten von Ad-hoc-Maßnahmen zur Eindämmung von Bedrohungen zu reduzieren. Dies dürfte die erforderlichen Investitionskosten überwiegen. Wenn gegen die Fragmentierung im Binnenmarkt vorgegangen wird, würde dies auch zu faireren Wettbewerbsbedingungen für Betreiber führen.

- Für die Mitgliedstaaten könnte das Risiko steigender Haushaltsausgaben für Ad-hoc-Maßnahmen zur Eindämmung von Bedrohungen und zusätzlicher Kosten im Zusammenhang mit Cybersicherheitsvorfällen weiter reduziert werden.
- Für Bürgerinnen und Bürger dürften Einkommenseinbußen aufgrund wirtschaftlicher Störungen geringer ausfallen, wenn gegen Cybersicherheitsvorfälle vorgegangen wird.

Das höhere Cybersicherheitsniveau in den Mitgliedstaaten und die Fähigkeit von Unternehmen und Behörden, rasch auf Vorfälle zu reagieren und deren Auswirkungen einzudämmen, wird höchstwahrscheinlich dazu führen, dass das Vertrauen der Bürgerinnen und Bürger in die digitale Wirtschaft insgesamt zunimmt, was sich wiederum positiv auf Wachstum und Investitionen auswirken könnte.

Wird das Cybersicherheitsniveau insgesamt erhöht, nimmt wahrscheinlich auch die Sicherheit zu, und wesentliche Dienste von kritischer Bedeutung für die Gesellschaft funktionieren störungsfrei. Die Initiative hat unter Umständen auch andere positive Auswirkungen auf die Gesellschaft wie z. B. weniger Cyberkriminalität und Terrorismus und ein besserer Katastrophenschutz. Wenn die Vorsorge gegen Cyberangriffe für Unternehmen und andere Organisationen erhöht wird, könnten potenzielle finanzielle Verluste infolge von Cyberangriffen vermieden und so notwendige Entlassungen verhindert werden.

Eine Erhöhung des Cybersicherheitsniveaus könnte auch dazu führen, dass im Falle eines Angriffs auf einen wesentlichen Dienst Umweltgefahren und oder -schäden verhindert werden. Dies könnte insbesondere für den Energie- und den Verkehrssektor sowie die Trinkwasserversorgung von Belang sein. Wenn die Cybersicherheitskapazitäten verstärkt werden, könnte die Initiative dazu führen, dass IKT-Infrastrukturen und -Dienste der neuesten Generation, die zudem umweltverträglicher sind, vermehrt genutzt und ineffiziente und weniger sichere alte Infrastrukturen ersetzt werden. Dies wird voraussichtlich ebenfalls dazu beitragen, die Zahl mit hohen Kosten verbundener Cybersicherheitsvorfälle zu senken, sodass mehr Ressourcen für nachhaltige Investitionen zur Verfügung stehen.

- **Effizienz der Rechtsetzung und Vereinfachung**

Der Vorschlag sieht vor, dass Kleinst- und Kleineinrichtungen generellen aus dem NIS-Anwendungsbereich ausgeschlossen sind und dass eine Vielzahl neuer Einrichtungen des neuen Anwendungsbereichs (sogenannte wichtige Einrichtungen) einer weniger strengen Ex-post-Überwachung unterzogen wird. Durch diese Maßnahmen soll der Aufwand für Unternehmen und Behörden minimiert und gleichmäßiger verteilt werden. Ferner wird in dem Vorschlag das komplexe System für die Ermittlung von Betreibern wesentlicher Dienste durch eine allgemeine Pflicht ersetzt und ein höheres Harmonisierungsniveau der Sicherheits- und Meldepflichten eingeführt, wodurch sich der Befolgungsaufwand insbesondere für die Einrichtungen verringert, die grenzüberschreitende Dienste erbringen.

Der Vorschlag minimiert die Befolgungskosten für KMU, da Einrichtungen nur die Maßnahmen ergreifen müssen, die zur Gewährleistung eines dem jeweiligen Risiko entsprechenden Sicherheitsniveaus für Netz- und Informationssysteme erforderlich sind.

- **Grundrechte**

Die EU setzt alles daran, hohe Standards für den Schutz der Grundrechte zu gewährleisten. Alle freiwillig vereinbarten Informationsweitergaben zwischen Einrichtungen, die diese Richtlinie fördert, fänden in vertrauenswürdiger Umgebung unter uneingeschränkter

Einhaltung der Datenschutzvorschriften der Union, vor allem der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[8] statt.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Siehe Finanzbogen

5. WEITERE ANGABEN

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

Der Vorschlag umfasst einen allgemeinen Plan für das Monitoring und die Bewertung der Auswirkungen auf die spezifischen Ziele, wonach die Kommission spätestens [54 Monate] nach dem Inkrafttreten eine Überprüfung durchführen und dem Europäischen Parlament und dem Rat über die wichtigsten Ergebnisse Bericht erstatten muss.

Die Überprüfung muss gemäß den Leitlinien für eine bessere Rechtsetzung der Kommission durchgeführt werden.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Der Vorschlag ist nach verschiedenen Hauptpolitikfeldern gegliedert, die ineinander greifen und das Cybersicherheitsniveau in der Union verbessern sollen.

Gegenstand und Anwendungsbereich (Artikel 1 und 2)

Die Richtlinie a) verpflichtet die Mitgliedstaaten, eine nationale Cybersicherheitsstrategie zu verabschieden, zuständige nationale Behörden zu benennen und zentrale Anlaufstellen und Soforteinsatzteams für IT-Sicherheitsvorfälle (CSIRTs) einzurichten, b) sieht vor, dass die Mitgliedstaaten Cybersicherheitsrisikomanagement- und Meldepflichten für die in Anhang I genannten wesentlichen Einrichtungen und für die in Anhang II genannten wichtigen Einrichtungen festlegen, c) sieht vor, dass die Mitgliedstaaten Pflichten für die Weitergabe von Cybersicherheitsinformationen festlegen.

Sie gilt für bestimmte öffentliche und private wesentliche Einrichtungen, die in den in Anhang I aufgeführten Sektoren tätig sind (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung und Weltraum) und bestimmte wichtige Einrichtungen, die in den in Anhang II aufgeführten Sektoren tätig sind (Post- und Kurierdienste, Abfallwirtschaft, Herstellung und Vertrieb von Chemikalien, Erzeugung, Verarbeitung und Vertrieb von Nahrungsmitteln, verarbeitende Industrie und Anbieter digitaler Dienste). Kleinst- und Kleineinrichtungen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 fallen nicht in den Anwendungsbereich der Richtlinie, ausgenommen Betreiber von elektronischen Kommunikationsnetzen und Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten, Vertrauensdiensteanbieter, TLD-Namen-Register und öffentliche Verwaltung sowie bestimmte weitere Einrichtungen wie z. B. der einzige Anbieter eines Dienstes in einem Mitgliedstaat.

[8] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Nationale Cybersicherheitsrahmen (Artikel 5 bis 11)

Die Mitgliedstaaten müssen eine nationale Cybersicherheitsstrategie verabschieden, in der die strategischen Ziele und angemessene Politik- und Regulierungsmaßnahmen festgelegt werden, mit denen ein hohes Cybersicherheitsniveau erreicht und aufrechterhalten werden soll.

Die Richtlinie sieht auch einen Rahmen für die koordinierte Offenlegung von Sicherheitslücken vor, und die Mitgliedstaaten müssen CSIRTs einrichten, die als vertrauenswürdige Intermediäre fungieren und die Interaktion zwischen den meldenden Einrichtungen und den Herstellern und Anbietern von IKT-Produkten und IKT-Diensten vereinfachen. Die ENISA muss ein europäisches Register der aufgedeckten Sicherheitslücken einrichten und pflegen.

Die Mitgliedstaaten müssen nationale Rahmen für das Cybersicherheitskrisenmanagement schaffen, u. a. indem sie nationale Behörden benennen, die im Falle großer Cybersicherheitsvorfälle und -krisen zuständig sind.

Ferner müssen die Mitgliedstaaten mindestens eine nationale Cybersicherheitsbehörde benennen, die für die Aufsichtsaufgaben gemäß dieser Richtlinie zuständig ist, sowie eine zentrale nationale Cybersicherheitsanlaufstelle (Single Point of Contact on Cybersecurity, SPOC), die als Verbindungsstelle fungiert, um die grenzübergreifende Zusammenarbeit mitgliedstaatlicher Behörden sicherzustellen. Ferner müssen die Mitgliedstaaten CSIRTs benennen.

Zusammenarbeit (Artikel 12 bis 16)

Die Richtlinie sieht die Einsetzung einer Kooperationsgruppe vor, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zu unterstützen und zu erleichtern und Vertrauen aufzubauen. Ferner sieht sie die Errichtung eines CSIRT-Netzwerks vor, um zur Vertrauensbildung zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern.

Es wird ein Europäisches Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network, EU-CyCLONe) eingerichtet, um die koordinierte Bewältigung großer Cybersicherheitsvorfälle und -krisen zu unterstützen und den regelmäßigen Informationsaustausch zwischen Mitgliedstaaten und EU-Organen zu gewährleisten.

Die ENISA muss in Zusammenarbeit mit der Kommission einen zweijährlichen Bericht über die Cybersicherheitslage in der Union herausgeben.

Die Kommission muss ein System einführen, das regelmäßige Peer-Reviews der Wirksamkeit der Cybersicherheitspolitik der Mitgliedstaaten ermöglicht.

Cybersicherheitsrisikomanagement- und Meldepflichten (Artikel 17 bis 23)

Gemäß dem Vorschlag müssen die Mitgliedstaaten vorschreiben, dass die Führungsebenen aller Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen, die von ihren jeweiligen Einrichtungen ergriffenen Cybersicherheitsrisikomanagementmaßnahmen genehmigen und spezielle Cybersicherheitsschulungen absolvieren müssen.

Die Mitgliedstaaten müssen sicherstellen, dass die in den Anwendungsbereich der Richtlinie fallenden Eirichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Cybersicherheit von Netz- und Informationssystemen zu bewältigen. Sie müssen ferner sicherstellen, dass die Einrichtungen den zuständigen nationalen Behörden oder den CSIRTs jeden Cybersicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung des von ihnen erbrachten Dienstes hat, unverzüglich melden.

TLD-Register und die Einrichtungen, die Domänennamenregistrierungsdienste für die TLD erbringen, sammeln exakte und vollständige Daten über die Registrierung der Domänennamen und pflegen diese. Darüber hinaus müssen diese Einrichtungen auch dafür sorgen, dass berechtigte Zugangsnachfrager effektiv Zugang zu Daten über die Registrierung von Domänennamen haben.

Gerichtsbarkeit und Registrierung (Artikel 24 and 25)

Grundsätzlich wird davon ausgegangen, dass wesentliche und wichtige Einrichtungen unter die Gerichtsbarkeit des Mitgliedstaats fallen, in dem sie ihre Dienste anbieten. Für bestimmte Arten von Einrichtungen (DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten und Betreiber von Inhaltszustellnetzen sowie bestimmte Anbieter digitaler Dienste) wird davon ausgegangen, dass sie unter die Gerichtsbarkeit des Mitgliedstaats fallen, in dem sie ihre Hauptniederlassung in der Union haben. So soll sichergestellt werden, dass diese Einrichtungen nicht mit einer Vielzahl unterschiedlicher gesetzlicher Anforderungen konfrontiert werden, wenn sie in besonders ausgeprägtem Maße Dienste über Grenzen hinweg anbieten. Die ENISA muss ein Register solcher Einrichtungen einrichten und pflegen.

Informationsweitergabe (Artikel 26 and 27)

Die Mitgliedstaaten legen Regeln fest, die es Einrichtungen ermöglichen, im Einklang mit Artikel 101 AEUV innerhalb des Rahmens für freiwillig vereinbarte Weitergaben spezifischer Cybersicherheitsinformationen cybersicherheitsbezogene Informationen weiterzugeben. Außerdem ermöglichen die Mitgliedstaaten es nicht in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen, freiwillig erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle zu melden.

Aufsicht und Durchsetzung (Artikel 28 bis 34)

Die zuständigen Behörden müssen die in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen beaufsichtigen, insbesondere um sicherzustellen, dass sie die Sicherheitsanforderungen und die Pflicht zur Meldung von Sicherheitsvorfällen einhalten. Es wird zwischen einer Ex-ante-Beaufsichtigung wesentlicher Einrichtungen und einer Ex-post-Beaufsichtigung wichtiger Einrichtungen unterschieden. Bei letzterer müssen die zuständigen Behörden erst dann tätig werden, wenn ihnen Beweise dafür oder Hinweise darauf vorgelegt werden, dass eine wichtige Einrichtung die Sicherheitsanforderungen oder die Pflicht zur Meldung von Sicherheitsvorfällen nicht einhält.

Die Richtlinie sieht ferner vor, dass die Mitgliedstaaten Geldbußen gegen wesentliche und wichtige Einrichtungen verhängen, und legt bestimmte Höchstgeldbußen fest.

Die Mitgliedstaaten müssen im Bedarfsfall zusammenarbeiten und einander unterstützen, wenn Einrichtungen Dienste in mehr als einem Mitgliedstaat anbieten oder wenn sich die

Hauptniederlassung einer Einrichtung oder ihr Vertreter in einem Mitgliedstaat befinden, ihre Netz- und Informationssysteme aber in einem oder mehreren anderen Mitgliedstaaten verortet sind.

2020/0359 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[9],

nach Stellungnahme des Ausschusses der Regionen[10],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[11] war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Cybersicherheitsvorfällen, um so zum reibungslosen Funktionieren der Wirtschaft und Gesellschaft der Union beizutragen.

(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Festlegung nationaler Cybersicherheitsstrategien, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen sichergestellt. Darüber hinaus hat sie durch die Einrichtung der Kooperationsgruppe[12] und eines Netzwerks nationaler Reaktionsteams für IT-

[9] ABl. C [...] vom [...], S. [...].

[10] ABl. C [...] vom [...], S. [...].

[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

[12] Artikel 11 der Richtlinie (EU) 2016/1148.

Sicherheitsvorfälle (CSIRT-Netzwerk)[13] zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern.

(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen. Heute sind daher im Bereich Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts.

(4) Rechtsgrundlage der Richtlinie (EU) 1148/2016 war Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der verstärkte Maßnahmen zur Angleichung der einzelstaatlichen Vorschriften vorsieht, die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben. Die Anforderungen an die Cybersicherheit, die Einrichtungen, die Dienste erbringen oder wirtschaftlich relevante Tätigkeiten ausüben, auferlegt werden, unterscheiden sich von Mitgliedstaat zu Mitgliedstaat erheblich in Bezug auf die Art der Anforderung, ihre Detailliertheit und die Art der Aufsicht. Diese Unterschiede verursachen zusätzliche Kosten und führen zu Schwierigkeiten für Unternehmen, die Waren oder Dienstleistungen grenzüberschreitend anbieten. Anforderungen, die von einem Mitgliedstaat auferlegt werden und sich von denen eines anderen Mitgliedstaats unterscheiden oder sogar im Widerspruch zu ihnen stehen, können diese grenzüberschreitenden Tätigkeiten wesentlich beeinträchtigen. Darüber hinaus dürfte, insbesondere angesichts des intensiven grenzüberschreitenden Austauschs, eine etwaige suboptimale Gestaltung oder Umsetzung von Cybersicherheitsstandards in einem Mitgliedstaat Auswirkungen auf das Cybersicherheitsniveau anderer Mitgliedstaaten haben. Die Überprüfung der Richtlinie (EU) 2016/1148 hat gezeigt, dass die Mitgliedstaaten die Richtlinie sehr unterschiedlich umsetzen, unter anderem in Bezug auf ihren Anwendungsbereich, dessen Abgrenzung weitgehend im Ermessen der Mitgliedstaaten lag. In der Richtlinie (EU) 2016/1148 wurde den Mitgliedstaaten auch ein sehr großer Ermessensspielraum bei der Umsetzung der in der Richtlinie festgelegten Verpflichtungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen eingeräumt. Diese Verpflichtungen wurden daher auf nationaler Ebene auf sehr unterschiedliche Weise umgesetzt. Ähnliche Unterschiede gab es bei der Umsetzung der in der Richtlinie enthaltenen Bestimmungen zu Aufsicht und Durchsetzung.

(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von

[13] Artikel 12 der Richtlinie (EU) 2016/1148.

Diensten und das Niveau der Cyberresilienz beeinträchtigen. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.

(6) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang sind nationale und Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol[14] von Bedeutung.

(7) Mit der Aufhebung der Richtlinie (EU) 2016/1148 sollte der Anwendungsbereich nach Sektoren aus den in den Erwägungsgründen 4 bis 6 dargelegten Gründen auf einen größeren Teil der Wirtschaft ausgeweitet werden. Die Liste der Sektoren, die unter die Richtlinie (EU) 2016/1148 fallen, sollte daher erweitert werden, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind. Bei den Vorschriften sollte nicht danach unterschieden werden, ob es sich bei den Einrichtungen um Betreiber wesentlicher Dienste oder um Anbieter digitaler Dienste handelt. Diese Differenzierung hat sich als überholt erwiesen, da sie nicht die tatsächliche Bedeutung der Sektoren oder Dienste für die gesellschaftlichen und wirtschaftlichen Tätigkeiten im Binnenmarkt widerspiegelt.

(8) Gemäß der Richtlinie (EU) 2016/1148 waren die Mitgliedstaaten dafür zuständig zu bestimmen, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen („Ermittlungsprozess“). Um die diesbezüglichen großen Unterschiede zwischen den Mitgliedstaaten zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich der Risikomanagementanforderungen und der Meldepflichten zu gewährleisten, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle mittleren und großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[15], die in den Sektoren tätig sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den

[14] Mithilfe des Traffic Light Protocol (TLP) kann jemand, der Informationen weitergibt, die Empfänger über etwaige Einschränkungen bei der weiteren Verbreitung dieser Informationen informieren. Es wird in fast allen CSIRT-Gemeinschaften und einigen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) genutzt.

[15] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

Anwendungsbereich der Richtlinie fallen. Die Mitgliedstaaten sollten nicht verpflichtet sein, eine Liste der Einrichtungen zu erstellen, die dieses allgemein anwendbare größenbezogene Kriterium erfüllen.

(9) Allerdings sollten auch Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln.

(10) Die Kommission kann in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für Klein- und Kleinstunternehmen geltenden Kriterien herausgeben.

(11) Je nach Sektor, in dem sie tätig sind, oder der Art der von ihnen erbrachten Dienste sollten bei den in den Anwendungsbereich der vorliegenden Richtlinie fallenden Einrichtungen zwei Kategorien unterschieden werden: wesentlich und wichtig. Bei der Einstufung sollte dem Grad der Kritikalität des Sektors oder der Art des Dienstes sowie dem Grad der Abhängigkeit anderer Sektoren oder Arten von Diensten Rechnung getragen werden. Sowohl die wesentlichen als auch die wichtigen Einrichtungen sollten denselben Risikomanagementanforderungen und Meldepflichten unterliegen. Bei den Aufsichts- und Sanktionsregelungen sollte zwischen diesen beiden Kategorien von Einrichtungen differenziert werden, um ein ausgewogenes Verhältnis zwischen Anforderungen und Pflichten einerseits und dem Verwaltungsaufwand, der sich andererseits aus der Überwachung der Einhaltung ergibt, zu gewährleisten.

(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle oder erhebliche Cyberbedrohungen melden und ist dies in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. Die Kommission kann Leitlinien im Zusammenhang mit der Umsetzung der *lex specialis* herausgeben. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur Meldung von Sicherheitsvorfällen erlassen werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

(13) Die Verordnung XXXX/XXXX des Europäischen Parlaments und des Rates[16] sollte im Zusammenhang mit der vorliegenden Richtlinie als sektorspezifischer Rechtsakt der Union in Bezug auf Einrichtungen des Finanzsektors betrachtet werden. Anstelle der Bestimmungen der vorliegenden Richtlinie sollten die Bestimmungen der Verordnung XXXX/XXXX gelten, die sich auf Risikomanagementmaßnahmen im Bereich der Informations- und Kommunikationstechnologie (IKT), das Management

[16] *[vollständigen Titel und Fundstelle im Amtsblatt einfügen sobald bekannt]*.

und insbesondere die Meldung von IKT-bezogenen Vorfällen sowie die Prüfung der digitalen Betriebsstabilität, Vereinbarungen über den Informationsaustausch und Risiken durch IKT-Drittanbieter beziehen. Die Mitgliedstaaten sollten daher die Bestimmungen der vorliegenden Richtlinie, die sich auf Cybersicherheitsrisikomanagement und Meldepflichten, Informationsaustausch sowie Aufsicht und Durchsetzung beziehen, nicht auf Finanzunternehmen anwenden, die unter die Verordnung XXXX/XXXX fallen. Gleichzeitig ist es wichtig, im Rahmen der vorliegenden Richtlinie eine enge Beziehung zum und den Informationsaustausch mit dem Finanzsektor aufrechtzuerhalten. Zu diesem Zweck ist es gemäß der Verordnung XXXX/XXXX zulässig, dass die Finanzaufsichtsbehörden, die Europäischen Aufsichtsbehörden für den Finanzsektor und die gemäß der Verordnung XXXX/XXXX zuständigen nationalen Behörden sich an strategischen politischen Diskussionen und der technischen Arbeit der Kooperationsgruppe beteiligen und mit den gemäß der vorliegenden Richtlinie benannten zentralen Anlaufstellen sowie den nationalen CSIRTs Informationen austauschen und zusammenarbeiten. Die gemäß der Verordnung XXXX/XXXX zuständigen Behörden sollten Einzelheiten zu schwerwiegenden IKT-bezogenen Vorfällen auch an die gemäß der vorliegenden Richtlinie benannten zentralen Anlaufstellen übermitteln. Darüber hinaus sollten die Mitgliedstaaten den Finanzsektor weiterhin in ihre Cybersicherheitsstrategien einbeziehen, und die nationalen CSIRTs dürfen den Finanzsektor bei ihren Tätigkeiten einbeziehen.

(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen gleichgestellte Einrichtungen im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen der gemäß der vorliegenden Richtlinie zuständigen Behörde und der gemäß Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über Sicherheitsvorfälle und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ihre Aufsichts- und Durchsetzungsbefugnisse gegenüber einer als kritisch eingestuften wesentlichen Einrichtung auszuüben. Beide Behörden sollten zu diesem Zweck zusammenarbeiten und Informationen austauschen.

(15) Die Beibehaltung eines zuverlässigen, resilienten und sicheren Domänennamensystems (DNS) ist ein Schlüsselfaktor für die Wahrung der Integrität des Internets und von entscheidender Bedeutung für dessen kontinuierlichen und stabilen Betrieb, von dem die digitale Wirtschaft und Gesellschaft abhängig ist. Daher sollte die vorliegende Richtlinie für alle Anbieter von DNS-Diensten entlang der

[17] *[vollständigen Titel und Fundstelle im Amtsblatt einfügen sobald bekannt]*.

DNS-Auflösungskette gelten, einschließlich Betreibern von Root-Namenservern, Namenservern der Domäne oberster Stufe (TLD-Namenservern), autoritativen Namenservern für Domänennamen und rekursiven Resolvern.

(16) Cloud-Computing-Dienste sollten Dienste umfassen, die auf Abruf und umfassend Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer und verteilter Rechenressourcen ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste. Die Bereitstellungsmodelle für Cloud-Computing sollten die private, die gemeinschaftliche, die öffentliche und die hybride Cloud umfassen. Die genannten Dienst- und Bereitstellungsmodelle haben dieselbe Bedeutung wie die in der Norm ISO/IEC 17788:2014 definierten Dienst- und Bereitstellungsmodelle. Dass sich der Cloud-Computing-Nutzer selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als Verwaltung auf Abruf beschrieben werden. Der Begriff „umfassender Fernzugang“ wird verwendet, um zu beschreiben, dass die Cloud-Kapazitäten über das Netz bereitgestellt und über Mechanismen zugänglich gemacht werden, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (einschließlich Mobiltelefonen, Tablets, Laptops, Arbeitsplatzrechnern) fördern. Der Begriff „skalierbar“ bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastischer Pool“ wird verwendet, um die Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die Menge der verfügbaren Ressourcen je nach Arbeitsaufkommen rasch erhöht oder reduziert werden kann. Der Begriff „gemeinsam nutzbar“ wird verwendet, um die Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird. Der Begriff „verteilt“ wird verwendet, um die Rechenressourcen zu beschreiben, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und koordinieren.

(17) Angesichts des Aufkommens innovativer Technologien und neuer Geschäftsmodelle dürften auf dem Markt neue Bereitstellungs- und Dienstmodelle für Cloud-Computing entstehen, um den sich wandelnden Kundenbedürfnissen gerecht zu werden. In diesem Zusammenhang können Cloud-Computing-Dienste in hochgradig verteilter Form, noch näher am Ort der Datengenerierung oder -sammlung, erbracht werden, wodurch vom traditionellen Modell zu einem hochgradig verteilten Modell („Edge-Computing“) übergegangen wird.

(18) Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur. Um allen Risiken für die Sicherheit von Netz- und Informationssystemen zu begegnen, sollte die vorliegende Richtlinie auch für Anbieter solcher Rechenzentrumsdienste gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Für die Zwecke der vorliegenden Richtlinie sollte der Begriff „Rechenzentrumsdienst“ Dienstleistungen umfassen, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie und Netzausrüstungen zur Erbringung von

Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden. Der Begriff „Rechenzentrumsdienst“ gilt nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von ihr für eigene Zwecke betrieben werden.

(19) Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates[18] sowie Anbieter von Express- und Kurierdiensten sollten der vorliegenden Richtlinie unterliegen, wenn sie mindestens einen der Schritte in der Postzustellkette und insbesondere Abholung, Sortierung oder Zustellung, einschließlich Abholung durch den Empfänger, anbieten. Transportdienste, die nicht in Verbindung mit einem dieser Schritte erbracht werden, sollten nicht unter Postdienste fallen.

(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die COVID-19-Pandemie hat gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.

(21) Angesichts der unterschiedlichen nationalen Governancestrukturen und zwecks Beibehaltung von bereits bestehenden sektorbezogenen Vereinbarungen und Aufsichts- oder Regulierungsstellen der Union sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von wesentlichen und wichtigen Einrichtungen gemäß der vorliegenden Richtlinie zuständig sind. Die Mitgliedstaaten sollten diese Funktion einer bestehenden Behörde zuweisen dürfen.

(22) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen Behörden und um die wirksame Umsetzung der vorliegenden Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat eine nationale zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der Sicherheit von Netz-und Informationssystemen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist.

[18] Richtlinie 97/67/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstequalität (ABl. L 15 vom 21.1.1998, S. 14).

(23) Einrichtungen sollten den zuständigen Behörden oder den CSIRTs Sicherheitsvorfälle wirksam und effizient melden. Die zentralen Anlaufstellen sollten beauftragt werden, die Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten. Damit sichergestellt ist, dass es pro Mitgliedstaat nur eine einzige behördliche Anlaufstelle gibt, sollten die zentralen Anlaufstellen auch relevante Informationen über Vorfälle, die Einrichtungen des Finanzsektors betreffen, von den gemäß der Verordnung XXXX/XXXX zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die zuständigen nationalen Behörden oder CSIRTs weiterleiten können sollten.

(24) Die Mitgliedstaaten sollten über angemessene technische und organisatorische Kapazitäten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen. Die Mitgliedstaaten sollten daher sicherstellen, dass sie über gut funktionierende Reaktionsteams für IT-Sicherheitsvorfälle – Computer Security Incident Response Teams (CSIRTs) oder auch Computer Emergency Response Teams (CERTs) genannt – verfügen, die die grundlegenden Anforderungen erfüllen, damit wirksame und kompatible Kapazitäten zur Bewältigung von Sicherheitsvorfällen und Risiken und eine effiziente Zusammenarbeit auf Unionsebene gewährleistet sind. Um das Vertrauensverhältnis zwischen den Einrichtungen und den CSIRTs zu stärken, sollten die Mitgliedstaaten in Fällen, in denen ein CSIRT Teil der zuständigen Behörde ist, eine funktionale Trennung zwischen den operativen Aufgaben der CSIRTs, insbesondere in Bezug auf den Informationsaustausch und die Unterstützung der Einrichtungen, und den Aufsichtstätigkeiten der zuständigen Behörden in Erwägung ziehen.

(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine proaktive Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.

(26) Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch die vorliegende Richtlinie geschaffenen CSIRT-Netzwerk an internationalen Kooperationsnetzen beteiligen können.

(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die

[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

[20] 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).

Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.

(28) Da durch die Ausnutzung von Schwachstellen in Netz- und Informationssystemen erhebliche Störungen und Schäden verursacht werden können, ist die rasche Erkennung und Behebung dieser Schwachstellen ein wichtiger Faktor bei der Verringerung des Cybersicherheitsrisikos. Einrichtungen, die solche Systeme entwickeln, sollten daher geeignete Verfahren für die Behandlung von entdeckten Schwachstellen festlegen. Da Schwachstellen häufig von Dritten (meldenden Einrichtungen) entdeckt und gemeldet (offengelegt) werden, sollte der Hersteller oder Anbieter von IKT-Produkten oder -Diensten auch Verfahren einführen, damit er von Dritten Informationen über Schwachstellen entgegennehmen kann. Diesbezüglich enthalten die internationalen Normen ISO/IEC 30111 und ISO/IEC 29417 Leitlinien für die Behandlung von Schwachstellen bzw. die Offenlegung von Schwachstellen. In Bezug auf die Offenlegung von Schwachstellen ist die Koordinierung zwischen meldenden Einrichtungen und Herstellern oder Anbietern von IKT-Produkten oder -Diensten besonders wichtig. Die koordinierte Offenlegung von Schwachstellen erfolgt in einem strukturierten Prozess, in dem den Organisationen Schwachstellen in einer Weise gemeldet werden, die der Organisation die Diagnose und Behebung der Schwachstelle ermöglicht, bevor detaillierte Informationen über die Schwachstelle an Dritte oder die Öffentlichkeit weitergegeben werden. Die koordinierte Offenlegung von Schwachstellen sollte auch die Koordinierung zwischen der meldenden Einrichtung und der Organisation in Bezug auf den Zeitplan für die Behebung und Veröffentlichung von Schwachstellen umfassen.

(29) Die Mitgliedstaaten sollten daher Maßnahmen ergreifen, um eine koordinierte Offenlegung von Schwachstellen zu erleichtern, indem sie eine einschlägige nationale Strategie festlegen. In diesem Zusammenhang sollten die Mitgliedstaaten ein CSIRT benennen, das die Rolle des „Koordinators“ übernimmt und gegebenenfalls zwischen den meldenden Einrichtungen und den Herstellern oder Anbietern von IKT-Produkten oder -Diensten vermittelt. Zu den Aufgaben des als Koordinator benannten CSIRT sollte insbesondere gehören, betroffene Einrichtungen zu ermitteln und zu kontaktieren, meldende Einrichtungen zu unterstützen, Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Organisationen betreffen (Offenlegung von Schwachstellen, die mehrere Parteien betreffen). Betreffen Schwachstellen mehrere Hersteller oder Anbieter von IKT-Produkten oder -Diensten, die in mehr als einem Mitgliedstaat niedergelassen sind, sollten die benannten CSIRTs aus den betroffenen Mitgliedstaaten im Rahmen des CSIRT-Netzwerkes zusammenarbeiten.

(30) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste beeinträchtigen, trägt zu einem besseren Cybersicherheitsrisikomanagement bei. In dieser Hinsicht sind öffentlich zugängliche Informationen über Schwachstellen nicht nur für Einrichtungen und deren Nutzer, sondern auch für die zuständigen nationalen Behörden und die CSIRTs ein wichtiges Instrument. Aus diesem Grund sollte die ENISA ein Schwachstellenregister

einrichten, in dem wesentliche und wichtige Einrichtungen und deren Anbieter sowie, auf freiwilliger Basis, Einrichtungen, die nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen, Schwachstellen offenlegen und Informationen über die Schwachstellen bereitstellen, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen.

(31) Es gibt zwar bereits ähnliche Register oder Datenbanken für Schwachstellen, aber diese werden von Einrichtungen betrieben und gepflegt, die nicht in der Union niedergelassen sind. Ein von der ENISA gepflegtes europäisches Schwachstellenregister würde für mehr Transparenz in Bezug auf den Prozess der Veröffentlichung vor der offiziellen Offenlegung der Schwachstelle sorgen und die Resilienz im Falle von Störungen oder Unterbrechungen bei der Erbringung ähnlicher Dienste verbessern. Um Doppelarbeit zu vermeiden und im Interesse der größtmöglichen Komplementarität, sollte die ENISA die Möglichkeit prüfen, Vereinbarungen über eine strukturierte Zusammenarbeit mit ähnlichen Registern in Drittländern zu schließen.

(32) Die Kooperationsgruppe sollte alle zwei Jahre ein Arbeitsprogramm aufstellen, in dem die Maßnahmen aufgeführt sind, die die Gruppe zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen hat. Der Zeitrahmen des ersten Programms, das gemäß der vorliegenden Richtlinie angenommen wird, sollte an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 angenommenen Programms angepasst werden, um etwaige Unterbrechungen der Arbeit der Gruppe zu vermeiden.

(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren.

(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3), die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit einzuladen.

(35) Die zuständigen Behörden und CSIRTs sollten befugt sein, an Austauschprogrammen für Bedienstete aus anderen Mitgliedstaaten teilzunehmen, um die Zusammenarbeit zu verbessern. Die zuständigen Behörden sollten Maßnahmen ergreifen, damit die Bediensteten aus anderen Mitgliedstaaten bei den Tätigkeiten der aufnehmenden zuständigen Behörde konstruktiv mitwirken können.

(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. Solche Übereinkünfte sollten einen angemessenen Datenschutz gewährleisten.

(37) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere das Netzwerk der Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe), das CSIRT-Netzwerk und die Kooperationsgruppe – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 beitragen. EU-CyCLONe und das CSIRT-Netzwerk sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Modalitäten dieser Zusammenarbeit festgelegt werden. In der Geschäftsordnung von EU-CyCLONe sollten die Modalitäten für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich, aber nicht beschränkt auf Funktion und Aufgaben, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) stützen. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. Berührt die Krise eine wichtige externe Dimension oder eine Dimension der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), so sollte der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD) ausgelöst werden.

(38) Für die Zwecke der vorliegenden Richtlinie sollte sich der Begriff „Risiko“ auf das Potenzial für Verluste oder Störungen infolge eines Cybersicherheitsvorfalls beziehen und als Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des besagten Sicherheitsvorfalls ausgedrückt werden.

(39) Für die Zwecke der vorliegenden Richtlinie sollte sich der Begriff „Beinahe-Vorfälle“ auf ein Ereignis beziehen, das das Potenzial gehabt hätte, Schäden zu verursachen, dessen vollständiger Eintritt jedoch verhindert wurde.

(40) Das Risikomanagement sollte auch Maßnahmen zur Ermittlung jeder Gefahr eines Sicherheitsvorfalls, zur Verhinderung, Aufdeckung und Bewältigung von Sicherheitsvorfällen sowie der Minderung ihrer Folgen umfassen. Die Sicherheit von Netz- und Informationssystemen sollte sich auch auf gespeicherte, übermittelte und verarbeitete Daten erstrecken.

(41) Damit keine unverhältnismäßige finanzielle und administrative Belastung für wesentliche und wichtige Einrichtungen entsteht, sollten die Anforderungen an das Cybersicherheitsrisikomanagement in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei wird dem bei solchen Maßnahmen geltenden neuesten Stand Rechnung getragen.

(42) Wesentliche und wichtige Einrichtungen sollten die Sicherheit der bei ihren Tätigkeiten verwendeten Netz- und Informationssysteme gewährleisten. Hauptsächlich handelt es sich dabei um private Netz- und Informationssysteme, die entweder von internem IT-Personal verwaltet werden oder deren Sicherheit Dritten anvertraut wurde. Die Anforderungen an das Cybersicherheitsrisikomanagement und die Meldepflicht gemäß der vorliegenden Richtlinie sollten für die einschlägigen wesentlichen und wichtigen Einrichtungen unabhängig davon gelten, ob sie ihre Netz- und Informationssysteme intern warten oder diese Aufgabe ausgliedern.

(43) Besonders wichtig ist die Bewältigung von Cybersicherheitsrisiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten betreffen, da sich die

Vorfälle häufen, bei denen Einrichtungen Opfer von Cyberangriffen werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Dienstleistungen Dritter ausgenutzt werden. Die Einrichtungen sollten daher die Gesamtqualität der Produkte und Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen.

(44) Unter den Diensteanbietern spielen die Anbieter verwalteter Sicherheitsdienste (Managed Security Services Providers, MSSP) in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung eine überaus wichtige Rolle, indem sie Einrichtungen bei deren Bemühungen um die Erkennung und Bewältigung von Sicherheitsvorfällen unterstützen. Allerdings sind auch die MSSP selbst das Ziel von Cyberangriffen und stellen durch ihre enge Einbindung in die Tätigkeiten der Betreiber ein besonderes Cybersicherheitsrisiko dar. Die Einrichtungen sollten daher bei der Wahl eines MSSP erhöhte Sorgfalt walten lassen.

(45) Die Einrichtungen sollten sich auch mit Cybersicherheitsrisiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben. Insbesondere sollten die Einrichtungen durch geeignete Maßnahmen sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht und dabei bewährte Verfahren befolgt werden, was den sicheren Zugang zu sowie die Verbreitung von Informationen im Allgemeinen und den Schutz des geistigen Eigentums im Besonderen angeht. Auch sollten in Anbetracht der Bedeutung und des Wertes von Daten für die Tätigkeiten der Einrichtungen letztere alle geeigneten Cybersicherheitsmaßnahmen ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen.

(46) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Cybersicherheitsrisiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe, an der die einschlägigen nationalen Behörden beteiligt sind, in Zusammenarbeit mit der Kommission und der ENISA koordinierte sektorenbezogene Lieferketten-Risikobewertungen – wie im Fall der 5G-Netze gemäß der einschlägigen Empfehlung (EU) 2019/534[21] – durchführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.

(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter

[21] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).

kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.

(48) Zur Straffung der rechtlichen Verpflichtungen, die Anbietern öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste sowie Vertrauensdiensteanbietern hinsichtlich der Sicherheit ihrer Netze und Informationssysteme auferlegt werden, und um diese Einrichtungen und ihre jeweiligen zuständigen Behörden von dem durch diese Richtlinie geschaffenen Rechtsrahmen profitieren zu lassen (u. a. Benennung der für die Bewältigung von Risiken und Vorfällen zuständigen Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs), Beteiligung der zuständigen Behörden und Stellen an der Arbeit der Kooperationsgruppe und des CSIRT-Netzwerks), sollten sie in den Anwendungsbereich dieser Richtlinie aufgenommen werden. Die entsprechenden Bestimmungen der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates[22] und der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates[23], mit denen diesen Arten von Einrichtungen Sicherheitsanforderungen und Meldepflichten auferlegt werden, sollten daher aufgehoben werden. Die Vorschriften über die Meldepflichten sollten die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[24] unberührt lassen.

(49) Sofern angebracht und um unnötige Unterbrechungen zu vermeiden, sollten bestehende nationale Leitlinien und nationale Rechtsvorschriften, die zur Umsetzung der Vorschriften über Sicherheitsmaßnahmen gemäß Artikel 40 Absatz 1 der Richtlinie (EU) 2018/1972 sowie der Anforderungen des Artikels 40 Absatz 2 der genannten Richtlinie bezüglich der Parameter zur Bestimmung des Ausmaßes eines Sicherheitsvorfalls erlassen wurden, weiterhin von den für die Überwachung und Durchsetzung im Sinne dieser Richtlinie zuständigen Behörden genutzt werden.

(50) Angesichts der wachsenden Bedeutung nummernunabhängiger interpersoneller Kommunikationsdienste muss sichergestellt werden, dass auch für diese Dienste angemessene Sicherheitsanforderungen entsprechend ihrer spezifischen Art und wirtschaftlichen Bedeutung gelten. Die Anbieter solcher Dienste sollten daher auch ein Sicherheitsniveau von Netz- und Informationssystemen gewährleisten, das dem bestehenden Risiko angemessen ist. Da die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze ausüben, kann das Risiko für solche Dienste in gewisser Hinsicht als geringer erachtet werden als für herkömmliche elektronische Kommunikationsdienste. Dasselbe gilt auch für interpersonelle

---

22 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

23 Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36).

24 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Kommunikationsdienste, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben.

(51) Das Funktionieren des Internets ist für den Binnenmarkt wichtiger denn je. Die Dienstleistungen praktisch aller wesentlichen und wichtigen Einrichtungen hängen ihrerseits von Diensten ab, die über das Internet erbracht werden. Für die reibungslose Bereitstellung von Diensten wesentlicher und wichtiger Einrichtungen ist es wichtig, dass für öffentliche elektronische Kommunikationsnetze, z. B. Internet-Backbone- oder Seekabel, geeignete Cybersicherheitsmaßnahmen bestehen und diesbezügliche Sicherheitsvorfälle gemeldet werden.

(52) Gegebenenfalls sollten die Einrichtungen die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern. Die Verpflichtung zur Information der Empfänger über solche Bedrohungen sollte die Einrichtungen nicht von der Pflicht befreien, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen sollte für die Empfänger kostenlos sein.

(53) Insbesondere sollten die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über Maßnahmen zum Schutz von Kommunikationsinhalten, die sie treffen können, informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren.

(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste sollte die Verschlüsselung, insbesondere von Ende zu Ende, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke des Artikels 18 vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung sollte mit den Befugnissen der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen, in Einklang gebracht werden. Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten und zugleich eine wirksame Reaktion auf Straftaten gewährleisten.

(55) Mit dieser Richtlinie wird ein zweistufiger Ansatz für die Meldung von Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von Sicherheitsvorfällen entgegenwirkt und den Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Unternehmen und ganze Sektoren ihre Resilienz gegenüber Cyberbedrohungen im Laufe der Zeit verbessern können. Erhalten Einrichtungen Kenntnis von einem Sicherheitsvorfall, sollten sie innerhalb von 24 Stunden eine erste Meldung übermitteln und spätestens einen Monat danach einen Abschlussbericht vorlegen müssen. Die Erstmeldung sollte nur die Informationen enthalten, die unbedingt

erforderlich sind, um die zuständigen Behörden über den Sicherheitsvorfall zu unterrichten und es der Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Gegebenenfalls sollte aus dieser Meldung hervorgehen, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen der meldenden Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden. Zur weiteren Verhinderung, dass die Meldepflichten für Sicherheitsvorfälle entweder zulasten der Ressourcen gehen, auf solche Vorfälle zu reagieren, oder entsprechende Anstrengungen der Einrichtungen anderweitig beeinträchtigt werden, sollten die Mitgliedstaaten auch vorsehen, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von der Frist von 24 Stunden für die Erstmeldung bzw. einem Monat für den Abschlussbericht abweichen kann.

(56) Wesentliche und wichtige Einrichtungen sind häufig in einer Situation, in der ein bestimmter Sicherheitsvorfall aufgrund seiner Merkmale und sich aus verschiedenen Rechtsinstrumenten ergebender Meldepflichten verschiedenen Behörden gemeldet werden muss. Solche Fälle führen zu zusätzlichen Belastungen und unter Umständen auch zu Unsicherheiten hinsichtlich des Formats solcher Meldungen und der für sie geltenden Verfahren. Vor diesem Hintergrund und zur Vereinfachung der Meldung von Sicherheitsvorfällen sollten die Mitgliedstaaten eine zentrale Anlaufstelle für alle Meldungen einrichten, die aufgrund dieser Richtlinie sowie anderer EU-Rechtsvorschriften wie der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG vorgeschrieben sind. Die ENISA sollte in Zusammenarbeit mit der Kooperationsgruppe mittels Leitlinien einheitliche Meldemuster erstellen, die die im Unionsrecht geforderten Informationen vereinfachen und straffen und den Aufwand für die Unternehmen verringern würden.

(57) Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen nach Unionsrecht oder nationalem Recht steht, sollten die Mitgliedstaaten wesentliche und wichtige Einrichtungen – auf der Grundlage geltender strafverfahrensrechtlicher Bestimmungen im Einklang mit dem Unionsrecht – dazu anhalten, diese Sicherheitsvorfälle mit einem mutmaßlichen schwerwiegenden kriminellen Hintergrund den zuständigen Strafverfolgungsbehörden zu melden. Unbeschadet der für Europol geltenden Vorschriften für den Schutz personenbezogener Daten ist gegebenenfalls die Unterstützung durch das EC3 und die ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden verschiedener Mitgliedstaaten wünschenswert.

(58) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. In diesem Zusammenhang sollten die zuständigen Behörden gemäß der Richtlinie 2002/58/EG mit den Datenschutzbehörden und den Aufsichtsbehörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.

(59) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in der Union beiträgt. Werden auch personenbezogene Daten

verarbeitet, so muss diese Verarbeitung mit dem EU-Datenschutzrecht im Einklang stehen.

(60) Die Verfügbarkeit und zeitnahe Zugänglichkeit dieser Daten für Behörden, einschließlich der nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung oder Verfolgung von Straftaten zuständigen Behörden, CERTs, CSIRTs und – soweit es die Daten ihrer Kunden betrifft – Anbietern elektronischer Kommunikationsnetze und -dienste sowie Anbietern von Cybersicherheitstechnologien und -diensten, die im Namen dieser Kunden tätig sind, ist von wesentlicher Bedeutung, um Missbrauch des Domänennamensystems abzuwenden und zu bekämpfen und insbesondere Cybersicherheitsvorfällen vorzubeugen, sie zu erkennen und zu bewältigen. Dieser Zugang sollte, soweit personenbezogene Daten betroffen sind, mit dem EU-Datenschutzrecht im Einklang stehen.

(61) Zur Gewährleistung der Verfügbarkeit genauer und vollständiger Domänennamen-Registrierungsdaten sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen (sogenannte Registrierstellen), die Integrität und Verfügbarkeit von Domänennamen-Registrierungsdaten erfassen und garantieren. Insbesondere sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, Grundsätze und Verfahren festlegen, um im Einklang mit den EU-Datenschutzvorschriften genaue und vollständige Registrierungsdaten zu erfassen und zu pflegen sowie unrichtige Registrierungsdaten zu verhindern bzw. zu berichtigen.

(62) TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, sollten Domänennamen-Registrierungsdaten, die nicht den EU-Datenschutzvorschriften unterliegen, z. B. Daten, die juristische Personen betreffen[25], öffentlich zugänglich machen. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, sollten es auch ermöglichen, dass berechtigte Zugangsnachfrager rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten natürlicher Personen im Einklang mit dem EU-Datenschutzrecht erhalten. Die Mitgliedstaaten sollten sicherstellen, dass TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, Anträge berechtigter Zugangsnachfrager auf Offenlegung von Domänennamen-Registrierungsdaten unverzüglich beantworten. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, sollten Grundsätze und Verfahren für die Veröffentlichung und Offenlegung von Registrierungsdaten festlegen, einschließlich Leistungsvereinbarungen für die Bearbeitung von Anträgen berechtigter Zugangsnachfrager. Das Zugangsverfahren kann auch die Verwendung einer Schnittstelle, eines Portals oder eines anderen technischen Instruments umfassen, um ein effizientes System für die Anforderung von und den Zugriff auf Registrierungsdaten bereitzustellen. Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses Leitlinien zu solchen Verfahren erlassen.

[25] Erwägungsgrund 14 der VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES: „Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.“

(63) Alle wesentlichen und wichtigen Einrichtungen, die unter diese Richtlinie fallen, sollten der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Dienste erbringen. Erbringt die Einrichtung Dienste in mehreren Mitgliedstaaten, so sollte sie unter die getrennte und parallele gerichtliche Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten zusammenarbeiten, einander Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen.

(64) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Betreibern von Inhaltszustellnetzen, Anbietern von Cloud-Computing-Diensten sowie Anbietern von Rechenzentrumsdiensten und Anbietern digitaler Dienste erbracht werden, grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat für diese Einrichtungen zuständig sein. Die gerichtliche Zuständigkeit sollte bei dem Mitgliedstaat liegen, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob die Netz- und Informationssysteme an einem bestimmten Ort physisch untergebracht sind; die Existenz und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein ausschlaggebendes Kriterium für die Bestimmung der Hauptniederlassung. Die Hauptniederlassung sollte der Ort sein, an dem in der Union über Maßnahmen des Cybersicherheitsrisikomanagements entschieden wird. In der Regel entspricht dies dem Ort, an dem sich die Hauptverwaltung der Unternehmen in der Union befindet. Werden solche Entscheidungen nicht in der Union getroffen, sollte davon ausgegangen werden, dass sich die Hauptniederlassung in dem Mitgliedstaat befindet, in dem die Einrichtung über eine Niederlassung mit der unionsweit höchsten Beschäftigtenzahl verfügt. Werden die Dienste von einer Unternehmensgruppe ausgeführt, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten.

(65) Bieten DNS-Diensteanbieter, TLD-Namenregister, Betreiber von Inhaltszustellnetzen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten oder Anbieter digitaler Dienste, die keine Niederlassung in der Union haben, Dienste in der Union an, so sollten sie einen Vertreter benennen. Um festzustellen, ob eine solche Einrichtung in der Union Dienste anbietet, sollte geprüft werden, ob sie offensichtlich beabsichtigt, Personen in einem oder mehreren Mitgliedstaaten Dienste anzubieten. Die bloße Zugänglichkeit der Website einer Einrichtung oder eines Vermittlers von der Union aus oder einer E-Mail-Adresse oder anderer Kontaktdaten sind zur Feststellung einer solchen Absicht ebenso wenig ausreichend wie die Verwendung einer Sprache, die in dem Drittland, in dem die Einrichtung niedergelassen ist, allgemein gebräuchlich ist. Jedoch können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Dienste in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern in der Union darauf hindeuten, dass die Einrichtung beabsichtigt, in der Union Dienste anzubieten. Der Vertreter sollte im Auftrag der Einrichtung handeln, und es sollte für die zuständigen Behörden oder die CSIRTs möglich sein, mit ihm Kontakt aufzunehmen. Der Vertreter sollte von der Einrichtung ausdrücklich schriftlich beauftragt werden, im Rahmen der sich aus dieser

Richtlinie ergebenden Pflichten der Einrichtung in deren Auftrag zu handeln, was auch die Meldung von Sicherheitsvorfällen einschließt.

(66) Werden nach nationalem Recht oder Unionsrecht als Verschlusssache geltende Informationen gemäß den Bestimmungen dieser Richtlinie ausgetauscht, gemeldet oder auf andere Weise weitergegeben, so sollten die entsprechenden besonderen Vorschriften für den Umgang mit Verschlusssachen angewandt werden.

(67) Da Cyberbedrohungen komplexer und technisch ausgereifter werden, hängen gute Erkennungs- und Präventionsmaßnahmen in hohem Maße von einem regelmäßigen Informationsaustausch zwischen den Einrichtungen über Bedrohungen und Schwachstellen ab. Ein Informationsaustausch trägt dazu bei, das Bewusstsein für Cyberbedrohungen zu schärfen, wodurch die Einrichtungen Bedrohungen abwehren können, bevor sie in reale Sicherheitsvorfälle münden, und in der Lage sind, die Auswirkungen von Sicherheitsvorfällen besser einzudämmen und effizienter zu reagieren. In Ermangelung von Leitlinien auf Unionsebene scheinen mehrere Faktoren einen solchen Wissensaustausch verhindert zu haben, insbesondere die nicht geklärte Vereinbarkeit mit den Wettbewerbs- und Haftungsvorschriften.

(68) Die Einrichtungen sollten ermutigt werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen, abzuwehren und auf sie zu reagieren. Daher muss dafür gesorgt werden, dass auf Unionsebene Mechanismen für Vereinbarungen über den freiwilligen Informationsaustausch entstehen können. Zu diesem Zweck sollten die Mitgliedstaaten auch einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen, aktiv unterstützen und dazu anhalten, sich an solchen Mechanismen zum Informationsaustausch zu beteiligen. Diese Mechanismen sollten unter uneingeschränkter Einhaltung der Wettbewerbsvorschriften und des Datenschutzrechts der Union eingerichtet werden.

(69) Die Verarbeitung personenbezogener Daten durch Einrichtungen, Behörden, CERTs, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten sollte im Sinne der Verordnung (EU) 2016/679 ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellen, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist. Dies sollte auch Folgendes einschließen: Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. Diese Maßnahmen können die Verarbeitung folgender Arten personenbezogener Daten erfordern: IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen.

(70) Zur Stärkung der Aufsichtsbefugnisse und der Maßnahmen, die zu einer wirksamen Befolgung der Vorschriften beitragen, sollte diese Richtlinie einen Mindestumfang an Aufsichtsmaßnahmen und -mitteln vorsehen, mit welchen die zuständigen Behörden wesentliche und wichtige Einrichtungen beaufsichtigen können. Darüber hinaus sollte in dieser Richtlinie eine Abgrenzung zwischen den Aufsichtssystemen für wesentliche und für wichtige Einrichtungen vorgenommen werden, um die Verpflichtungen

sowohl für die Einrichtungen als auch für die zuständigen Behörden ausgewogen zu gestalten. Wesentliche Einrichtungen sollten deshalb einem vollständigen Aufsichtssystem (ex-ante und ex-post) und wichtige Einrichtungen einem vereinfachten Aufsichtssystem (nur ex-post) unterliegen. Im letzteren Fall bedeutet dies, dass wichtige Einrichtungen die Erfüllung der Anforderungen an das Cybersicherheitsrisikomanagement nicht systematisch zu dokumentieren hätten und die zuständigen Behörden ein reaktives Ex-post-Aufsichtskonzept anwenden und nicht generell verpflichtet sein sollten, diese Einrichtungen zu beaufsichtigen.

(71) Für eine wirksame Durchsetzung sollte ein Mindestumfang von Verwaltungssanktionen für Verstöße gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten gemäß dieser Richtlinie festgelegt werden, womit für die gesamte Union ein klarer und kohärenter Rahmen für solche Sanktionen geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, den tatsächlich entstandenen Schäden oder Verlusten bzw. den Schäden oder Verlusten, die hätten entstehen können, der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung der entstandenen Schäden/Verluste, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, dem Umfang der Zusammenarbeit mit der Aufsichtsbehörde sowie jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

(72) Um die wirksame Durchsetzung der in dieser Richtlinie festgelegten Verpflichtungen zu gewährleisten, sollte jede zuständige Behörde befugt sein, Geldbußen aufzuerlegen oder ihre Auferlegung zu beantragen.

(73) Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der geeigneten Bemessung der Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die zuständigen Behörden bereits Geldbußen auferlegt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen verhängen, die in den nationalen Vorschriften zur Umsetzung dieser Richtlinie festgelegt sind.

(74) Die Mitgliedstaaten sollten die strafrechtlichen Sanktionen für Verstöße gegen die nationalen Vorschriften zur Umsetzung dieser Richtlinie festlegen können. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von entsprechenden verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom Gerichtshof ausgelegt worden ist, führen.

(75) Soweit diese Richtlinie verwaltungsrechtliche Sanktionen nicht harmonisiert oder wenn es in anderen Fällen — beispielsweise bei schweren Verstößen gegen die Verpflichtungen aus dieser Richtlinie — erforderlich ist, sollten die Mitgliedstaaten eine Regelung anwenden, die wirksame, verhältnismäßige und abschreckende

Sanktionen vorsieht. Im Recht der Mitgliedstaaten sollte geregelt werden, ob diese Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind.

(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, Sanktionen zu verhängen, die darin bestehen, die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten Dienste auszusetzen und natürlichen Personen die Ausübung von Leitungsaufgaben vorübergehend zu untersagen. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche Sanktionen im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. Solche Sanktionen sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die Sanktionen beziehen, erfüllen. Für die Verhängung solcher Sanktionen muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

(77) Mit dieser Richtlinie sollten Regeln für die Zusammenarbeit zwischen den zuständigen Behörden und den Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 festgelegt werden, um gegen Verstöße im Zusammenhang mit personenbezogenen Daten vorzugehen.

(78) Die Richtlinie sollte darauf abzielen, auf Ebene der Organisationen ein hohes Maß an Verantwortung für die Risikomanagementmaßnahmen und die Meldepflichten im Bereich der Cybersicherheit sicherzustellen. Aus diesen Gründen sollten die Verwaltungsorgane der unter diese Richtlinie fallenden Einrichtungen die Cybersicherheitsrisikomaßnahmen genehmigen und deren Umsetzung überwachen.

(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten benannte Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen.

(80) Um neuen Cyberbedrohungen, technologischen Entwicklungen oder sektorspezifischen Eigenschaften Rechnung zu tragen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte in Bezug auf Elemente zu erlassen, die die in dieser Richtlinie vorgeschriebenen Risikomanagementmaßnahmen betreffen. Der Kommission sollte auch die Befugnis übertragen werden, delegierte Rechtsakte zu erlassen, in denen festgelegt wird, welche Kategorien wesentlicher Einrichtungen ein Zertifikat erlangen müssen und welche spezifischen europäischen Schemata für die Cybersicherheitszertifizierung dabei anzuwenden sind. 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[26] 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.

(81) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung der einschlägigen Bestimmungen dieser Richtlinie in Bezug auf die Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, die technischen Elemente im Zusammenhang mit Risikomanagementmaßnahmen oder die Art der Informationen, das Format und das Verfahren für die Meldung von Sicherheitsvorfällen, sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[27] ausgeübt werden.

(82) Die Kommission sollte diese Richtlinie regelmäßig in Abstimmung mit interessierten Kreisen überprüfen, insbesondere um festzustellen, ob sie veränderten gesellschaftlichen, politischen oder technischen Bedingungen oder veränderten Marktbedingungen anzupassen ist.

(83) Da das Ziel dieser Richtlinie, nämlich die Erreichung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen der Wirkung der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union in Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(84) Diese Richtlinie steht mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang. Diese Richtlinie sollte im Einklang mit diesen Rechten und Grundsätzen umgesetzt werden —

[26] ABl. L 123 vom 12.5.2016, S. 1.

[27] 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).

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand

(1) Mit dieser Richtlinie werden Maßnahmen festgelegt, mit denen in der Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll.

(2) Zu diesem Zweck sieht diese Richtlinie Folgendes vor:

a) die Pflicht für alle Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden und zuständige nationale Behörden, zentrale Anlaufstellen und Reaktionsteams für IT-Sicherheitsvorfälle (Computer Security Incident Response Teams, CSIRTs) zu benennen;

b) für Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Meldepflichten;

c) die Pflicht zum Austausch von Cybersicherheitsinformationen.

Artikel 2

Anwendungsbereich

(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten. Diese Richtlinie gilt nicht für Einrichtungen, die als Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[28] angesehen werden.

(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie jedoch auch für die in den Anhängen I und II genannten Einrichtungen, wenn

a) die Dienste von einer der folgenden Einrichtungen erbracht werden:

i) öffentlichen elektronischen Kommunikationsnetzen oder öffentlich zugänglichen elektronischen Kommunikationsdiensten gemäß Anhang I Nummer 8;

ii) Vertrauensdiensteanbietern gemäß Anhang I Nummer 8;

iii) Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern (DNS-Diensteanbietern) gemäß Anhang I Nummer 8;

[28] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

b) es sich bei der Einrichtung um eine Einrichtung der öffentlichen Verwaltung im Sinne des Artikels 4 Nummer 23 handelt;

c) es sich bei der Einrichtung um den einzigen Anbieter eines Dienstes in einem Mitgliedstaat handelt;

d) sich eine mögliche Störung des von der Einrichtung erbrachten Dienstes auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;

e) eine mögliche Störung des von der Einrichtung erbrachten Dienstes zu Systemrisiken führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

f) es sich aufgrund der besonderen Bedeutung, die die Einrichtung auf regionaler oder nationaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in dem Mitgliedstaat hat, um eine kritische Einrichtung handelt;

g) wenn die Einrichtung als kritische Einrichtung im Sinne der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [Richtlinie über die Resilienz kritischer Einrichtungen][29] oder als einer kritischen Einrichtung gleichgestellte Einrichtung gemäß Artikel 7 der genannten Richtlinie gilt.

Die Mitgliedstaaten erstellen eine Liste der gemäß den Buchstaben b bis f ermittelten Einrichtungen und übermitteln sie der Kommission bis zum [6 Monate nach Ablauf der Umsetzungsfrist]. Danach überprüfen die Mitgliedstaaten die Liste regelmäßig und mindestens alle zwei Jahre und aktualisieren sie gegebenenfalls.

(3) Diese Richtlinie lässt die Zuständigkeiten der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der öffentlichen Sicherheit, der Landesverteidigung und der nationalen Sicherheit im Einklang mit dem Unionsrecht unberührt.

(4) Diese Richtlinie gilt unbeschadet der Richtlinie 2008/114/EG des Rates[30] sowie der Richtlinien 2011/93/EU[31] und 2013/40/EU[32] des Europäischen Parlaments und des Rates.

(5) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf den zum Zweck dieses Informationsaustauschs relevanten und angemessenen Umfang

---

29 *[vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt]*.

30 Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75).

31 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).

32 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).

beschränkt. Beim Informationsaustausch werden die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen wesentlicher oder wichtiger Einrichtungen geschützt.

(6) Wenn wesentliche oder wichtige Einrichtungen gemäß den Bestimmungen sektorspezifischer Rechtsakte der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle und erhebliche Cyberbedrohungen melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen, auch den in Kapitel VI festgelegten Bestimmungen in Bezug auf die Aufsicht und die Durchsetzung, zumindest gleichwertig sind, finden die einschlägigen Bestimmungen dieser Richtlinie keine Anwendung.

Artikel 3

Mindestharmonisierung

Unbeschadet ihrer sonstigen unionsrechtlichen Verpflichtungen können die Mitgliedstaaten im Einklang mit dieser Richtlinie Bestimmungen erlassen oder beibehalten, die ein höheres Cybersicherheitsniveau gewährleisten.

Artikel 4

Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

1. „Netz- und Informationssystem“

   a) ein elektronisches Kommunikationsnetz im Sinne des Artikels 2 Nummer 1 der Richtlinie 2018/1972/EU,

   b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder

   c) digitale Daten, die von den — in den Buchstaben a und b genannten — Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

2. „Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Angriffe abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen;

3. „Cybersicherheit“ die Cybersicherheit im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 2019/881 des Europäischen Parlaments und des Rates[33];

[33] 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

4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen in diesem Mitgliedstaat;

5. „Sicherheitsvorfall“ jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen;

6. „Bewältigung von Sicherheitsvorfällen“ alle Maßnahmen und Verfahren zur Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf;

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

8. „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion einer Anlage, eines Systems, eines Prozesses oder einer Steuerung, die bei einer Cyberbedrohung ausgenutzt werden kann;

9. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag i) eines DNS-Diensteanbieters, eines TLD-Registers, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltszustellnetzen gemäß Anhang I Nummer 8 oder ii) von in Anhang II Nummer 6 aufgeführten nicht in der Union niedergelassenen Einrichtungen zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT – statt an die Einrichtung – hinsichtlich der Pflichten dieser Einrichtung gemäß dieser Richtlinie wenden kann;

10. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[34];

11. „technische Spezifikation“ eine technische Spezifikation im Sinne des Artikels 2 Nummer 4 der Verordnung (EU) Nr. 1025/2012;

12. „Internet-Knoten“ (Internet Exchange Point, IXP) eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr; ein IXP dient nur der Zusammenschaltung autonomer Systeme; ein IXP setzt nicht voraus, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; auch wird der betreffende Datenverkehr weder verändert noch anderweitig beeinträchtigt;

13. „Domänennamensystem (DNS)“ ein verteiltes hierarchisches Verzeichnissystem, das es den Endnutzern ermöglicht, Dienste und Ressourcen im Internet zu erreichen;

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).

[34] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).

14. „DNS-Diensteanbieter“ eine Einrichtung, die Internet-Endnutzern und anderen DNS-Diensteanbietern rekursive oder autoritative Dienste zur Auflösung von Domänennamen anbietet;

15. „Namenregister der Domäne oberster Stufe“ (TLD-Register) eine Einrichtung, der eine bestimmte Domäne oberster Stufe (Top Level Domain – TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, zuständig ist;

16. „digitaler Dienst“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates[35];

17. „Online-Marktplatz“ einen digitalen Dienst im Sinne des Artikels 2 Buchstabe n der Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates[36];

18. „Online-Suchmaschine“ einen digitalen Dienst im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates[37];

19. „Cloud-Computing-Dienst“ einen digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer und verteilter Rechenressourcen ermöglicht;

20. „Rechenzentrumsdienst“ einen Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden;

21. „Inhaltszustellnetz“ bezeichnet ein Netz dezentraler Server zur Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder schnellen Zustellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern;

22. „Plattform für Dienste sozialer Netzwerke“ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;

23. „Einrichtung der öffentlichen Verwaltung“ eine Einrichtung in einem Mitgliedstaat, die die folgenden Kriterien erfüllt:

---

35 Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

36 Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken) (ABl. L 149 vom 11.6.2005, S. 22).

37 Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (ABl. L 186 vom 11.7.2019, S. 57).

a) sie wurde zu dem Zweck gegründet, im allgemeinen Interesse liegende Aufgaben zu erfüllen, und hat keinen gewerblichen oder kommerziellen Charakter,

b) sie besitzt Rechtspersönlichkeit,

c) sie wird überwiegend vom Staat, einer Gebietskörperschaft oder von anderen Körperschaften des öffentlichen Rechts finanziert, oder sie untersteht hinsichtlich ihrer Leitung der Aufsicht dieser Körperschaften, oder sie verfügt über ein Verwaltungs-, Leitungs- bzw. Aufsichtsorgan, das mehrheitlich aus Mitgliedern besteht, die vom Staat, von Gebietskörperschaften oder von anderen Körperschaften des öffentlichen Rechts eingesetzt worden sind,

d) sie ist befugt, an natürliche oder juristische Personen Verwaltungs- oder Regulierungsentscheidungen zu richten, die deren Rechte im grenzüberschreitenden Personen-, Waren-, Dienstleistungs- oder Kapitalverkehr berühren.

Einrichtungen der öffentlichen Verwaltung, die Tätigkeiten in den Bereichen öffentliche Sicherheit, Strafverfolgung, Verteidigung oder nationale Sicherheit ausüben, sind davon ausgeschlossen.

24. „Einrichtung“ jede natürliche Person oder jede nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann;

25. „wesentliche Einrichtung“ jede Einrichtung der in Anhang I als wesentliche Einrichtungen aufgeführten Arten;

26. „wichtige Einrichtung“ jede Einrichtung der in Anhang II als wichtige Einrichtungen aufgeführten Arten.

KAPITEL II

Koordinierte Rechtsrahmen für die Cybersicherheit

Artikel 5
Nationale Cybersicherheitsstrategie

(1) Jeder Mitgliedstaat verabschiedet eine nationale Cybersicherheitsstrategie, in der die strategischen Ziele sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden. Die nationale Cybersicherheitsstrategie muss insbesondere Folgendes umfassen:

a) eine Beschreibung der für die Cybersicherheitsstrategie des jeweiligen Mitgliedstaats festgelegten Ziele und Prioritäten;

b) einen Steuerungsrahmen zur Verwirklichung dieser Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte sowie die Aufgaben und Zuständigkeiten öffentlicher Stellen und Einrichtungen sowie anderer relevanter Akteure umfasst;

c) eine Bewertung zur Ermittlung von relevanten Anlagen und Cybersicherheitsrisiken in diesem Mitgliedstaat;

d) die Bestimmung von Maßnahmen zur Gewährleistung der Vorsorge, Reaktion und Wiederherstellung bei Sicherheitsvorfällen, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;

e) eine Liste der verschiedenen Behörden und Akteure, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind;

f) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [Richtlinie über die Resilienz kritischer Einrichtungen][38] für die Zwecke des Informationsaustauschs über Sicherheitsvorfälle und Cyberbedrohungen und der Wahrnehmung von Aufsichtsaufgaben.

(2) Im Rahmen der nationalen Cybersicherheitsstrategie nehmen die Mitgliedstaaten insbesondere die folgenden Konzepte an:

a) ein Konzept für die Cybersicherheit in der Lieferkette für IKT-Produkte und -Dienste, die von wesentlichen und wichtigen Einrichtungen für die Erbringung ihrer Dienste genutzt werden;

b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge;

c) ein Konzept zur Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen im Sinne des Artikels 6;

d) ein Konzept im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit und Integrität des öffentlichen Kerns des offenen Internets;

e) ein Konzept zur Förderung und Entwicklung von Cybersicherheitskompetenzen, Sensibilisierungsmaßnahmen sowie Forschungs- und Entwicklungsinitiativen;

f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur;

g) ein Konzept, einschlägige Verfahren und geeignete Instrumente für den Informationsaustausch, um den freiwilligen Austausch von Cybersicherheits-Informationen zwischen Unternehmen im Einklang mit dem Unionsrecht zu unterstützen;

h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet.

(3) Die Mitgliedstaaten notifizieren der Kommission ihre nationalen Cybersicherheitsstrategien innerhalb von drei Monaten nach ihrer Verabschiedung. Die Mitgliedstaaten können bestimmte Informationen von der Notifizierung

[38] *[vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt]*.

ausnehmen, wenn und soweit dies zur Wahrung der nationalen Sicherheit unbedingt erforderlich ist.

(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien mindestens alle vier Jahre auf der Grundlage wesentlicher Leistungsindikatoren und ändern diese erforderlichenfalls. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützt die Mitgliedstaaten auf Anfrage bei der Entwicklung einer nationalen Strategie und wesentlicher Leistungsindikatoren für die Bewertung der Strategie.

Artikel 6

Koordinierte Offenlegung von Schwachstellen und europäisches Schwachstellenregister

(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs gemäß Artikel 9 als Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen. Das benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der meldenden Einrichtung und dem Hersteller oder Anbieter von IKT-Produkten oder -Diensten. Betrifft die gemeldete Schwachstelle mehrere Hersteller oder Anbieter von IKT-Produkten oder -Diensten in der Union, so arbeitet das benannte CSIRT jedes betroffenen Mitgliedstaats mit dem CSIRT-Netzwerk zusammen.

(2) Die ENISA entwickelt und pflegt ein europäisches Schwachstellenregister. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen Zugang zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. Das Register muss insbesondere Folgendes umfassen: Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können.

Artikel 7

Nationale Rahmen für das Cybersicherheitskrisenmanagement

(1) Jeder Mitgliedstaat benennt eine oder mehrere für das Management massiver Sicherheitsvorfälle und Krisen zuständige Behörden. Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über angemessene Ressourcen verfügen, um die ihnen übertragenen Aufgaben wirksam und effizient erfüllen zu können.

(2) Jeder Mitgliedstaat ermittelt die Kapazitäten, Mittel und Verfahren, die im Krisenfall für die Zwecke dieser Richtlinie eingesetzt werden können.

(3) Jeder Mitgliedstaat verabschiedet einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen, in dem die Ziele und Modalitäten für das

Management massiver Cybersicherheitsvorfälle und -krisen festgelegt sind. In diesem Plan wird insbesondere Folgendes festgelegt:

a) die Ziele der nationalen Vorsorgenmaßnahmen und -tätigkeiten;

b) die Aufgaben und Zuständigkeiten der nationalen zuständigen Behörden;

c) die Krisenmanagementverfahren und die Kanäle für den Informationsaustausch;

d) die Vorsorgemaßnahmen, einschließlich Übungen und Ausbildungsmaßnahmen;

e) die einschlägigen öffentlichen und privaten interessierten Kreise sowie die beteiligten Infrastrukturen;

f) die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich der Mitgliedstaat wirksam am koordinierten Management massiver Cybersicherheitsvorfälle und -krisen auf Unionsebene beteiligen und dieses unterstützen kann.

(4) Die Mitgliedstaaten teilen der Kommission ihre gemäß Absatz 1 benannten zuständigen Behörden innerhalb von drei Monaten nach der Benennung mit und übermitteln ihre nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen gemäß Absatz 3 innerhalb von drei Monaten nach der Verabschiedung dieser Pläne. Die Mitgliedstaaten können bestimmte Informationen von ihrem Plan ausnehmen, wenn und soweit dies für ihre nationale Sicherheit unbedingt erforderlich ist.

Artikel 8

Nationale zuständige Behörden und zentrale Anlaufstellen

(1) Jeder Mitgliedstaat benennt eine oder mehrere für die Cybersicherheit und die in Kapitel VI dieser Richtlinie genannten Aufsichtsaufgaben zuständige Behörden. Die Mitgliedstaaten können dafür eine oder mehrere bereits bestehende Behörden benennen.

(2) Die zuständigen Behörden gemäß Absatz 1 überwachen die Anwendung dieser Richtlinie auf nationaler Ebene.

(3) Jeder Mitgliedstaat benennt eine für die Cybersicherheit zuständige nationale zentrale Anlaufstelle (im Folgenden „zentrale Anlaufstelle“). Benennt ein Mitgliedstaat nur eine zuständige Behörde, so ist diese zuständige Behörde auch die zentrale Anlaufstelle dieses Mitgliedstaats.

(4) Jede zentrale Anlaufstelle fungiert als Verbindungsstelle, um die grenzüberschreitende Zusammenarbeit der Behörden des Mitgliedstaats mit den entsprechenden Behörden in anderen Mitgliedstaaten sowie die sektorübergreifende Zusammenarbeit mit anderen nationalen zuständigen Behörden innerhalb des Mitgliedstaats zu gewährleisten.

(5) Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden gemäß Absatz 1 und die zentralen Anlaufstellen mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient erfüllen können und die Ziele dieser Richtlinie somit erreicht werden können. Die Mitgliedstaaten

stellen eine wirksame, effiziente und sichere Zusammenarbeit der benannten Vertreter in der Kooperationsgruppe gemäß Artikel 12 sicher.

(6) Die Mitgliedstaaten notifizieren der Kommission unverzüglich die Benennung der zuständigen Behörde gemäß Absatz 1 und der zentralen Anlaufstelle gemäß Absatz 3, deren Aufgaben sowie etwaige spätere Änderungen dieser Angaben. Jeder Mitgliedstaat gibt seine Benennungen öffentlich bekannt. Die Kommission veröffentlicht die Liste der benannten zentralen Anlaufstellen.

Artikel 9

Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs)

(1) Jeder Mitgliedstaat benennt ein oder mehrere CSIRTs, die die in Artikel 10 Absatz 1 festgelegten Anforderungen erfüllen, mindestens die in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen abdecken und für die Bewältigung von Sicherheitsvorfällen nach einem genau festgelegten Ablauf zuständig sind. Ein CSIRT kann innerhalb einer zuständigen Behörde gemäß Artikel 8 eingerichtet werden.

(2) Die Mitgliedstaaten gewährleisten, dass jedes CSIRT mit angemessenen Ressourcen ausgestattet ist, damit es seine in Artikel 10 Absatz 2 aufgeführten Aufgaben wirksam erfüllen kann.

(3) Die Mitgliedstaaten stellen sicher, dass jedes CSIRT über eine geeignete, sichere und belastbare Kommunikations- und Informationsinfrastruktur für den Austausch von Informationen mit wesentlichen und wichtigen Einrichtungen und anderen einschlägigen interessierten Kreisen verfügt. Zu diesem Zweck stellen die Mitgliedstaaten sicher, dass die CSIRTs zur Einführung sicherer Instrumente für den Informationsaustausch beitragen.

(4) Die CSIRTs arbeiten mit vertrauenswürdigen sektorspezifischen oder sektorübergreifenden Gruppierungen wesentlicher und wichtiger Einrichtungen zusammen und tauschen mit diesen gemäß Artikel 26 gegebenenfalls einschlägige Informationen aus.

(5) Die CSIRTs nehmen an gemäß Artikel 16 organisierten Peer Reviews teil.

(6) Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs in dem in Artikel 13 genannten CSIRT-Netzwerk wirksam, effizient und sicher zusammenarbeiten.

(7) Die Mitgliedstaaten teilen der Kommission unverzüglich die gemäß Absatz 1 benannten CSIRTs, das gemäß Artikel 6 Absatz 1 als Koordinator benannte CSIRT und deren jeweilige in Bezug auf die in den Anhängen I und II genannten Einrichtungen vorgesehenen Aufgaben mit.

(8) Die Mitgliedstaaten können die ENISA um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.

Artikel 10

Anforderungen an die CSIRTs und Aufgaben der CSIRTs

(1) Die CSIRTs müssen den folgenden Anforderungen genügen:

a) Die CSIRTs sorgen für einen hohen Grad der Verfügbarkeit ihrer Kommunikationsdienste, indem sie punktuellen Ausfällen vorbeugen und mehrere Kanäle bereitstellen, damit sie jederzeit erreichbar bleiben und selbst mit anderen Kontakt aufnehmen können. Die CSIRTs legen die Kommunikationskanäle genau fest und machen sie den CSIRT-Nutzern und Kooperationspartnern bekannt;

b) Die Räumlichkeiten der CSIRTs und die unterstützenden Informationssysteme werden an sicheren Standorten eingerichtet;

c) Die CSIRTs müssen über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügen, insbesondere, um wirksame und effiziente Übergaben zu erleichtern;

d) Die CSIRTs müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft gewährleisten können;

e) Die CSIRTs müssen über Redundanzsysteme und Ausweicharbeitsräume verfügen, um die Kontinuität ihrer Dienste zu sicherzustellen;

f) Die CSIRTs müssen die Möglichkeit haben, sich an internationalen Kooperationsnetzen zu beteiligen.

(2) Die CSIRTs haben folgende Aufgaben:

a) Überwachung von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen auf nationaler Ebene;

b) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wesentlichen und wichtigen Einrichtungen sowie andere interessierte Kreise;

c) Reaktion auf Sicherheitsvorfälle;

d) dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Cybersicherheit;

e) auf Ersuchen einer Einrichtung Durchführung einer proaktiven Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen (Schwachstellenscan);

f) Beteiligung am CSIRT-Netzwerk und auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des Netzwerks auf deren Ersuchen.

(3) Die CSIRTs bauen Kooperationsbeziehungen mit einschlägigen Akteuren des Privatsektors auf, um die Ziele der Richtlinie besser erreichen zu können.

(4) Zur Erleichterung der Zusammenarbeit fördern die CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für Klassifizierungssysteme und Taxonomien für

a) Verfahren zur Bewältigung von Sicherheitsvorfällen,

b) das Cybersicherheitskrisenmanagement,

c) die koordinierte Offenlegung von Schwachstellen.

Artikel 11

Zusammenarbeit auf nationaler Ebene

(1) Handelt es sich bei den zuständigen Behörden gemäß Artikel 8, der zentralen Anlaufstelle und dem/den CSIRT(s) eines Mitgliedstaats um getrennte Einrichtungen, so arbeiten sie bei der Erfüllung der in dieser Richtlinie festgelegten Pflichten zusammen.

(2) Die Mitgliedstaaten stellen sicher, dass Meldungen von Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen gemäß dieser Richtlinie entweder ihren zuständigen Behörden oder ihren CSIRTs übermittelt werden. Entscheidet ein Mitgliedstaat, dass diese Meldungen nicht an seine CSIRTs zu richten sind, so wird den CSIRTs in dem zur Wahrnehmung ihrer Aufgaben erforderlichen Umfang Zugang zu den Daten über Sicherheitsvorfälle gewährt, die gemäß Artikel 20 von wesentlichen oder wichtigen Einrichtungen gemeldet werden.

(3) Jeder Mitgliedstaat stellt sicher, dass seine zuständigen Behörden oder CSIRTs seine zentrale Anlaufstelle über gemäß dieser Richtlinie vorgenommene Meldungen von Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen unterrichten.

(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung][39] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden.

(5) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden regelmäßig über Cybersicherheitsrisiken, Cyberbedrohungen und Sicherheitsvorfälle unterrichten, die als kritische Einrichtungen oder kritischen Einrichtungen gleichgestellte Einrichtungen gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] ermittelte wesentliche Einrichtungen betreffen, sowie über die von den zuständigen Behörden als Reaktion auf diese Risiken und Sicherheitsvorfälle ergriffenen Maßnahmen.

[39] *[vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt]*.

KAPITEL III

Zusammenarbeit

Artikel 12
Kooperationsgruppe

(1) Zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten bei der Anwendung der Richtlinie wird eine Kooperationsgruppe eingesetzt.

(2) Die Kooperationsgruppe nimmt ihre Aufgaben auf der Grundlage von zweijährlichen Arbeitsprogrammen gemäß Absatz 6 wahr.

(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Der Europäische Auswärtige Dienst nimmt an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) können sich gemäß Artikel 17 Absatz 5 Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe beteiligen.

Gegebenenfalls kann die Kooperationsgruppe Vertreter der maßgeblichen Interessenträger einladen, an ihren Arbeiten teilzunehmen.

Die Sekretariatsgeschäfte werden von der Kommission geführt.

(4) Die Kooperationsgruppe hat folgende Aufgaben:

a) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Umsetzung und Durchführung dieser Richtlinie;

b) Austausch bewährter Verfahren und Informationsaustausch im Zusammenhang mit der Umsetzung dieser Richtlinie, auch in Bezug auf Cyberbedrohungen, Sicherheitsvorfälle, Schwachstellen, Beinahe-Vorfälle, Sensibilisierungsinitiativen, Schulungen, Übungen und Kompetenzen, Kapazitätsaufbau sowie Normen und technische Spezifikationen;

c) beratender Austausch und Zusammenarbeit mit der Kommission in Bezug auf neue politische Initiativen im Bereich der Cybersicherheit;

d) beratender Austausch und Zusammenarbeit mit der Kommission bei Entwürfen von Durchführungsrechtsakten oder delegierten Rechtsakten der Kommission, die gemäß dieser Richtlinie erlassen werden;

e) Austausch bewährter Verfahren und Informationsaustausch mit den einschlägigen Organen, Einrichtungen, Ämtern und Agenturen der Union;

f) Erörterung von Berichten über die in Artikel 16 Absatz 7 genannten Peer Reviews;

g) Erörterung von Ergebnissen der gemeinsamen Aufsichtstätigkeiten in grenzübergreifenden Fällen gemäß Artikel 34;

h) Bereitstellung strategischer Orientierungshilfen für das CSIRT-Netzwerk zu spezifischen neu auftretenden Fragen;

i) Beitrag zu den Cybersicherheitsfähigkeiten in der gesamten Union durch Erleichterung des Austauschs nationaler Bediensteter im Rahmen eines Programms zum Kapazitätsaufbau, an dem sich Mitarbeiter der zuständigen Behörden oder der CSIRTs der Mitgliedstaaten beteiligen;

j) Organisation regelmäßiger gemeinsamer Sitzungen mit einschlägigen interessierten Kreisen des Privatsektors aus der gesamten Union, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen;

k) Erörterung der Arbeiten im Zusammenhang mit Cybersicherheitsübungen, einschließlich der Arbeit der ENISA.

(5) Die Kooperationsgruppe kann das CSIRT-Netzwerk um einen technischen Bericht zu ausgewählten Themen ersuchen.

(6) Die Kooperationsgruppe erstellt bis zum … [24 Monate nach Inkrafttreten dieser Richtlinie] und danach alle zwei Jahre ein Arbeitsprogramm mit den zur Umsetzung ihrer Ziele und Aufgaben zu ergreifenden Maßnahmen. Der Zeitrahmen des ersten gemäß dieser Richtlinie angenommenen Programms wird an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 angenommenen Programms angepasst.

(7) Die Kommission kann Durchführungsrechtsakte zur Festlegung der Verfahrensmodalitäten erlassen, die für das Funktionieren der Kooperationsgruppe erforderlich sind. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

(8) Die Kooperationsgruppe tagt regelmäßig, mindestens aber einmal jährlich gemeinsam mit der mit der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit und den Informationsaustausch zu fördern.

Artikel 13
CSIRT-Netzwerk

(1) Um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zwischen ihnen zu fördern, wird ein Netzwerk der nationalen CSIRTs errichtet.

(2) Das CSIRT-Netzwerk setzt sich aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU zusammen. Die Kommission nimmt als Beobachterin am CSIRT-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs.

(3) Das CSIRT-Netzwerk hat folgende Aufgaben:

a) Informationsaustausch zu den Kapazitäten der CSIRTs;

b) Austausch relevanter Informationen über Sicherheitsvorfälle, Beinahe-Vorfälle, Cyberbedrohungen, Risiken und Schwachstellen;

c) auf Antrag eines potenziell von einem Sicherheitsvorfall betroffenen Vertreters des CSIRT-Netzwerkes Austausch und Erörterung von Informationen über

diesen Sicherheitsvorfall und die damit verbundenen Cyberbedrohungen, Risiken und Schwachstellen;

d) auf Antrag eines Vertreters des CSIRT-Netzwerkes Erörterung und, sofern möglich, Umsetzung einer koordinierten Reaktion auf einen Sicherheitsvorfall, der im Gebiet seines Mitgliedstaats festgestellt wurde;

e) Unterstützung der Mitgliedstaaten bei der Bewältigung grenzübergreifender Sicherheitsvorfälle gemäß dieser Richtlinie;

f) Zusammenarbeit mit und Unterstützung von gemäß Artikel 6 benannten CSIRTs im Hinblick auf das Vorgehen bei einer mehrseitigen koordinierten Offenlegung von Schwachstellen, von denen mehrere in verschiedenen Mitgliedstaaten niedergelassene Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen betroffen sind;

g) Erörterung und Bestimmung weiterer Formen der operativen Zusammenarbeit, unter anderem im Zusammenhang mit

   i) Kategorien von Cyberbedrohungen und Sicherheitsvorfällen,

   ii) Frühwarnungen,

   iii) gegenseitiger Unterstützung,

   iv) Grundsätzen und Modalitäten der Koordinierung bei der Reaktion auf grenzüberschreitende Risiken und Sicherheitsvorfälle,

   v) dem Beitrag zum nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen gemäß Artikel 7 Absatz 3;

h) Unterrichtung der Kooperationsgruppe über seine Tätigkeiten und über die gemäß Buchstabe g erörterten weiteren Formen der operativen Zusammenarbeit und gegebenenfalls Ersuchen um Orientierungshilfen dafür;

i) Berücksichtigung von Erkenntnissen aus Cybersicherheitsübungen, einschließlich der von der ENISA organisierten Übungen;

j) auf Antrag eines einzelnen CSIRT Erörterung der Kapazitäten und der Vorsorge dieses CSIRT;

k) Zusammenarbeit und Informationsaustausch mit regionalen und unionsweiten Sicherheitseinsatzzentren, um die gemeinsame Lageerfassung bei Sicherheitsvorfällen und Bedrohungen in der gesamten Union zu verbessern;

l) Erörterung der in Artikel 16 Absatz 7 genannten Peer Reviews;

m) Erstellung von Leitlinien zur Erleichterung der Konvergenz der operativen Verfahrensweisen in Bezug auf die Anwendung der die operative Zusammenarbeit betreffenden Bestimmungen dieses Artikels.

(4) Für die Zwecke der Überprüfung gemäß Artikel 35 bewertet das CSIRT-Netzwerk bis zum [24 Monate nach Inkrafttreten dieser Richtlinie] und danach alle zwei Jahre die Fortschritte bei der operativen Zusammenarbeit und erstellt einen Bericht. Der Bericht muss insbesondere Schlussfolgerungen zu den Ergebnissen der Peer Reviews gemäß Artikel 16 enthalten, die in Bezug auf nationale CSIRTs durchgeführt wurden, einschließlich der Schlussfolgerungen und Empfehlungen gemäß dem genannten Artikel. Dieser Bericht wird auch der Kooperationsgruppe übermittelt.

(5) Das CSIRT-Netzwerk gibt sich eine Geschäftsordnung.

Artikel 14

Das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe)

(1) Zur Unterstützung des koordinierten Managements massiver Cybersicherheitsvorfälle und -krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Informationsaustauschs zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Agenturen der Union wird hiermit das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network, EU-CyCLONe) eingerichtet.

(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen Behörden der Mitgliedstaaten, der Kommission und der ENISA zusammen. ENISA führt die Sekretariatsgeschäfte des Netzwerks und unterstützt den sicheren Informationsaustausch.

(3) EU-CyCLONe hat folgende Aufgaben:

a) Verbesserung der Vorsorge im Hinblick auf das Management massiver Sicherheitsvorfälle und Krisen;

b) Entwicklung einer gemeinsamen Lageerfassung für relevante Cybersicherheitsereignisse;

c) Koordinierung des Managements massiver Sicherheitsvorfälle und Krisen sowie Unterstützung der Entscheidungsfindung auf politischer Ebene in Bezug auf solche Sicherheitsvorfälle und Krisen;

d) Erörterung des nationalen Plans für die Reaktion auf Cybersicherheitsvorfälle gemäß Artikel 7 Absatz 2.

(4) EU-CyCLONe gibt sich eine Geschäftsordnung.

(5) EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über Cyberbedrohungen, Sicherheitsvorfälle und Trends, wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche und wichtige Einrichtungen liegt.

(6) EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten mit dem CSIRT-Netzwerk zusammen.

Artikel 15

Bericht über den Stand der Cybersicherheit in der Union

(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen zweijährlichen Bericht über den Stand der Cybersicherheit in der Union. Dieser Bericht muss insbesondere Folgendes enthalten:

a) eine Bewertung der Entwicklung von Cybersicherheitskapazitäten in der gesamten Union;

b) eine Bewertung der den zuständigen Behörden und für Cybersicherheitskonzepte zur Verfügung stehenden technischen, finanziellen

und personellen Ressourcen sowie der Durchführung von Aufsichts- und Durchsetzungsmaßnahmen unter Berücksichtigung der Ergebnisse der Peer Reviews gemäß Artikel 16;

c) einen Cybersicherheitsindex für eine aggregierte Bewertung des Entwicklungsstands der Cybersicherheitskapazitäten.

(2) Der Bericht muss insbesondere politische Empfehlungen zur Erhöhung des Cybersicherheitsniveaus in der gesamten Union und eine Zusammenfassung der Ergebnisse der von der ENISA gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 für den entsprechenden Zeitraum erstellten technischen EU-Cybersicherheitslageberichte umfassen.

Artikel 16

Peer Reviews

(1) Nach Konsultation der Kooperationsgruppe und der ENISA legt die Kommission spätestens 18 Monate nach Inkrafttreten dieser Richtlinie die Methode und den Inhalt eines Peer-Review-Systems zur Bewertung der Wirksamkeit der Cybersicherheitskonzepte der Mitgliedstaaten fest. Die Peer Reviews werden von technischen Sachverständigen für Cybersicherheit aus anderen als den überprüften Mitgliedstaaten durchgeführt und erstrecken sich mindestens auf Folgendes:

i) die Wirksamkeit der Umsetzung der Anforderungen an das Cybersicherheitsrisikomanagement und der Meldepflichten gemäß den Artikeln 18 und 20;

ii) das Niveau der Kapazitäten, einschließlich der verfügbaren finanziellen, technischen und personellen Ressourcen, und die Wirksamkeit bei der Durchführung der Aufgaben der zuständigen nationalen Behörden;

iii) die operativen Kapazitäten und die Wirksamkeit der CSIRTs;

iv) die Wirksamkeit der Amtshilfe gemäß Artikel 34;

v) die Wirksamkeit des in Artikel 26 dieser Richtlinie genannten Rahmens für den Informationsaustausch.

(2) Die Methode muss objektive, nichtdiskriminierende, faire und transparente Kriterien umfassen, anhand deren die Mitgliedstaaten Sachverständige benennen, die für die Durchführung der Peer Reviews infrage kommen. Die ENISA und die Kommission benennen Sachverständige, die als Beobachter an den Peer Reviews teilnehmen. Die Kommission legt mit Unterstützung der ENISA im Rahmen der in Absatz 1 genannten Methode für jede Peer Review ein objektives, nichtdiskriminierendes, faires und transparentes System für die Auswahl und die Zufallszuweisung von Sachverständigen fest.

(3) Die organisatorischen Aspekte der Peer Reviews werden von der Kommission mit Unterstützung der ENISA beschlossen und beruhen nach Konsultation der Kooperationsgruppe auf Kriterien, die in der in Absatz 1 genannten Methode festgelegt sind. Bei den Peer Reviews werden für alle Mitgliedstaaten und Sektoren die in Absatz 1 genannten Aspekte bewertet, einschließlich gezielter Fragen, die speziell einen oder mehrere Mitgliedstaaten oder einen oder mehrere Sektoren betreffen.

(4) Die Peer Reviews müssen tatsächliche oder virtuelle Besuche am Standort und Möglichkeiten zum Austausch außerhalb des Standorts umfassen. In Anbetracht des Grundsatzes der guten Zusammenarbeit stellen die überprüften Mitgliedstaaten den benannten Sachverständigen die für die Bewertung der überprüften Aspekte erforderlichen Informationen zur Verfügung. Sämtliche durch das Peer-Review-Verfahren erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die an der Peer Review beteiligten Sachverständigen geben keine sensiblen oder vertraulichen Informationen, die im Laufe der Peer Review erlangt wurden, an Dritte weiter.

(5) Nach Abschluss einer Peer Review in einem Mitgliedstaat dürfen in den beiden Jahren danach in diesem Mitgliedstaat keine weiteren Peer Reviews zu denselben Aspekten durchgeführt werden, es sei denn, die Kommission beschließt nach Konsultation der ENISA und der Kooperationsgruppe etwas anderes.

(6) Die Mitgliedstaaten stellen sicher, dass jegliches Risiko eines Interessenkonflikts im Zusammenhang mit den benannten Sachverständigen den anderen Mitgliedstaaten, der Kommission und der ENISA unverzüglich offengelegt wird.

(7) Die an Peer Reviews beteiligten Sachverständigen erstellen Berichte über die Ergebnisse und Schlussfolgerungen der Peer Reviews. Die Berichte werden der Kommission, der Kooperationsgruppe, dem CSIRT-Netzwerk und der ENISA vorgelegt. Sie werden in der Kooperationsgruppe und im CSIRT-Netzwerk erörtert. Die Berichte können auf der speziellen Website der Kooperationsgruppe veröffentlicht werden.

KAPITEL IV

Risikomanagement und Meldepflichten im Bereich Cybersicherheit

ABSCHNITT I

Risikomanagement und Meldungen im Bereich Cybersicherheit

Artikel 17

Governance

(1) Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 18 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung beaufsichtigen und für die Nichteinhaltung der Verpflichtungen nach diesem Artikel durch die betreffenden Einrichtungen rechenschaftspflichtig sind.

(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane regelmäßig an spezifischen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf den Betrieb der Einrichtung zu erwerben.

Artikel 18

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen bei der Erbringung ihrer Dienste nutzen, zu beherrschen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

(2) Die in Absatz 1 genannten Maßnahmen müssen zumindest Folgendes umfassen:

a) Risikoanalyse- und Sicherheitskonzepte für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen (Prävention und Erkennung von Sicherheitsvorfällen und Reaktion auf Sicherheitsvorfälle);

c) Aufrechterhaltung des Betriebs und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren Anbietern oder Diensteanbietern beispielsweise Anbietern von Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten (MSS);

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren (Erprobung und Prüfung) zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) Einsatz von Kryptografie und Verschlüsselung.

(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.

(4) Die Mitgliedstaaten stellen sicher, dass Einrichtungen, die feststellen, dass ihre Dienste oder Aufgaben die Anforderungen nach Absatz 2 nicht erfüllen, unverzüglich alle erforderlichen Korrekturmaßnahmen ergreifen, um den betreffenden Dienst mit den Anforderungen in Einklang zu bringen.

(5) Die Kommission kann Durchführungsrechtsakte erlassen, um die technischen und methodischen Spezifikationen für die in Absatz 2 genannten Elemente festzulegen. Bei der Ausarbeitung dieser Rechtsakte verfährt die Kommission nach dem Prüfverfahren gemäß Artikel 37 Absatz 2 und beachtet dabei so weit wie möglich internationale und europäische Normen sowie die einschlägigen technischen Spezifikationen.

(6) Der Kommission wird die Befugnis übertragen, zur Ergänzung der in Absatz 2 genannten Elemente delegierte Rechtsakte gemäß Artikel 36 zu erlassen, um neuen

Cyberbedrohungen, technologischen Entwicklungen oder sektorspezifischen Besonderheiten Rechnung zu tragen.

Artikel 19

EU-weit koordinierte Risikobewertungen kritischer Lieferketten

(1) Die Kooperationsgruppe kann in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durchführen.

(2) Die Kommission legt nach Konsultation der Kooperationsgruppe und der ENISA fest, welche spezifischen kritischen IKT-Dienste, -Systeme oder -Produkte der koordinierten Risikobewertung nach Absatz 1 unterzogen werden können.

Artikel 20

Meldepflichten

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich jeden Sicherheitsvorfall melden, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat. Gegebenenfalls unterrichten diese Einrichtungen die Empfänger ihrer Dienste unverzüglich über Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es den zuständigen Behörden oder dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.

(2) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT unverzüglich jede von diesen Einrichtungen ermittelte erhebliche Cyberbedrohung melden, die nach deren Auffassung möglicherweise zu einem erheblichen Sicherheitsvorfall hätte führen können.

Gegebenenfalls unterrichten diese Einrichtungen die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger ihrer Dienste unverzüglich über alle Maßnahmen oder Abhilfemaßnahmen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger gegebenenfalls auch über die Bedrohung selbst. Mit der Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.

(3) Ein Sicherheitsvorfall gilt als erheblich, wenn

a) der Sicherheitsvorfall erhebliche Betriebsstörungen oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder potenziell verursachen könnte;

b) der Sicherheitsvorfall andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt hat oder potenziell schädigen könnte.

(4) Die Mitgliedstaaten stellen sicher, dass die betreffenden Einrichtungen den zuständigen Behörden oder dem CSIRT für die Zwecke der Meldung nach Absatz 1 Folgendes übermitteln:

a) unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des Sicherheitsvorfalls, eine erste Meldung, in der gegebenenfalls angegeben wird, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist;

b) auf Ersuchen einer zuständigen Behörde oder eines CSIRT einen Zwischenbericht über relevante Statusaktualisierungen;

c) spätestens einen Monat nach Vorlage des Berichts gemäß Buchstabe a einen Abschlussbericht, der mindestens Folgendes enthält:

i) eine ausführliche Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen;

ii) Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat;

iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.

Die Mitgliedstaaten sehen vor, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von den unter den Buchstaben a und c festgelegten Fristen abweichen kann.

(5) Die zuständigen nationalen Behörden oder das CSIRT übermitteln der meldenden Einrichtung innerhalb von 24 Stunden nach Eingang der ersten Meldung gemäß Absatz 4 Buchstabe a eine Antwort, einschließlich einer ersten Rückmeldung zu dem Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen für die Durchführung möglicher Abhilfemaßnahmen. Wurde die in Absatz 1 genannte Meldung nicht dem CSIRT übermittelt, werden die Orientierungshilfen von der zuständigen Behörde in Zusammenarbeit mit dem CSIRT bereitgestellt. Das CSIRT leistet auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung. Wird bei dem Sicherheitsvorfall ein krimineller Hintergrund vermutet, geben die zuständigen nationalen Behörden oder das CSIRT ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

(6) Gegebenenfalls und insbesondere, wenn der in Absatz 1 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten und die ENISA über den Sicherheitsvorfall. Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.

(7) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen Sicherheitsvorfall zu verhindern oder einen laufenden Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so können die zuständige Behörde oder das CSIRT sowie gegebenenfalls die Behörden oder die CSIRTs anderer betroffener Mitgliedstaaten nach Konsultation der betroffenen Einrichtung die Öffentlichkeit über den Sicherheitsvorfall informieren oder die Einrichtung auffordern, dies zu tun.

(8) Auf Ersuchen der zuständigen Behörde oder des CSIRT leitet die zentrale Anlaufstelle die nach den Absätzen 1 und 2 eingegangenen Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.

(9) Die zentrale Anlaufstelle legt der ENISA monatlich einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß den Absätzen 1 und 2 und gemäß Artikel 27 gemeldet wurden. Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die ENISA technische Leitlinien zu den Parametern der in den zusammenfassenden Bericht aufzunehmenden Angaben herausgeben.

(10) Die zuständigen Behörden stellen den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden Informationen über Sicherheitsvorfälle und Cyberbedrohungen zur Verfügung, die nach den Absätzen 1 und 2 von wesentlichen Einrichtungen, die im Sinne der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als kritischen Einrichtungen gleichwertige Einrichtungen gelten, gemeldet wurden.

(11) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß den Absätzen 1 und 2 näher bestimmt werden. Die Kommission kann ferner Durchführungsrechtsakte erlassen, um genauer zu bestimmen, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne des Absatzes 3 anzusehen ist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 21

Nutzung der europäischen Systeme für die Cybersicherheitszertifizierung

(1) Die Mitgliedstaaten können wesentliche und wichtige Einrichtungen dazu verpflichten, bestimmte IKT-Produkte, -Dienste und -Prozesse im Rahmen spezifischer europäischer Systeme für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifizieren zu lassen, um die Erfüllung bestimmter in Artikel 18 genannter Anforderungen nachzuweisen. Die zu zertifizierenden Produkte, Dienstleistungen und Prozesse können von einer wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft worden sein.

(2) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte zu erlassen, in denen ausgeführt wird, welche Kategorien wesentlicher Einrichtungen ein Zertifikat erlangen müssen und welche spezifischen europäischen Systeme für die Cybersicherheitszertifizierung dabei nach Absatz 1 anzuwenden sind. Die delegierten Rechtsakte werden gemäß Artikel 36 erlassen.

(3) Ist kein geeignetes europäisches System für die Cybersicherheitszertifizierung für die Zwecke des Absatzes 2 vorhanden, kann die Kommission die ENISA auffordern, ein vorläufiges System gemäß Artikel 48 Absatz 2 der Verordnung (EU) 2019/881 auszuarbeiten.

Artikel 22

Normung

(1) Um die einheitliche Anwendung des Artikels 18 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

(2) In Zusammenarbeit mit den Mitgliedstaaten bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen — einschließlich der nationalen Normen der Mitgliedstaaten —, mit denen diese Bereiche abgedeckt werden könnten.

Artikel 23

Datenbanken der Domänennamen und Registrierungsdaten

(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, stellen die Mitgliedstaaten sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank sammeln und pflegen, wobei die Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt zu beachten sind.

(2) Die Mitgliedstaaten stellen sicher, dass die Datenbanken zu den in Absatz 1 genannten Domänennamen-Registrierungsdaten einschlägige Angaben enthalten, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.

(3) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird, dass die Datenbanken genaue und vollständige Angaben enthalten. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.

(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, unverzüglich nach der Registrierung eines Domänennamens die nicht personenbezogenen Domänenregistrierungsdaten veröffentlichen.

(5) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auf rechtmäßige und hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, alle Anträge auf Zugang unverzüglich beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

Abschnitt II

Gerichtliche Zuständigkeit und Registrierung

Artikel 24

Gerichtliche Zuständigkeit und Territorialität

(1) Es gilt, dass DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten und Betreiber von Inhaltszustellnetzen gemäß Anhang I Nummer 8 sowie Anbieter digitaler Dienste gemäß Anhang II Nummer 6 der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Hauptniederlassung in der Union haben.

(2) Für die Zwecke dieser Richtlinie wird davon ausgegangen, dass als Hauptniederlassung in der Union der in Absatz 1 genannten Einrichtungen jeweils die Niederlassung in demjenigen Mitgliedstaat gilt, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement getroffen werden. Werden solche Entscheidungen in keiner Niederlassung in der Union getroffen, wird davon ausgegangen, dass sich die Hauptniederlassung der Einrichtung in dem Mitgliedstaat befindet, in dem die Niederlassung mit der höchsten Beschäftigtenzahl in der Union angesiedelt ist.

(3) Hat eine in Absatz 1 genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienstleistungen innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es gilt, dass solche Einrichtungen der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen Nichteinhaltung der Verpflichtungen nach dieser Richtlinie einleiten.

(4) Die Benennung eines Vertreters durch eine in Absatz 1 genannte Einrichtung lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

Artikel 25

Register wesentlicher und wichtiger Einrichtungen

(1) Die ENISA erstellt und pflegt ein Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1. Die Einrichtungen übermitteln der ENISA spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie] folgende Angaben:

a) Name der Einrichtung,

b) Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Union oder, falls sie nicht in der Union niedergelassen ist, Anschrift ihres nach Artikel 24 Absatz 3 benannten Vertreters;

c) aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtungen.

(2) Im Falle einer Änderung der gemäß Absatz 1 übermittelten Angaben unterrichten die in Absatz 1 genannten Einrichtungen die ENISA unverzüglich über diese Änderung, in jedem Fall aber innerhalb von drei Monaten nach Wirksamwerden der Änderung.

(3) Nach Eingang der Angaben gemäß Absatz 1 leitet die ENISA diese an die zentralen Anlaufstellen des angegebenen Ortes der Hauptniederlassung der jeweiligen Einrichtung weiter bzw., falls sie nicht in der Union niedergelassen ist, an die zentralen Anlaufstellen am Ort der Niederlassung ihres benannten Vertreters. Hat eine in Absatz 1 genannte Einrichtung neben ihrer Hauptniederlassung in der Union weitere Niederlassungen in anderen Mitgliedstaaten, unterrichtet die ENISA auch die zentralen Anlaufstellen dieser Mitgliedstaaten.

(4) Unterlässt es eine Einrichtung, innerhalb der in Absatz 1 genannten Frist ihre Tätigkeit zu registrieren oder die einschlägigen Angaben vorzulegen, ist jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, befugt sicherzustellen, dass die Einrichtung die in dieser Richtlinie festgelegten Verpflichtungen erfüllt.

KAPITEL V

Informationsaustausch

Artikel 26

Vereinbarungen über den Austausch von Informationen zur Cybersicherheit

(1) Unbeschadet der Verordnung (EU) 2016/679 stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, Schwachstellen, Gefährdungsindikatoren (indicators of compromise – IoC), Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, sofern

a) dieser Informationsaustausch darauf abzielt, Sicherheitsvorfälle zu verhindern, aufzudecken, zu bewältigen oder ihre Folgen einzudämmen;

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

(2) Die Mitgliedstaaten stellen sicher, dass der Informationsaustausch innerhalb vertrauenswürdiger Gemeinschaften wesentlicher und wichtiger Einrichtungen stattfindet. Dieser Austausch muss im Wege von Vereinbarungen über den Informationsaustausch unter Beachtung des potenziell sensiblen Charakters der ausgetauschten Informationen und im Einklang mit den in Absatz 1 genannten Vorschriften des Unionsrechts erfolgen.

(3) Die Mitgliedstaaten legen Vorschriften fest, in denen das Verfahren, die operativen Elemente (einschließlich der Nutzung spezieller IKT-Plattformen), der Inhalt und die Bedingungen der in Absatz 2 genannten Vereinbarungen über den Informationsaustausch bestimmt werden. In diesen Vorschriften werden auch die Einzelheiten der Beteiligung von Behörden an solchen Vereinbarungen sowie operative Elemente, einschließlich der Nutzung spezieller IT-Plattformen, festgelegt. Die Mitgliedstaaten unterstützen die Anwendung solcher Vereinbarungen im Einklang mit ihren in Artikel 5 Absatz 2 Buchstabe g genannten Konzepten.

(4) Wesentliche und wichtige Einrichtungen unterrichten die zuständigen Behörden beim Abschluss von in Absatz 2 genannten Vereinbarungen über den Informationsaustausch oder gegebenenfalls über ihren Rücktritt von solchen Vereinbarungen, sobald dieser wirksam wird.

(5) Im Einklang mit dem Unionsrecht unterstützt die ENISA den Abschluss von Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Absatz 2, indem sie bewährte Verfahren und Orientierungshilfen zur Verfügung stellt.

Artikel 27

Freiwillige Meldung relevanter Informationen

Die Mitgliedstaaten stellen sicher, dass unbeschadet von Artikel 3 Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, auf freiwilliger Basis erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle melden können. Bei der Bearbeitung dieser Meldungen werden die Mitgliedstaaten gemäß dem in Artikel 20 vorgesehenen Verfahren tätig. Die Mitgliedstaaten können Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten. Freiwillige Meldungen dürfen nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

KAPITEL VI

Aufsicht und Durchsetzung

Artikel 28

Allgemeine Aspekte der Aufsicht und Durchsetzung

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden die Einhaltung dieser Richtlinie, insbesondere der Verpflichtungen nach den Artikeln 18 und 20, wirksam überwachen und die erforderlichen Maßnahmen treffen.

(2) Bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, arbeiten die zuständigen Behörden eng mit den Datenschutzbehörden zusammen.

Artikel 29

Aufsicht und Durchsetzung in Bezug auf wesentliche Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Aufsichts- bzw. Durchsetzungsmaßnahmen, die wesentlichen Einrichtungen in Bezug auf die in dieser Richtlinie festgelegten Verpflichtungen auferlegt werden, unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf wesentliche Einrichtungen befugt sind, in Bezug auf diese Einrichtungen folgende Maßnahmen vorzunehmen:

a) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich Stichprobenkontrollen;

b) regelmäßige Prüfungen;

c) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;

d) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien;

e) Anforderung von Informationen, die für die Bewertung der von der Einrichtung ergriffenen Cybersicherheitsmaßnahmen erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Meldepflicht gegenüber der ENISA nach Artikel 25 Absätze 1 und 2;

f) Anforderung des Zugangs zu Daten, Dokumenten oder sonstigen Informationen, die zur Erfüllung ihrer Aufsichtsaufgaben erforderlich sind;

g) Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise.

(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstaben e bis g geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an.

(4) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf wesentliche Einrichtungen befugt sind,

a) die Einrichtungen bei Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen zu verwarnen;

b) verbindliche Anweisungen oder Anordnungen zu erteilen, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen die in dieser Richtlinie festgelegten Verpflichtungen zu beheben;

c) diese Einrichtungen anzuweisen, das nicht mit den in dieser Richtlinie festgelegten Verpflichtungen zu vereinbarende Verhalten einzustellen und von Wiederholungen abzusehen;

d) diese Einrichtungen anzuweisen, ihre Risikomanagementmaßnahmen und/oder die Erfüllung ihrer Meldepflichten entsprechend bestimmter Vorgaben und innerhalb einer bestimmten Frist mit den in den Artikeln 18 und 20 festgelegten Verpflichtungen in Einklang zu bringen;

e) diese Einrichtungen anzuweisen, die natürliche(n) oder juristische(n) Person(en), für die sie Dienste oder Tätigkeiten erbringen und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können;

f) diese Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;

g) für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten zu benennen, der die Einhaltung ihrer Verpflichtungen nach den Artikeln 18 und 20 überwacht;

h) diese Einrichtungen anzuweisen, Aspekte der Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen entsprechend bestimmter Vorgaben öffentlich bekannt zu machen;

i) eine öffentliche Erklärung abzugeben, in der die Art des Verstoßes sowie die juristische(n) und natürliche(n) Person(en) genannt wird bzw. werden, die für den Verstoß gegen eine in dieser Richtlinie festgelegte Verpflichtung verantwortlich ist bzw. sind;

j) je nach den einzelstaatlichen Rechtsvorschriften und den Umständen des Einzelfalls zusätzlich zu den oder anstelle der unter den Buchstaben a bis i dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 31 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

(5) Erweisen sich die gemäß Absatz 4 Buchstaben a bis d und f ergriffenen Durchsetzungsmaßnahmen als unwirksam, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden befugt sind, eine Frist festzusetzen, innerhalb derer die wesentliche Einrichtung die erforderlichen Maßnahmen ergreifen muss, um die Mängel zu beheben oder die Anforderungen dieser Behörden zu erfüllen. Für den Fall, dass die geforderten Maßnahmen nicht innerhalb der gesetzten Frist ergriffen werden, stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden befugt sind,

a) die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten Dienste oder Tätigkeiten auszusetzen oder eine Zertifizierungs- oder Genehmigungsstelle aufzufordern, die Zertifizierung oder Genehmigung auszusetzen;

b) gegen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters Leitungsaufgaben in dieser wesentlichen Einrichtung wahrnehmen, und gegen jede andere natürliche Person, die für den Verstoß Verantwortung trägt, ein vorübergehendes Verbot zur Wahrnehmung von Leitungsaufgaben in dieser Einrichtung zu verhängen oder von den zuständigen Stellen oder Gerichten die Verhängung eines solchen Verbots zu verlangen.

Diese Sanktionen werden nur so lange angewandt, bis die Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Sanktionen verhängt wurden, zu erfüllen.

(6) Die Mitgliedstaaten stellen sicher, dass jede natürliche Person, die für eine wesentliche Einrichtung verantwortlich ist oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu gewährleisten, dass die Einrichtung die in dieser Richtlinie festgelegten Verpflichtungen erfüllt. Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung der in dieser Richtlinie festgelegten Verpflichtungen haftbar gemacht werden können.

(7) Bei der Ergreifung von Durchsetzungsmaßnahmen oder der Verhängung von Sanktionen gemäß den Absätzen 4 und 5 müssen die zuständigen Behörden die Verteidigungsrechte einhalten und den Umständen des Einzelfalls Rechnung tragen und dabei zumindest Folgendes gebührend berücksichtigen:

a) die Schwere des Verstoßes und die Wichtigkeit der Bestimmungen, gegen die verstoßen wurde. Insbesondere sollten folgende Verstöße als schwerwiegend betrachtet werden: wiederholte Verstöße, unterlassene Meldung oder Behebung von Sicherheitsvorfällen, die eine erhebliche Störung bewirken, Nichtbehebung von Mängeln nach verbindlicher Anweisung der zuständigen Behörden, Behinderung von Prüfungen oder Überwachungstätigkeiten, die nach der Feststellung eines Verstoßes von der zuständigen Behörde angeordnet wurden, sowie Übermittlung falscher oder grob verfälschender Informationen in Bezug auf Risikomanagementanforderungen oder Meldepflichten gemäß den Artikeln 18 und 20.

b) die Dauer des Verstoßes, einschließlich des Wiederholungsaspekts;

c) die Höhe des tatsächlich entstandenen Schadens bzw. entstandener Verluste oder potenzieller Schäden oder Verluste, die hätten verursacht werden können, sofern sich diese feststellen lassen. Bei der Bewertung dieses Aspekts sind unter anderem tatsächliche oder potenzielle finanzielle oder wirtschaftliche Verluste, Auswirkungen auf andere Dienste sowie die Zahl der betroffenen oder potenziell betroffenen Nutzer zu berücksichtigen;

d) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

e) von der Einrichtung ergriffene Maßnahmen zur Verhinderung oder Minderung des Schadens und/oder der Verluste;

f) Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren;

g) Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Person(en) mit den zuständigen Behörden.

(8) Die zuständigen Behörden müssen ihre Durchsetzungsentscheidungen ausführlich begründen. Bevor sie solche Entscheidungen treffen, teilen die zuständigen Behörden den betroffenen Einrichtungen ihre vorläufigen Erkenntnisse mit und räumen ihnen eine angemessene Frist zur Stellungnahme ein.

(9) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als einer kritischen Einrichtung gleichgestellte Einrichtungen eingestuft wurden,

die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden des betreffenden Mitgliedstaats, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannt wurden, unterrichten. Auf Ersuchen von gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] zuständigen Behörden dürfen die zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine als kritisch oder als einer kritischen Einrichtung gleichwertig eingestufte wesentliche Einrichtung ausüben.

Artikel 30

Aufsicht und Durchsetzung in Bezug auf wichtige Einrichtungen

(1) Werden Nachweise oder Hinweise dafür vorgelegt, dass eine wichtige Einrichtung ihren Verpflichtungen nach dieser Richtlinie, insbesondere den Artikeln 18 und 20, nicht nachkommt, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von nachträglichen Aufsichtsmaßnahmen tätig werden.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf wichtige Einrichtungen befugt sind, in Bezug auf diese Einrichtungen folgende Maßnahmen vorzunehmen:

a) Vor-Ort-Kontrollen und nachträgliche externe Aufsichtsmaßnahmen;

b) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;

c) Sicherheitsscans auf der Grundlage objektiver, fairer und transparenter Risikobewertungskriterien;

d) Anforderung von Informationen, die für die nachträgliche Bewertung der ergriffenen Cybersicherheitsmaßnahmen erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Meldepflicht gegenüber der ENISA nach Artikel 25 Absätze 1 und 2;

e) Anforderung auf Zugang zu Daten, Dokumenten und/oder sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind.

(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstabe d oder e geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an.

(4) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf wichtige Einrichtungen befugt sind,

a) die Einrichtungen bei Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen zu verwarnen;

b) verbindliche Anweisungen oder Anordnungen zu erteilen, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder den Verstoß gegen die in dieser Richtlinie festgelegten Verpflichtungen zu beheben;

c) diese Einrichtungen anzuweisen, das nicht mit den in dieser Richtlinie festgelegten Verpflichtungen zu vereinbarende Verhalten einzustellen, und von Wiederholungen abzusehen;

d) diese Einrichtungen anzuweisen, ihre Risikomanagementmaßnahmen oder die Erfüllung ihrer Meldepflichten entsprechend bestimmter Vorgaben und innerhalb einer bestimmten Frist mit den in den Artikeln 18 und 20 festgelegten Verpflichtungen in Einklang zu bringen;

e) diese Einrichtungen anzuweisen, die natürliche(n) oder juristische(n) Person(en), für die sie Dienste oder Tätigkeiten erbringen und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können;

f) diese Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;

g) diese Einrichtungen anzuweisen, Aspekte der Nichteinhaltung ihrer in dieser Richtlinie festgelegten Verpflichtungen entsprechend bestimmter Vorgaben öffentlich bekannt zu machen;

h) eine öffentliche Erklärung abzugeben, in der die Art des Verstoßes sowie die juristische(n) und natürliche(n) Person(en) genannt wird bzw. werden, die für den Verstoß gegen eine in dieser Richtlinie festgelegte Verpflichtung verantwortlich ist bzw. sind;

i) je nach den einzelstaatlichen Rechtsvorschriften und den Umständen des Einzelfalls zusätzlich zu den oder anstelle der unter den Buchstaben a bis h dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 31 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

(5) Artikel 29 Absätze 6 bis 8 gelten auch für die Aufsichts- und Durchsetzungsmaßnahmen, die in diesem Artikel für die in Anhang II aufgeführten wichtigen Einrichtungen vorgesehen sind.

Artikel 31

Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen gemäß diesem Artikel bei Verstößen gegen die in dieser Richtlinie festgelegten Verpflichtungen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 29 Absatz 4 Buchstaben a bis i, Artikel 29 Absatz 5 und Artikel 30 Absatz 4 Buchstaben a bis h verhängt.

(3) Bei der Entscheidung über die Verhängung einer Geldbuße und deren Höhe sind in jedem Einzelfall zumindest die in Artikel 29 Absatz 7 genannten Elemente gebührend zu berücksichtigen.

(4) Die Mitgliedstaaten stellen sicher, dass für Verstöße gegen die Verpflichtungen nach Artikel 18 oder Artikel 20 im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens 10 000 000 EUR oder

von bis zu 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche oder wichtige Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

(5) Die Mitgliedstaaten können die Befugnis vorsehen, Zwangsgelder zu verhängen, um eine wesentliche oder wichtige Einrichtung zu zwingen, einen Verstoß gemäß einer vorherigen Entscheidung der zuständigen Behörde einzustellen.

(6) Unbeschadet der Befugnisse der zuständigen Behörden gemäß den Artikeln 29 und 30 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Einrichtungen der öffentlichen Verwaltung im Sinne von Artikel 4 Absatz 23, die den in dieser Richtlinie festgelegten Verpflichtungen unterliegen, Geldbußen verhängt werden können.

Artikel 32

Verstöße mit Verletzungen des Schutzes personenbezogener Daten

(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Absatz 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung zuständigen Aufsichtsbehörden innerhalb einer angemessenen Frist.

(2) Beschließen die gemäß den Artikeln 55 und 56 der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörden, ihre Befugnisse gemäß Artikel 58 Buchstabe i der genannten Verordnung auszuüben und eine Geldbuße zu verhängen, so dürfen die zuständigen Behörden für denselben Verstoß keine Geldbuße nach Artikel 31 der vorliegenden Richtlinie verhängen. Die zuständigen Behörden können jedoch die Durchsetzungsmaßnahmen oder die Sanktionsbefugnisse gemäß Artikel 29 Absatz 4 Buchstaben a bis i, Artikel 29 Absatz 5 und Artikel 30 Absatz 4 Buchstaben a bis h dieser Richtlinie anwenden bzw. ausüben.

(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so kann die zuständige Behörde die im selben Mitgliedstaat angesiedelte Aufsichtsbehörde davon in Kenntnis setzen.

Artikel 33

Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen für Verstöße gegen die nach dieser Richtlinie erlassenen nationalen Bestimmungen und treffen alle erforderlichen Maßnahmen, um deren Anwendung sicherzustellen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum ... [zwei Jahre nach dem Inkrafttreten dieser Richtlinie] mit und melden ihr unverzüglich etwaige spätere Änderungen daran.

Artikel 34

Amtshilfe

(1) Wenn eine wesentliche oder wichtige Einrichtung ihre Dienste in mehr als einem Mitgliedstaat erbringt oder wenn sie ihre Hauptniederlassung oder einen Vertreter in einem Mitgliedstaat hat, während sich ihre Netz- und Informationssysteme in einem oder mehreren anderen Mitgliedstaaten befinden, so arbeiten die zuständige Behörde des Mitgliedstaats der Hauptniederlassung oder einer anderen Niederlassung oder des Vertreters und die zuständigen Behörden der betreffenden anderen Mitgliedstaaten zusammen und unterstützen einander. Diese Zusammenarbeit umfasst mindestens Folgendes:

a) über die zentralen Anlaufstellen unterrichten die zuständigen Behörden, die in einem Mitgliedstaat Aufsichts- oder Durchsetzungsmaßnahmen ergreifen, die zuständigen Behörden in den anderen betroffenen Mitgliedstaaten über die nach den Artikeln 29 und 30 ergriffenen Aufsichts- und Durchsetzungsmaßnahmen und deren Folgemaßnahmen und konsultieren sie zu diesen;

b) eine zuständige Behörde kann eine andere zuständige Behörde ersuchen, die in den Artikeln 29 und 30 genannten Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen;

c) auf begründetes Ersuchen einer anderen zuständigen Behörde leistet eine zuständige Behörde der ersuchenden Behörde Unterstützung, damit die in den Artikeln 29 und 30 genannten Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können. Diese Amtshilfe kann Auskunftsersuchen und Aufsichtsmaßnahmen umfassen, einschließlich Ersuchen um Durchführung von Vor-Ort-Kontrollen und externen Aufsichtsmaßnahmen oder gezielten Sicherheitsprüfungen. Die ersuchte zuständige Behörde darf das Amtshilfeersuchen nur ablehnen, wenn nach einem Austausch mit den anderen betroffenen Behörden, der ENISA und der Kommission entweder festgestellt wird, dass die Behörde für die erbetene Amtshilfe nicht zuständig ist oder dass die ersuchte Amtshilfe in keinem angemessenen Verhältnis zu den Aufsichtsaufgaben der zuständigen Behörde gemäß Artikel 29 oder Artikel 30 steht.

(2) Die zuständigen Behörden verschiedener Mitgliedstaaten können, wenn angezeigt und im gegenseitigen Einvernehmen die in den Artikeln 29 und 30 genannten gemeinsamen Aufsichtsmaßnahmen durchführen.

KAPITEL VII

Übergangs- und Schlussbestimmungen

Artikel 35

Überprüfung

Die Kommission überprüft regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere die Relevanz der in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen unterschiedlicher Größe und Art für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit bewertet. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRT-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Der erste Bericht dieser Art ist bis zum … [54 Monate nach Inkrafttreten dieser Richtlinie] vorzulegen.

Artikel 36

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 18 Absatz 6 und Artikel 21 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem […] übertragen.

(3) Die Befugnisübertragung gemäß Artikel 18 Absatz 6 und Artikel 21 Absatz 2 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 18 Absatz 6 und Artikel 21 Absatz 2 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 37

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss 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.

(3) Wird die Stellungnahme des Ausschusses im schriftlichen Verfahren eingeholt, so wird das Verfahren ohne Ergebnis abgeschlossen, wenn der Vorsitz des Ausschusses dies innerhalb der Frist zur Abgabe der Stellungnahme beschließt oder ein Ausschussmitglied dies verlangt.

Artikel 38

Umsetzung

(1) Die Mitgliedstaaten erlassen und veröffentlichen spätestens am … [18 Monate nach dem Tag des Inkrafttretens dieser Richtlinie] die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis. Sie wenden diese Vorschriften ab dem... [einen Tag nach dem im ersten Unterabsatz genannten Datum] an.

(2) Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf die vorliegende Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

Artikel 39

Änderung der Verordnung (EU) Nr. 910/2014

Artikel 19 der Verordnung (EU) Nr. 910/2014 wird gestrichen.

Artikel 40

Änderung der Richtlinie (EU) 2018/1972

Die Artikel 40 und 41 der Richtlinie (EU) 2018/1972 werden gestrichen.

Artikel 41

Aufhebung

Die Richtlinie (EU) 2016/1148 wird mit Wirkung vom … [Datum der Frist für die Umsetzung der Richtlinie] aufgehoben.

Bezugnahmen auf die Richtlinie (EU) 2016/1148 gelten als Bezugnahmen auf die vorliegende Richtlinie und sind nach Maßgabe der Entsprechungstabelle in Anhang III zu lesen.

Artikel 42

Inkrafttreten

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

Artikel 43

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

FINANZBOGEN

Inhalt

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

1.2. Politikbereich(e) *(Cluster)*

Kommunikationsnetze, Inhalte und Technologien

1.3. Der Vorschlag/Die Initiative betrifft:

☐ **eine neue Maßnahme**

☐ **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[40]

☒ **die Verlängerung einer bestehenden Maßnahme**

☐ **die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme**

1.4. Begründung des Vorschlags/der Initiative

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

Ziel der Überarbeitung ist es, die Cyberresilienz eines alle relevanten Sektoren umfassenden Spektrums von Unternehmen, die in der Europäischen Union tätig sind, zu erhöhen, eine gleich starke Resilienz bei den bereits unter die Richtlinie fallenden Sektoren im Binnenmarkt zu fördern und die gemeinsame Lageerfassung und kollektive Vorsorge und Reaktionsfähigkeit zu verbessern.

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

Eine unionsweite Cyberresilienz kann nicht erreicht werden, solange sie in nationalen oder regionalen Silos uneinheitlich angegangen wird. Mit der NIS-Richtlinie sollte dieser Mangel behoben werden, indem ein Rahmen für die Sicherheit der Netz- und Informationssysteme auf der Ebene der Mitgliedstaaten und auf Unionsebene geschaffen wurde. Bei der ersten Überprüfung der NIS-Richtlinie wurde jedoch auf eine Reihe inhärenter Mängel hingewiesen, die letztlich zu erheblichen Unterschieden zwischen den Mitgliedstaaten in Bezug auf Kapazitäten, Planung und Schutzniveau geführt haben, was sich gleichzeitig auf die Wettbewerbsbedingungen für ähnliche Unternehmen im Binnenmarkt auswirkt.

Ein Tätigwerden der EU über die geltenden Maßnahmen der NIS-Richtlinie hinaus ist hauptsächlich durch folgende Faktoren gerechtfertigt: i) den grenzüberschreitenden Charakter des Problems; ii) das Potenzial der EU-

[40] im Sinne des Artikels 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

Maßnahmen zur Verbesserung und Erleichterung wirksamer nationaler Strategien; iii) den Beitrag konzertierter und kooperativer NIS-Politikmaßnahmen zum wirksamen Schutz des Datenschutzes und der Privatsphäre.

Die genannten Ziele können daher besser auf EU-Ebene als durch die Mitgliedstaaten allein erreicht werden.

1.4.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Die NIS-Richtlinie ist das erste horizontale Binnenmarktinstrument, mit dem die Resilienz von Netzen und Systemen in der Union gegenüber Cybersicherheitsrisiken verbessert werden soll. Sie hat bereits erheblich zur Anhebung des gemeinsamen Cybersicherheitsniveaus in den Mitgliedstaaten beigetragen. Die Überprüfung der Funktionsweise und Umsetzung der Richtlinie hat jedoch eine Reihe von Mängeln ergeben, die neben der zunehmenden Digitalisierung und der Notwendigkeit einer zeitnahen Reaktion in einem überarbeiteten Rechtsakt angegangen werden müssen.

1.4.4. Vereinbarkeit mit anderen geeigneten Instrumenten sowie mögliche Synergieeffekte

Der neue Vorschlag steht voll und ganz im Einklang mit anderen einschlägigen Initiativen wie dem Vorschlag für eine Verordnung über die digitale Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) und dem Vorschlag für eine Richtlinie über die Resilienz kritischer Betreiber wesentlicher Dienste. Sie steht auch im Einklang mit dem europäischen Kodex für die elektronische Kommunikation, der Datenschutz-Grundverordnung und der eIDAS-Verordnung.

Der Vorschlag ist ein wesentlicher Bestandteil der EU-Strategie für die Sicherheitsunion.

1.5. Laufzeit der Maßnahme(n) und Dauer ihrer finanziellen Auswirkungen

☐ **befristete Laufzeit**

– ☐ Laufzeit: [TT.MM.]JJJJ bis [TT.MM.]JJJJ

– ☐ Finanzielle Auswirkungen auf die Mittel für Verpflichtungen von JJJJ bis JJJJ und auf die Mittel für Zahlungen von JJJJ bis JJJJ

☒ **unbefristete Laufzeit**

– Anlaufphase von 2022 bis 2025,

– anschließend reguläre Umsetzung.

1.6. Vorgeschlagene Methode(n) der Mittelverwaltung[41]

Direkte Mittelverwaltung durch die Kommission

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

– ☐ durch Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

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

– ☐ Drittländer oder die von ihnen benannten Einrichtungen

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

– ☐ die EIB und den Europäischen Investitionsfonds

– X☐ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

– ☐ öffentlich-rechtliche Körperschaften

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende finanzielle Garantien bieten

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

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

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

Bemerkungen

Die Agentur der Europäischen Union für Cybersicherheit (ENISA), die durch den Rechtsakt zur Cybersicherheit ein neues ständiges Mandat erhalten hat, würde die Mitgliedstaaten und die Kommission bei der Umsetzung der überarbeiteten NIS-Richtlinie unterstützen.

[41] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

Infolge der überarbeiteten NIS-Richtlinie wird die ENISA ab 2022/23 über zusätzliche Handlungsbereiche verfügen. Diese Aktionsbereiche werden zwar durch die allgemeinen Aufgaben der ENISA gemäß ihrem Mandat abgedeckt, sie führen jedoch zu einer zusätzlichen Arbeitsbelastung für die Agentur. Genauer gesagt soll die ENISA gemäß dem Vorschlag der Kommission für eine überarbeitete NIS-Richtlinie neben ihren derzeitigen Aktionsbereichen auch die folgenden Maßnahmen in ihr Arbeitsprogramm aufnehmen: i) Entwicklung und Pflege eines europäischen Schwachstellenregisters (Artikel 6 Absatz 2 des Vorschlags), ii) Bereitstellung des Sekretariats des Europäischen Netzes der Verbindungsorganisationen für Cyberkrisen (CyCLONe) (Artikel 14 des Vorschlags) und Herausgabe eines jährlichen Berichts über den Stand der Cybersicherheit in der EU (Artikel 15 des Vorschlags), iii) Unterstützung der Durchführung von Peer Reviews zwischen den Mitgliedstaaten (Artikel 16 des Vorschlags), iv) Erhebung aggregierter Daten über Sicherheitsvorfälle in den Mitgliedstaaten und Bereitstellung technischer Leitlinien (Artikel 20 Absatz 9 des Vorschlags) sowie Aufstellung und Pflege eines Verzeichnisses der Einrichtungen, die grenzüberschreitende Dienste erbringen (Artikel 25 des Vorschlags).

Daher werden ab 2022 fünf zusätzliche VZÄ mit den entsprechenden Haushaltsmitteln in Höhe von etwa 0,61 Mio. EUR pro Jahr beantragt, um diese neuen Stellen abzudecken (siehe separater Finanzbogen für Agenturen).

2. VERWALTUNGSMASSNAHMEN

2.1. Überwachung und Berichterstattung

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

Die Kommission wird die Anwendung der Richtlinie regelmäßig überprüfen und dem Europäischen Parlament und dem Rat erstmals drei Jahre nach ihrem Inkrafttreten Bericht erstatten. Darüber hinaus wird die Kommission die ordnungsgemäße Umsetzung der Richtlinie durch die Mitgliedstaaten bewerten.

2.2. Verwaltungs- und Kontrollsystem(e)

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

Das für diesen Politikbereich zuständige Referat der GD CNECT wird die Umsetzung der Richtlinie verwalten.

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

Sehr geringes Risiko, da das Ökosystem der NIS-Richtlinie bereits besteht.

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

Nicht relevant. Ausschließlich Verwendung von Verwaltungsmitteln („Globaldotation“).

2.3. Prävention von Betrug und Unregelmäßigkeiten

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

Nicht relevant. Ausschließlich Verwendung von Verwaltungsmitteln („Globaldotation“).

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Rubrik des Mehrjährigen Finanzrahmens und neu vorgeschlagene Ausgabenlinie(n) im Haushaltsplan

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer [Rubrik…7……...……]	GM/NGM [42]	von EFTA-Ländern[43]	von Kandidatenländern[44]	von Drittländern	nach Artikel [21 Absatz 2 Buchstabe b] der Haushaltsordnung
	20 02 06 Verwaltungsausgaben 20 02 06	NGM	NEIN	NEIN	NEIN	NEIN

[42] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.

[43] EFTA: Europäische Freihandelsassoziation.

[44] Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.2.1. Übersicht über die geschätzten Auswirkungen auf die Ausgaben

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	**<…>**	[Rubrik……...……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Nach 2027***	**INSGESAMT**
Operative Mittel (getrennt nach den unter 3.1 aufgeführten Haushaltslinien)	Verpflichtungen	1)									
	Zahlungen	2)									
Aus der Finanzausstattung bestimmter spezifischer Programme finanzierte Verwaltungsausgaben[45]	Verpflichtungen = Zahlungen	3)									
Mittel für die Finanzausstattung des Programms INSGESAMT	Verpflichtungen	= 1 + 3									
	Zahlungen	= 2 + 3									

Rubrik des Mehrjährigen Finanzrahmens	7	Verwaltungsausgaben Sitzungen: Plenarsitzungen der NIS-Kooperationsgruppe finden in der Regel viermal jährlich statt. Die Kommission übernimmt die Kosten für Bewirtung und Reisekosten von Vertretern aus 27 Mitgliedstaaten (ein Vertreter pro Mitgliedstaat). Die Kosten einer Sitzung könnten bis zu 15.000 EUR betragen. Dienstreisen: Die Dienstreisen sind mit der Überwachung der Umsetzung der NIS-Richtlinie verbunden. Beispiel: In einem Jahr (Mai 2019 bis Juli 2020) sollten wir so genannte „NIS-Länderbesuche“ organisieren und alle 27 Mitgliedstaaten besuchen,

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

		um die Umsetzung der NIS-Richtlinie in der gesamten EU zu erörtern.

Zum Ausfüllen dieses Teils ist die „Tabelle für Verwaltungsausgaben“ zu verwenden, die zuerst in den Anhang des Finanzbogens zu Rechtsakten, der für die dienststellenübergreifende Konsultation in DECIDE hochgeladen wird, aufgenommen wird.

in Mio. EUR (3 Dezimalstellen)

		2021	2022	2023	2024	2025	2026	2027	*Nach 2027*	INSGESAMT
Personal		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Sonstige Verwaltungsausgaben		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
Mittel unter der RUBRIK 7 des Mehrjährigen Finanzrahmens INSGESAMT	(Verpflichtungen insges. = Zahlungen insges.)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

in Mio. EUR (3 Dezimalstellen)

		2021	2022	2023	2024	2025	2026	2027	*Nach 2027*	INSGESAMT
Mittel in allen RUBRIKEN des mehrjährigen Finanzrahmens **INSGESAMT**	Verpflichtungen									
	Zahlungen									

3.2.2. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

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

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

in Mio. EUR (3 Dezimalstellen)

Jahre	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**INSGESAMT**
RUBRIK 7 des Mehrjährigen Finanzrahmens								
Personal	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Sonstige Verwaltungsausgaben	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Zwischensumme RUBRIK 7 des Mehrjährigen Finanzrahmens	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

Außerhalb der RUBRIK 7[46] of the multiannual financial framework								
Personal								
Sonstige Verwaltungsausgaben								
Zwischensumme Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens								

INSGESAMT	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

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

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

3.2.2.1. Geschätzter Personalbedarf

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

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

Schätzung in Vollzeitäquivalenten

Jahre		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)								
Sitz und Vertretungen der Kommission		6	6	6	6	6	6	6
Delegationen								
Forschung								
• Externes Personal (in Vollzeitäquivalenten – (VZÄ)) – VB, ÖB, ANS, LAK und JFD[47] Rubrik 7								
Aus der RUBRIK 7 des Mehrjährigen Finanzrahmens finanziert	- am Sitz	3	3	3	3	3	3	3
	- in den Delegationen							
Aus der Finanzausstattung des Programms finanziert [48]	- am Sitz							
	- in den Delegationen							
Forschung								
Sonstiges (bitte angeben)								
INSGESAMT		**9**	**9**	**9**	**9**	**9**	**9**	**9**

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

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	• Ausarbeitung delegierter Rechtsakte gemäß Artikel 18 Absatz 6, Artikel 21 Absatz 2 und Artikel 36; • Ausarbeitung von Durchführungsrechtsakten gemäß Artikel 12 Absatz 8, Artikel 18 Absatz 5 und Artikel 20 Absatz 11; • Bereitstellung eines Sekretariats für die NIS-Kooperationsgruppe; • Organisation der Plenar- und Arbeitssitzungen der NIS-Kooperationsgruppe; • Koordinierung der Arbeit der Mitgliedstaaten an verschiedenen Dokumenten (Leitlinien, Instrumentarien usw.); • Zusammenarbeit mit anderen Kommissionsdienststellen, ENISA und nationalen Behörden im Hinblick auf die Umsetzung der NIS-Richtlinie; • Analyse nationaler Methoden und bewährter Verfahren im Zusammenhang mit der Umsetzung der NIS-Richtlinie.
Externes Personal	Bedarfsgerechte Unterstützung aller oben genannten Aufgaben

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

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

3.2.3. Finanzierungsbeteiligung Dritter

Der Vorschlag/Die Initiative

– ☐X sieht keine Kofinanzierung durch Dritte vor.

– ☐ sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

Jahre	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**INSGESAMT**
Kofinanzierende Einrichtung								
Kofinanzierung INSGESAMT								

3.3. Geschätzte Auswirkungen auf die Einnahmen

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

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

☐ auf die Eigenmittel

☐ auf die übrigen Einnahmen

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

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Auswirkungen des Vorschlags/der Initiative[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artikel ….							

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

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

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

ANHANG
des FINANZBOGENS ZU RECHTSAKTEN

Bezeichnung des Vorschlags/der Initiative:

Vorschlag für eine Richtlinie zur Überarbeitung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

……
……

1. VORAUSSICHTLICHER BEDARF an PERSONAL und MITTEL hierfür

2. SONSTIGE VERWALTUNGSAUSGABEN

3. KOSTENSCHÄTZUNGSMETHODEN

3.1 Personal

3.2 Sonstige Verwaltungsausgaben

Bei der Einleitung der dienststellenübergreifenden Konsultation ist dieser Anhang, ***der von den einzelnen an dem Vorschlag/der Initiative beteiligten Generaldirektionen/Dienststellen auszufüllen ist****, dem Finanzbogen zu Rechtsakten beizulegen.*

Die in diesen Tabellen enthaltenen Daten fließen in die Tabellen des Finanzbogens zu Rechtsakten ein. Die Tabellen sind als interne Dokumente ausschließlich für den Dienstgebrauch der Kommission bestimmt.

1. Voraussichtlicher Bedarf an Personal und Mittel hierfür

☐ Für den Vorschlag/die Initiative werden keine Mittel für Personal benötigt.

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

in Mio. EUR (3 Dezimalstellen)

RUBRIK 7 des Mehrjährigen Finanzrahmens		**2021**		**2022**		**2023**		**2024**		**2025**		**2026**		**2027**		**INSGESAMT**	
		VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel
• Planstellen (Beamte und Bedienstete auf Zeit)																	
Sitz und Vertretungen der Kommission	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
In den Delegationen der Union	AD																
	AST																
• Externes Personal [50] 0,24																	
Globaldotation	VB	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	ANS																
	LAK																
In den Delegationen der Union	VB																
	ÖB																

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

	ANS																
	LAK																
	JFD																
Sonstige Haushaltslinien (*bitte angeben*)																	
Zwischensumme – RUBRIK 7 des Mehrjährigen Finanzrahmens		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

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

Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens		2021		2022		2023		2024		2025		2025		2025		INSGESAMT	
		VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel	VZÄ	Mittel
• Planstellen (Beamte und Bedienstete auf Zeit)																	
Forschung	AD																
	AST																
• Externes Personal [51]																	
Aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien)	- am Sitz	VB															
		ANS															
		LAK															
	- in den Delegationen der Union	VB															
		ÖB															
		ANS															
		LAK															
		JFD															
Forschung		VB															
		ANS															
		LAK															
Sonstige Haushaltslinien (*bitte*																	

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

angeben)																	
Zwischensumme – Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens																	

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

Geschätzte Auswirkungen auf die Humanressourcen der ENISA

Die Agentur der Europäischen Union für Cybersicherheit (ENISA), die durch den Rechtsakt zur Cybersicherheit ein neues ständiges Mandat erhalten hat, würde die Mitgliedstaaten und die Kommission bei der Umsetzung der überarbeiteten NIS-Richtlinie unterstützen.

Infolge der überarbeiteten NIS-Richtlinie wird die ENISA ab 2022/23 über zusätzliche Handlungsbereiche verfügen. Diese Aktionsbereiche würden zwar durch die allgemeinen Aufgaben der ENISA gemäß ihrem Mandat abgedeckt, sie würden jedoch zu einer zusätzlichen Arbeitsbelastung für die Agentur führen. Genauer gesagt soll die ENISA gemäß dem Vorschlag der Kommission für eine überarbeitete NIS-Richtlinie neben ihren derzeitigen Aktionsbereichen auch die folgenden Maßnahmen in ihr Arbeitsprogramm aufnehmen: i) Entwicklung und Pflege eines europäischen Schwachstellenregisters (Artikel 6 Absatz 2 des Vorschlags), ii) Bereitstellung des Sekretariats des Europäischen Netzes der Verbindungsorganisationen für Cyberkrisen (CyCLONe) (Artikel 14 des Vorschlags) und Herausgabe eines jährlichen Berichts über den Stand der Cybersicherheit in der EU (Artikel 15 des Vorschlags), iii) Unterstützung der Durchführung von Peer Reviews zwischen den Mitgliedstaaten (Artikel 16 des Vorschlags), iv) Erhebung aggregierter Daten über Sicherheitsvorfälle in den Mitgliedstaaten und Bereitstellung technischer Orientierungshilfen (Artikel 20 Absatz 9 des Vorschlags) sowie Pflege eines Verzeichnisses der Einrichtungen, die grenzüberschreitende Dienste erbringen (Artikel 25 des Vorschlags).

Daher werden ab 2022 5 zusätzliche VZÄ mit den entsprechenden Haushaltsmitteln in Höhe von etwa 0,61 Mio. EUR pro Jahr beantragt, um diese neuen Stellen abzudecken (siehe separater Finanzbogen für Agenturen).

Daher werden ab 2022 5 zusätzliche VZÄ mit den entsprechenden Haushaltsmitteln beantragt, um diese neuen Stellen abzudecken.

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

☐X Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr **N** [52] **2022**	Jahr **N+1** **2023**	Jahr **N+2** **2024**	Jahr **N+3** **2025**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.	**INSGESAMT**

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

Bedienstete auf Zeit (Funktionsgruppe AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Bedienstete auf Zeit (Funktionsgruppe A ST)								
Vertragsbedienstete	0,160	0,160	0,160	0,160	0,160	0,160		
Abgeordnete nationale Sachverständige								**0,96**

INSGESAMT	**0,61**	**0,61**	**0,61**	**0,61**	**0.61**	**0,61**		**3,66**

Personalbedarf (VZÄ):

	Jahr **N** [53] **2022**	Jahr **N+1** **2023**	Jahr **N+2** **2024**	Jahr **N+3** **2025**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.	**INSGESAMT**

	3	3	3	3	3	3		**18**
Vertragsbedienstete	2	2	2	2	2	2		**12**

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

Abgeordnete nationale Sachverständige								

INSGESAMT	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Sonstige Verwaltungsausgaben

☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.
☐X Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

RUBRIK 7 des Mehrjährigen Finanzrahmens	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insgesamt**
Am Sitz der Kommission:								
Dienstreisen und Repräsentationszwecke	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Konferenzen und Sitzungen	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Ausschusssitzungen[54]								
Untersuchungen und Konsultationen								
Informations- und Managementsysteme								

[54] Art des Ausschusses sowie jeweilige Gruppe angeben.

Ausgaben für IKT-Ausstattung und -Dienstleistungen in der Kommission[55]								
Sonstige Haushaltslinien (*ggf. bitte angeben*)								
In den Delegationen der Union:								
Dienstreise- und Repräsentationskosten, Ausgaben für Konferenzen								
Berufliche Fortbildung des Personals								
Kauf oder Miete von Gebäuden und Nebenkosten								
Ausstattung, Mobiliar, Bürobedarf und Dienstleistungen								
Zwischensumme RUBRIK 7 des Mehrjährigen Finanzrahmens	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[55] IKT: Informations- und Kommunikationstechnologien: GD DIGIT ist zu konsultieren.

in Mio. EUR (3 Dezimalstellen)

Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Insgesamt**
Aus operativen Mitteln finanzierte technische und administrative Unterstützung ohne externes Personal (vormalige BA-Linien)								
- am Sitz								
- in den Delegationen der Union								
Sonstige Verwaltungsausgaben für die Forschung								
Sonstige Haushaltslinien (*ggf. bitte angeben*)								
Zwischensumme – Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens								

INSGESAMT RUBRIK 7 und Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Der Bedarf an Verwaltungsmitteln wird aus den Mitteln gedeckt, die für die Verwaltung der Maßnahme bereits zugewiesen wurden bzw. ggf. neu zugewiesen werden. Hinzu kommen etwaige zusätzliche Mittel, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

3. Kostenschätzungsmethoden

3.1 Personal

In diesem Teil ist zu erläutern, nach welcher Methode der geschätzte Personalbedarf berechnet wird (Annahmen hinsichtlich des Arbeitsaufwands mit Angabe der genauen Funktionsbezeichnungen (Arbeitsprofile nach Sysper 2), der Personalkategorie und entsprechender Durchschnittskosten)

RUBRIK 7 des Mehrjährigen Finanzrahmens

Hinweis: Für die am Sitz der Kommission tätigen Personalkategorien sind die Durchschnittskosten unter folgender Adresse abrufbar (BudgWeb):
https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx

- Beamte sowie Bedienstete auf Zeit

6 VZÄ-Bedienstete (Durchschnittskosten 0,150) = 0,9 pro Jahr

- Ausarbeitung delegierter Rechtsakte gemäß Artikel 18 Absatz 6, Artikel 21 Absatz 2 und Artikel 36;
- Ausarbeitung von Durchführungsrechtsakten gemäß Artikel 12 Absatz 8, Artikel 18 Absatz 5 und Artikel 20 Absatz 11;
- Bereitstellung eines Sekretariats für die NIS-Kooperationsgruppe;
- Organisation der Plenar- und Arbeitssitzungen der NIS-Kooperationsgruppe;
- Koordinierung der Arbeit der Mitgliedstaaten an verschiedenen Dokumenten (Leitlinien, Instrumentarien usw.);
- Zusammenarbeit mit anderen Kommissionsdienststellen, ENISA und nationalen Behörden im Hinblick auf die Umsetzung der NIS-Richtlinie;
- Analyse nationaler Methoden und bewährter Verfahren im Zusammenhang mit der Umsetzung der NIS-Richtlinie.

- Externes Personal

3 VB (Durchschnittskosten 0,08) = 0,24 pro Jahr

- Bedarfsgerechte Unterstützung aller oben genannten Aufgaben

Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens

- Nur für aus dem Forschungshaushalt finanzierte Stellen

- Externes Personal

3.2 Sonstige Verwaltungsausgaben

Für jede Haushaltslinie ist die verwendete Berechnungsmethode darzulegen,

insbesondere auch die zugrunde gelegten Annahmen (z. B. Anzahl der Sitzungen pro Jahr, Durchschnittskosten usw.)

RUBRIK 7 des Mehrjährigen Finanzrahmens

Sitzungen: Plenarsitzungen der NIS-Kooperationsgruppe finden in der Regel viermal jährlich statt. Die Kommission übernimmt die Kosten für Bewirtung und Reisekosten von Vertretern aus 27 Mitgliedstaaten (ein Vertreter pro Mitgliedstaat). Die Kosten einer Sitzung könnten bis zu 15.000 EUR betragen, was 60.000 EUR pro Jahr entspricht.

Dienstreisen: Die Dienstreisen sind mit der Überwachung der Umsetzung der NIS-Richtlinie verbunden. Beispiel: In einem Jahr (Mai 2019 – Juli 2020) sollten wir sogenannte „NIS-Länderbesuche“ durchführen und alle 27 Mitgliedstaaten besuchen, um

die Umsetzung der NIS-Richtlinie in der gesamten EU zu erörtern.

Außerhalb der RUBRIK 7 des Mehrjährigen Finanzrahmens

ANHANG 7

des
BESCHLUSSES DER KOMMISSION

über die Internen Vorschriften für die Ausführung des Gesamthaushaltsplans der Europäischen Union (Einzelplan Kommission), gerichtet an die Dienststellen der Kommission

FINANZBOGEN ZU RECHTSAKTEN – AGENTUREN

Dieser Finanzbogen deckt den Antrag ab, das Personal der ENISA ab 2022 um 5 VZÄ aufzustocken, um zusätzliche Tätigkeiten im Zusammenhang mit der Umsetzung der NIS-Richtlinie durchzuführen. Diese Tätigkeiten fallen bereits unter das ENISA-Mandat.

Inhalt

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

1.2. Politikbereich(e)

Kommunikationsnetze, Inhalte und Technologien

1.3. Der Vorschlag/Die Initiative betrifft

☐ **eine neue Maßnahme**

☐ **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[56]

☒ **die Verlängerung einer bestehenden Maßnahme**

☐ **die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme**

1.4. Ziel(e)

1.4.1. Allgemeine(s) Ziel(e)

Ziel der Überarbeitung ist es, die Cyberresilienz eines alle relevanten Sektoren umfassenden Spektrums von Unternehmen, die in der Europäischen Union tätig sind, zu erhöhen, eine gleich starke Resilienz bei den bereits unter die Richtlinie fallenden Sektoren im Binnenmarkt zu fördern und die gemeinsame Lageerfassung und kollektive Vorsorge und Reaktionsfähigkeit zu verbessern.

1.4.2. Einzelziel(e)

Um dem Problem der geringen Cyberresilienz der in der Europäischen Union tätigen Unternehmen zu begegnen, besteht das spezifische Ziel darin, sicherzustellen, dass Unternehmen in allen Sektoren, die von Netz- und Informationssystemen abhängig sind und wichtige Dienste für Wirtschaft und Gesellschaft insgesamt erbringen, verpflichtet sind, Cybersicherheitsmaßnahmen zu ergreifen und Sicherheitsvorfälle zu melden, um die Resilienz gegenüber Cyberangriffen im gesamten Binnenmarkt insgesamt zu erhöhen.

Um das Problem der uneinheitlichen Resilienz der Mitgliedstaaten und Sektoren anzugehen, besteht das spezifische Ziel darin, sicherzustellen, dass alle Einrichtungen, die in Sektoren tätig sind, die unter den NIS-Rechtsrahmen fallen, und die eine ähnliche Größe und Bedeutung haben, demselben Regulierungsrahmen unterliegen (d. h. innerhalb oder außerhalb des Anwendungsbereichs liegen), und zwar unabhängig davon, unter welche Gerichtsbarkeit sie in der EU fallen.

Um sicherzustellen, dass alle Einrichtungen, die in Sektoren tätig sind, die unter den NIS-Rechtsrahmen fallen, die gleichen Verpflichtungen auf der Grundlage des Konzepts des Risikomanagements in Bezug auf Sicherheitsmaßnahmen erfüllen und alle Sicherheitsvorfälle

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

auf der Grundlage einheitlicher Kriterien melden müssen, besteht das spezifische Ziel darin, sicherzustellen, dass die zuständigen Behörden die in dem Rechtsinstrument festgelegten Vorschriften durch abgestimmte Aufsichts- und Durchsetzungsmaßnahmen wirksamer durchsetzen, und ein vergleichbares Niveau der den zuständigen Behörden zugewiesenen Ressourcen in allen Mitgliedstaaten sicherzustellen, damit sie die Kernaufgaben des NIS-Rahmens erfüllen können.

Um das Problem der mangelnden gemeinsamen Lageerfassung und Krisenreaktion anzugehen, besteht das spezifische Ziel darin, den Austausch wesentlicher Informationen zwischen den Mitgliedstaaten sicherzustellen, indem klare Verpflichtungen für die zuständigen Behörden eingeführt werden, Informationen weiterzugeben und bei Cyberbedrohungen und Sicherheitsvorfällen zusammenzuarbeiten, und indem eine gemeinsame operative Krisenreaktionskapazität der Union entwickelt wird.

1.4.3. Erwartete Ergebnisse und Auswirkungen

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

Der Vorschlag dürfte erhebliche Vorteile mit sich bringen: Schätzungen zufolge könnte er dazu führen, dass die Kosten von Cybersicherheitsvorfällen um 11,3 Mrd. EUR gesenkt würden. Der sektorale Anwendungsbereich würde im Rahmen des NIS-Rahmens erheblich erweitert, aber neben den oben genannten Vorteilen wäre die Belastung, die sich aus den NIS-Anforderungen ergeben könnte, insbesondere aus aufsichtsrechtlicher Sicht, sowohl für die neu abzudeckenden Unternehmen als auch für die zuständigen Behörden ausgewogen. Dies liegt daran, dass das neue NIS-Rahmenwerk einen zweischichtigen Ansatz etablieren würde, mit einem Schwerpunkt auf großen und wesentlichen Einrichtungen und einer Differenzierung der Aufsichtsregelung, die nur eine Ex-post-Aufsicht für eine große Anzahl von ihnen erlaubt, insbesondere für diejenigen, die als „wichtig“, aber nicht als „wesentlich“ angesehen werden.

Insgesamt würde der Vorschlag zu effizienten Kompromissen und Synergien führen, und laut Analyse der Optionen über das größte Potenzial verfügen, unionsweit ein höheres und einheitliches Cyberresilienzniveau wesentlicher Einrichtungen zu gewährleisten, das schließlich zu Kosteneinsparungen für Unternehmen und für die Gesellschaft führen würde.

Der Vorschlag würde auch zu gewissen Einhaltungs- und Durchsetzungskosten für die zuständigen Behörden der Mitgliedstaaten führen (Schätzungen zufolge bedeutet dies eine Aufstockung der Mittel um insgesamt 20-30 %). Der neue Rahmen würde jedoch auch erhebliche Vorteile bringen, indem er einen besseren Überblick über und eine bessere Interaktion mit wesentlichen Unternehmen, eine verstärkte grenzüberschreitende Zusammenarbeit auf operativer Ebene sowie Amtshilfe und Peer-review-Mechanismen bietet. Dies würde zur Verbesserung der Cybersicherheitskapazitäten in den Mitgliedstaaten insgesamt führen.

Für die Unternehmen, die in den Anwendungsbereich des NIS-Rahmens fallen würden, wird geschätzt, dass sie in den ersten Jahren nach der Einführung des neuen NIS-Rahmens ihre derzeitigen Ausgaben für die IKT-Sicherheit um maximal 22 % erhöhen müssten (für Unternehmen, die bereits in den Anwendungsbereich der aktuellen NIS-Richtlinie fallen, wären dies 12 %). Dieser durchschnittliche Anstieg der Ausgaben für IKT-Sicherheit würde jedoch zu einem verhältnismäßigen Nutzen solcher Investitionen führen, insbesondere dadurch, dass die Kosten von Cybersicherheitsvorfällen (schätzungsweise 118 Mrd. EUR über einen Zeitraum von zehn Jahren) erheblich gesenkt würden.

Klein- und Kleinstunternehmen würden vom Anwendungsbereich des NIS-Rahmens ausgenommen. Für mittlere Unternehmen ist davon auszugehen, dass die Ausgaben für IKT-Sicherheit in den ersten Jahren nach Einführung des neuen NIS-Rahmens steigen werden. Gleichzeitig würde eine Anhebung der Sicherheitsanforderungen für diese Unternehmen auch Anreize für ihre Cybersicherheitskapazitäten schaffen und dazu beitragen, ihr IKT-Risikomanagement zu verbessern.

Die Auswirkungen auf nationale Haushalte und Behörden: Kurz- und mittelfristig ist mit einem Anstieg der benötigten Ressourcen um schätzungsweise 20-30 % zu rechnen.

Weitere signifikante negative Auswirkungen sind nicht zu erwarten. Es wird erwartet, dass der Vorschlag zu robusteren Cybersicherheitskapazitäten führt und folglich die Anzahl und den Schweregrad von Vorfällen, einschließlich Verstößen gegen den Datenschutz, stärker eindämmen würde. Er dürfte sich auch positiv auf die Gewährleistung gleicher Wettbewerbsbedingungen in allen Mitgliedstaaten auswirken, und zwar für alle Einrichtungen,

die in den Anwendungsbereich der NIS fallen, und die Informationsasymmetrien im Bereich der Cybersicherheit verringern.

1.4.4. Leistungsindikatoren

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

Die Bewertung der Indikatoren wird von der Kommission mit Unterstützung der ENISA und der Kooperationsgruppe drei Jahre nach Inkrafttreten des neuen NIS-Rechtsakts durchgeführt. Einige der Überwachungsindikatoren, auf deren Grundlage der Erfolg der NIS-Überprüfung bewertet würde, sind:

• Verbesserter Umgang mit Vorfällen: Durch Cybersicherheitsmaßnahmen verbessern Unternehmen nicht nur ihre Fähigkeit, bestimmte Sicherheitsvorfälle vollständig zu vermeiden, sondern auch ihre Fähigkeit, auf Sicherheitsvorfälle zu reagieren. Erfolgsmaßstäbe sind daher i) die Verkürzung der durchschnittlichen Zeit, die für die Erkennung eines Vorfalls benötigt wird, ii) die Zeit, die ein Unternehmen durchschnittlich benötigt, um sich von einem Vorfall zu erholen, und iii) die durchschnittlichen Kosten eines durch einen Vorfall verursachten Schadens.

• Stärkere Sensibilisierung der Führungskräfte von Unternehmen für Cybersicherheitsrisiken: Indem Unternehmen verpflichtet werden, Maßnahmen zu ergreifen, würde eine überarbeitete NIS-Richtlinie dazu beitragen, das Bewusstsein der Führungskräfte für Cybersicherheitsrisiken zu schärfen. Dies lässt sich messen, indem untersucht wird, inwieweit Unternehmen, die in den Anwendungsbereich der NIS fallen, der Cybersicherheit in unternehmensinternen Strategien und Prozessen Vorrang einräumen, was aus internen Unterlagen, einschlägigen Schulungsprogrammen und Sensibilisierungsmaßnahmen für die Beschäftigten hervorgeht, und inwieweit sicherheitsrelevante IKT-Investitionen priorisiert werden. Das Management aller wichtigen und wesentlichen Einrichtungen sollte sich auch der Vorschriften der NIS-Richtlinie bewusst sein.

• Angleichung der sektorspezifischen Ausgaben: Die Ausgaben für IKT-Sicherheit variieren erheblich zwischen den einzelnen Sektoren in der EU. Da Unternehmen in mehr Sektoren Maßnahmen ergreifen müssen, dürften sich die Abweichungen von den durchschnittlichen sektorspezifischen Ausgaben für IKT-Sicherheit als prozentualer Anteil an den IKT-Gesamtausgaben zwischen Sektoren und Mitgliedstaaten verringern.

• Stärkung der zuständigen Behörden und verstärkte Zusammenarbeit: Mit der überarbeiteten NIS-Richtlinie würden den zuständigen Behörden möglicherweise zusätzliche Aufgaben übertragen. Dies hätte messbare Auswirkungen auf die finanziellen und personellen Ressourcen, die den Cybersicherheitsagenturen auf nationaler Ebene zur Verfügung gestellt werden, und dürfte sich auch positiv auf die Fähigkeit der zuständigen Behörden auswirken, proaktiv zusammenzuarbeiten und somit die Zahl der Fälle, in denen die zuständigen Behörden miteinander kooperieren, um grenzüberschreitende Sicherheitsvorfälle zu bewältigen oder gemeinsame Aufsichtstätigkeiten durchzuführen, erhöhen.

• Verstärkter Informationsaustausch: Die überarbeiteten NIS würde auch den Informationsaustausch zwischen Unternehmen und mit den zuständigen Behörden verbessern. Eines der Ziele der Überprüfung könnte darin bestehen, die Zahl der Einrichtungen, die sich an den verschiedenen Formen des Informationsaustauschs beteiligen, zu erhöhen.

1.5. Begründung des Vorschlags/der Initiative

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

Ziel des Vorschlags ist es, die Cyberresilienz eines alle relevanten Sektoren umfassenden Spektrums von Unternehmen, die in der Europäischen Union tätig sind, zu erhöhen, eine einheitliche Resilienz bei den bereits unter die Richtlinie fallenden Sektoren im Binnenmarkt zu fördern und die gemeinsame Lageerfassung und kollektive Vorsorge und Reaktionsfähigkeit zu verbessern. Er wird auf den Ergebnissen aufbauen, die mit der Umsetzung der Richtlinie (EU) 2016/1148 in den letzten vier Jahren erreicht wurden.

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

Eine unionsweite Cyberresilienz kann nicht erreicht werden, solange sie in nationalen oder regionalen Silos uneinheitlich angegangen wird. Mit der NIS-Richtlinie sollte dieser Mangel behoben werden, indem ein Rahmen für die Sicherheit der Netz- und Informationssysteme auf der Ebene der Mitgliedstaaten und auf Unionsebene geschaffen wurde. Bei der ersten Überprüfung der NIS-Richtlinie wurde jedoch auf eine Reihe inhärenter Mängel hingewiesen, die letztlich zu erheblichen Unterschieden zwischen den Mitgliedstaaten in Bezug auf Kapazitäten, Planung und Schutzniveau geführt haben, was sich gleichzeitig auf die Wettbewerbsbedingungen für ähnliche Unternehmen im Binnenmarkt auswirkt.

Ein Tätigwerden der EU über die geltenden Maßnahmen der NIS-Richtlinie hinaus ist hauptsächlich durch folgende Faktoren gerechtfertigt: i) der grenzüberschreitende Charakter des Problems; ii) das Potenzial der EU-Maßnahmen zur Verbesserung und Förderung wirksamer nationaler Strategien; iii) der Beitrag konzertierter und kooperativer NIS-Politikmaßnahmen zum wirksamen Schutz des Datenschutzes und der Privatsphäre.

Die genannten Ziele können daher besser auf EU-Ebene als durch die Mitgliedstaaten allein erreicht werden.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Die NIS-Richtlinie ist das erste horizontale Binnenmarktinstrument, mit dem die Resilienz von Netzen und Systemen in der Union gegen Cybersicherheitsrisiken verbessert werden soll. Seit ihrem Inkrafttreten im Jahr 2016 hat sie bereits erheblich zur Anhebung des gemeinsamen Cybersicherheitsniveaus in den Mitgliedstaaten beigetragen. Die Überprüfung der Funktionsweise und Umsetzung der Richtlinie hat jedoch eine Reihe von Mängeln ergeben, die neben der zunehmenden Digitalisierung und der Notwendigkeit einer aktuelleren Reaktion in einem überarbeiteten Rechtsakt angegangen werden müssen.

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

Der neue Vorschlag steht voll und ganz im Einklang mit anderen einschlägigen Initiativen wie dem Vorschlag für eine Verordnung über die digitale Betriebsstabilität digitaler Systeme des

Finanzsektors (DORA) und dem Vorschlag für eine Richtlinie über die Resilienz kritischer Betreiber wesentlicher Dienste. Sie steht auch im Einklang mit dem europäischen Kodex für die elektronische Kommunikation, der Datenschutz-Grundverordnung und der eIDAS-Verordnung.

Der Vorschlag ist ein wesentlicher Bestandteil der EU-Strategie für die Sicherheitsunion.

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

Die Verwaltung dieser Aufgaben durch die ENISA erfordert spezifische Profile und bringt zusätzliche Arbeitsbelastung, die ohne Personalaufstockung nicht absorbiert werden können.

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

☐ **befristete Laufzeit**

– ☐ Laufzeit des Vorschlags/der Initiative: [TT.MM.]JJJJ bis [TT.MM.]JJJJ

– ☐ Finanzielle Auswirkungen von JJJJ bis JJJJ

☒ **unbefristete Laufzeit**

– Anlaufphase von 2022 bis 2025,

– anschließend reguläre Umsetzung.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[57]

☒ **Direkte Mittelverwaltung** durch die Kommission

durch

– ☐ Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

☐**X Indirekte Mittelverwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

☐ die EIB und den Europäischen Investitionsfonds

☒ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

☐ öffentlich-rechtliche Körperschaften

☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende finanzielle Garantien bieten

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

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

Bemerkungen

Die Agentur der Europäischen Union für Cybersicherheit (ENISA), die durch den Rechtsakt zur Cybersicherheit ein neues ständiges Mandat erhalten hat, würde die Mitgliedstaaten und die Kommission bei der Umsetzung der überarbeiteten NIS-Richtlinie unterstützen.

Infolge der überarbeiteten NIS-Richtlinie wird die ENISA ab 2022/23 über zusätzliche Handlungsbereiche verfügen. Diese Handlungsbereiche werden zwar durch die allgemeinen Aufgaben der ENISA gemäß ihrem Mandat abgedeckt, sie führen jedoch zu einer zusätzlichen Arbeitsbelastung für die Agentur. Genauer gesagt soll die ENISA gemäß dem Vorschlag der Kommission für eine überarbeitete NIS-Richtlinie neben ihren derzeitigen Handlungsbereichen auch die folgenden Maßnahmen in ihr Arbeitsprogramm aufnehmen: i) Entwicklung und Pflege eines europäischen

[57] Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Schwachstellenregisters (Artikel 6 Absatz 2 des Vorschlags), ii) Bereitstellung des Sekretariats des Europäischen Netzes der Verbindungsorganisationen für Cyberkrisen (CyCLONe) (Artikel 14 des Vorschlags) und Herausgabe eines jährlichen Berichts über den Stand der Cybersicherheit in der EU (Artikel 15 des Vorschlags), iii) Unterstützung der Durchführung von Peer Reviews zwischen den Mitgliedstaaten (Artikel 16 des Vorschlags), iv) Erhebung aggregierter Daten über Sicherheitsvorfälle in den Mitgliedstaaten und Bereitstellung technischer Orientierungshilfen (Artikel 20 Absatz 9 des Vorschlags) sowie Pflege eines Verzeichnisses der Einrichtungen, die grenzüberschreitende Dienste erbringen (Artikel 25 des Vorschlags).

Daher werden ab 2022 fünf zusätzliche VZÄ mit den entsprechenden Haushaltsmitteln in Höhe von etwa 0,61 Mio. EUR pro Jahr beantragt, um diese neuen Stellen abzudecken.

2. VERWALTUNGSMASSNAHMEN

2.1. Überwachung und Berichterstattung

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

Die Kommission wird die Anwendung der Richtlinie regelmäßig überprüfen und dem Europäischen Parlament und dem Rat erstmals drei Jahre nach ihrem Inkrafttreten Bericht erstatten.

Darüber hinaus wird die Kommission die ordnungsgemäße Umsetzung der Richtlinie durch die Mitgliedstaaten bewerten.

Die Überwachung und Berichterstattung über den Vorschlag erfolgt nach den Grundsätzen des ständigen Mandats der ENISA gemäß der VERORDNUNG (EU) 2019/881 (Rechtsakt zur Cybersicherheit).

Die Datenquellen für die geplante Überwachung würden hauptsächlich von der ENISA, der Kooperationsgruppe, dem CSIRT-Netzwerk und den Behörden der Mitgliedstaaten stammen. Neben den Daten aus den Berichten (einschließlich der jährlichen Tätigkeitsberichte) der ENISA, der Kooperationsgruppe und des CSIRT-Netzwerks könnten bei Bedarf spezifische Instrumente zur Datenerhebung eingesetzt werden (z. B. Umfragen bei nationalen Behörden, Eurobarometer, Berichte aus der Kampagne zum Monat der Cybersicherheit und europaweite Überprüfungen).

2.2. Verwaltungs- und Kontrollsystem(e)

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

Das für diesen Politikbereich zuständige Referat der GD CNECT wird die Umsetzung der Richtlinie verwalten.

In Bezug auf die Verwaltung der ENISA enthält Artikel 15 des Rechtsakts zur Cybersicherheit eine detaillierte Liste der Kontrollfunktionen des Verwaltungsrats der ENISA.

Gemäß Artikel 31 des Rechtsakts zur Cybersicherheit ist der Exekutivdirektor der ENISA für die Ausführung des Haushaltsplans der ENISA zuständig, und der Interne Prüfer der Kommission übt gegenüber der ENISA dieselben Befugnisse aus wie gegenüber den Kommissionsdienststellen. Der Verwaltungsrat der ENISA gibt eine Stellungnahme zum endgültigen Jahresabschluss der ENISA ab.

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

Sehr geringes Risiko, da das Ökosystem der NIS-Richtlinie bereits besteht und bereits die ENISA umfasst, die seit dem Inkrafttreten des Rechtsakts zur Cybersicherheit im Jahr 2019 über ein ständiges Mandat verfügt.

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

Die beantragte Mittelaufstockung betrifft Titel 1 und dient der Finanzierung der Gehälter. Dies bedeutet ein sehr geringes Fehlerrisiko auf der Ebene der Zahlungen.

2.3. Prävention von Betrug und Unregelmäßigkeiten

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

Die Präventions- und Schutzmaßnahmen der ENISA finden insbesondere in folgenden Fällen Anwendung:

- Zahlungen für die angeforderten Dienstleistungen oder Studien werden von den Bediensteten der Agentur vor der Zahlung unter Berücksichtigung etwaiger vertraglicher Verpflichtungen, wirtschaftlicher Grundsätze und einer guten Finanz- oder Verwaltungspraxis überprüft. In alle Vereinbarungen und Verträge zwischen der Agentur und den Zahlungsempfängern werden Bestimmungen zur Betrugsbekämpfung (Überwachung, Verpflichtung zur Berichterstattung usw.) aufgenommen.

- Zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen finden die Bestimmungen der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 25. Mai 1999 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) uneingeschränkt Anwendung.

- Gemäß Artikel 33 CSA trat die ENISA am 28. Dezember 2019 der Interinstitutionellen Vereinbarung vom 25. Mai 1999 zwischen dem Europäischen Parlament und dem Rat der Europäischen Union und der Kommission der Europäischen Gemeinschaften über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei. Die ENISA erlässt unverzüglich die entsprechenden Bestimmungen, die für alle Mitarbeiter der Agentur gelten.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

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

- Bestehende Haushaltslinien

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

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer	GM/NGM [58]	von EFTA-Ländern[59]	von Kandidatenländern[60]	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
2	02 10 04	./NGM	JA	NEIN	NEIN	/NEIN

- Neu zu schaffende Haushaltslinien

[58] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.
[59] EFTA: Europäische Freihandelsassoziation.
[60] Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

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

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer	GM/NGM	von EFTA-Ländern	von Kandidatenländern	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
	[XX.YY.YY.YY]		JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.2.1. Übersicht über die geschätzten Auswirkungen auf die Ausgaben

in Mio. EUR (3 Dezimalstellen)

Rubrik des Mehrjährigen Finanzrahmens	Nummer	[Rubrik…2 Binnenmarkt, Innovation und Digitales……..……]

[Einrichtung]: <... ENISA.... >			Jahr **N**[61] **2022**	Jahr **N+1** **2023**	Jahr **N+2** **2024**	Jahr **N+3** **2025**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen. **= 2026 + 2027**			**INSGESAMT**
Titel 1:	Verpflichtungen	1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Zahlungen	2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Titel 2:	Verpflichtungen	1a)								
	Zahlungen	2 a)								
Titel 3:	Verpflichtungen	3 a)								
	Zahlungen	3b)								
Mittelzuweisung INSGESAMT für [Einrichtung] <ENISA…….>	Verpflichtungen	=1+1a +3a	0,61	0,61	O.61.	0,61	0,61	0,61		**3,66**
	Zahlungen	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

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

Rubrik des Mehrjährigen Finanzrahmens	**5**	Verwaltungsausgaben

in Mio. EUR (3 Dezimalstellen)

		Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			**INSGESAMT**
GD: <…….>									
•Personal									
•Sonstige Verwaltungsausgaben									
GD INSGESAMT <…….>	Mittel								

Mittel INSGESAMT unter RUBRIK 5 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)								

in Mio. EUR (3 Dezimalstellen)

		Jahr **N**[62] **2022**	Jahr **N+1** **2023**	Jahr **N+2** **2024**	Jahr **N+3** **2025**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen. **2026 + 2027**			**INSGESAMT**
Mittel INSGESAMT unter den RUBRIKEN 1 bis 5 des Mehrjährigen Finanzrahmens	Verpflichtungen	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Zahlungen	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

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

3.2.2. Geschätzte Auswirkungen auf die Mittel [der Einrichtung]

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

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

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse angeben ⇩			Jahr **N**		Jahr **N+1**		Jahr **N+2**		Jahr **N+3**		Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.						**INSGESAMT**	
	ERGEBNISSE																	
	Art[63]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[64]…																		
- Ergebnis																		
- Ergebnis																		
- Ergebnis																		
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2 ...																		
- Ergebnis																		
Zwischensumme für Einzelziel Nr. 2																		
GESAMTKOSTEN																		

63 Ergebnisse sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer).

64 Wie unter 1.4.2. („Einzelziel(e)…“) beschrieben.

3.2.3. Geschätzte Auswirkungen auf die Humanressourcen der ENISA

3.2.3.1. Übersicht

Infolge der überarbeiteten NIS-Richtlinie wird die ENISA ab 2022/23 über zusätzliche Aufgaben verfügen. Diese Aufgaben werden durch das Mandat der ENISA abgedeckt, sie führen zu einer zusätzlichen Arbeitsbelastung für die Agentur. Genauer gesagt wird die ENISA zusätzlich zu ihren derzeitigen Aufgaben im Rahmen des Vorschlags der Kommission für eine überarbeitete NIS-Richtlinie unter anderem beauftragt werden, i) ein europäisches Schwachstellenregister zu entwickeln und zu führen (Artikel 6 Absatz 2 des Vorschlags), ii) das Sekretariat des Europäischen Netzes der Verbindungsorganisationen für Cyberkrisen (CyCLONe) bereitzustellen (Artikel 14 des Vorschlags) und einen jährlichen Bericht über den Stand der Cybersicherheit in der EU herauszugeben (Artikel 15 des Vorschlags), iii) die Durchführung von Peer Reviews zwischen den Mitgliedstaaten zu unterstützen (Artikel 16 des Vorschlags), iv) aggregierte Daten über Sicherheitsvorfälle in den Mitgliedstaaten zu erheben und technische Leitlinien bereitzustellen (Artikel 20 Absatz 9 des Vorschlags) sowie ein Verzeichnis der Einrichtungen, die grenzüberschreitende Dienste erbringen, aufzustellen und zu pflegen (Artikel 25 des Vorschlags).

Daher werden ab 2022 fünf zusätzliche VZÄ mit den entsprechenden Haushaltsmitteln beantragt, um diese neuen Stellen abzudecken.

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

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

in Mio. EUR (3 Dezimalstellen)

	Jahr **N**[65] **2022**	Jahr **N+1** **2023**	Jahr **N+2** **2024**	Jahr **N+3** **2025**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen. **2026 + 2027**			**INSGESAMT**
Bedienstete auf Zeit (Funktionsgruppe AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Bedienstete auf Zeit (Funktionsgruppe A ST)								
Vertragsbedienstete	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Abgeordnete nationale Sachverständige								

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

INSGESAMT	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Personalbedarf (VZÄ):

	Jahr **N**[66] **2022**	Jahr **N+1** **2023**	Jahr **N+2** **2024**	Jahr **N+3** **2025**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen. **2026 + 2027**			**INSGESAMT**
Bedienstete auf Zeit (Funktionsgruppe AD)	3	3	3	3	3	3		**18**
Bedienstete auf Zeit (Funktionsgruppe A ST)								
Vertragsbedienstete	2	2	2	2	2	2		**12**
Abgeordnete nationale Sachverständige								

INSGESAMT	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Geschätzter Personalbedarf bei der übergeordneten GD

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

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

Schätzung in ganzzahligen Werten (oder mit höchstens einer Dezimalstelle)

	Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
• **Planstellen (Beamte und Bedienstete auf Zeit)**							
XX 01 01 01 (am Sitz und in den Vertretungen der Kommission)							
XX 01 01 02 (in den Delegationen)							

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

XX 01 05 01 (indirekte Forschung)								
10 01 05 01 (direkte Forschung)								
• Externes Personal (in Vollzeitäquivalenten – VZÄ)[67]								
XX 01 02 01 (VB, ANS und LAK der Globaldotation)								
XX 01 02 02 (VB, ÖB, ANS, LAK und JFD in den Delegationen)								
XX 01 04 ***jj***[68]	- am Sitz[69]							
	- in den Delegationen							
XX 01 05 02 (VB, ANS und LAK – indirekte Forschung)								
10 01 05 02 (VB, ANS und LAK – direkte Forschung)								
Sonstige Haushaltslinien (bitte angeben)								
INSGESAMT								

XX steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

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

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	
Externes Personal	

Einzelheiten der Kostenberechnung für die Vollzeitäquivalente sind im Anhang V in Abschnitt 3 anzugeben.

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

68 Teilobergrenze für aus operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

69 Insbesondere für die Strukturfonds, den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) und den Europäischen Fischereifonds (EFF).

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

– ☐X Der Vorschlag/Die Initiative ist mit dem Mehrjährigen Finanzrahmen vereinbar.

– ☐ Der Vorschlag/Die Initiative erfordert eine Neuprogrammierung der betreffenden Rubrik des Mehrjährigen Finanzrahmens.

Bitte erläutern Sie die erforderliche Neuprogrammierung unter Angabe der betreffenden Haushaltslinien und der entsprechenden Beträge. Der Vorschlag ist mit dem MFR 21/27 vereinbar. Der Ausgleich der für die Aufstockung der Personalressourcen in der ENISA beantragten Haushaltsmittel erfolgt durch eine Kürzung der Mittel für das Programm „Digitales Europa“ (DEP) in derselben Rubrik um den gleichen Betrag.

– ☐ Der Vorschlag/Die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Revision des Mehrjährigen Finanzrahmens[70].

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

3.2.5. Finanzierungsbeteiligung Dritter

– Der Vorschlag/die Initiative sieht keine Kofinanzierung durch Dritte vor.

– Der Vorschlag/die Initiative sieht folgende Kofinanzierung durch Dritte vor:

in Mio. EUR (3 Dezimalstellen)

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

[70] Siehe Artikel 11 und 17 der Verordnung (EU, Euratom) Nr. 1311/2013 des Rates zur Festlegung des mehrjährigen Finanzrahmens für die Jahre 2014–2020.

3.3. Geschätzte Auswirkungen auf die Einnahmen

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

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

☐ auf die Eigenmittel

☐ auf die übrigen Einnahmen

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

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[71]						
		Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
Artikel ….								

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

Bitte geben Sie an, wie die Auswirkungen auf die Einnahmen berechnet werden.

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