EUROPÄISCHE
KOMMISSION

Brüssel, den 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

{SWD(2022) 67 final} - {SWD(2022) 68 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Mit diesem Vorschlag wird ein Rahmen für die Gewährleistung gemeinsamer Cybersicherheitsvorschriften und -maßnahmen der Organe, Einrichtungen und sonstigen Stellen der Union geschaffen. Er zielt darauf ab, die Resilienz aller Einrichtungen und ihre Kapazitäten zur Reaktion auf Sicherheitsvorfälle weiter zu verbessern. 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. Darüber hinaus ist die Gewährleistung einer sicheren und resilienten öffentlichen Verwaltung ein Eckpfeiler des digitalen Wandels der Gesellschaft insgesamt.

Dieser Vorschlag beruht auf der EU-Strategie für eine Sicherheitsunion (COM(2020) 605 final) und auf der Cybersicherheitsstrategie der EU für die digitale Dekade (JOIN(2020) 18 final).

Angesichts der veränderten und vermehrten Digitalisierung der Organe, Einrichtungen und sonstigen Stellen in den letzten Jahren und der sich wandelnden Bedrohungslandschaft im Bereich der Cybersicherheit wird mit dem Vorschlag der bestehende Rechtsrahmen des CERT-EU modernisiert. Beide Entwicklungen haben seit Beginn der COVID-19-Krise noch an Intensität gewonnen, wobei die Zahl der Sicherheitsvorfälle weiter steigt und immer ausgefeiltere Angriffe aus einer Vielzahl von Quellen kommen.

Mit dem Vorschlag wird das CERT-EU von „Reaktionsteam für IT-Sicherheitsvorfälle (Computer Emergency Response Team - CERT) umbenannt in „Cybersicherheitszentrum“ für die Organe, Einrichtungen und sonstigen Stellen der Union, was im Einklang mit den Entwicklungen in den Mitgliedstaaten und weltweit steht, wo viele CERTs in Cybersicherheitszentren umbenannt werden, die Kurzbezeichnung „CERT-EU“ wird jedoch aufgrund ihres Wiedererkennungswerts beibehalten.

• Kohärenz mit den bestehenden Vorschriften in diesem Bereich

Dieser Vorschlag zielt darauf ab, die Resilienz der Organe, Einrichtungen und sonstigen Stellen der Union im Bereich der Cybersicherheit gegen Cyberbedrohungen zu erhöhen und zugleich an die bestehenden Rechtsvorschriften – die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netzen und Informationssystemen in der Union – anzupassen.

- Er entspricht auch dem Vorschlag für eine Richtlinie (EU) XXXX/XXXX über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 [NIS-2-Vorschlag].
- Verordnung (EU) 2019/881 über die Agentur der Europäischen Union für Cybersicherheit und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit)
- Vorschlag für eine Verordnung (EU) XXXX/XXXX über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union
- Empfehlung der Kommission vom 23. Juni 2021 zum Aufbau einer gemeinsamen Cyber-Einheit
- Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen

Im Anhang der Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen wird das Konzept für eine koordinierte Reaktion auf große grenzüberschreitende Cybersicherheitsvorfälle und -krisen dargelegt.

In seiner Entschließung vom 9. März 2021 betonte der Rat der Europäischen Union, dass Cybersicherheit und das globale und offene Internet für das Funktionieren der öffentlichen Verwaltung und der öffentlichen Institutionen sowohl auf nationaler als auch auf EU-Ebene sowie für unsere Gesellschaft und die Wirtschaft insgesamt von entscheidender Bedeutung sind, und hob hervor, wie wichtig ein robuster und kohärenter Sicherheitsrahmen ist, um alle Mitarbeiter, Daten, Kommunikationsnetze und Informationssysteme der EU sowie Entscheidungsprozesse zu schützen. Dies soll demnach insbesondere durch die Stärkung der Abwehrfähigkeit und die Verbesserung der Sicherheitskultur der Organe, Einrichtungen und sonstigen Stellen der Union erreicht werden. Hierfür müssen ausreichende Ressourcen und Fähigkeiten, auch im Zusammenhang mit der Stärkung des Mandats des CERT-EU bereitgestellt werden.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Die Rechtsgrundlage für diese Verordnung ist Artikel 298 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der vorsieht, dass sich die Organe, Einrichtungen und sonstigen Stellen der Union zur Ausübung ihrer Aufgaben auf eine offene, effiziente und unabhängige europäische Verwaltung stützen. Die Bestimmungen zu diesem Zweck werden unter Beachtung des Statuts und der Beschäftigungsbedingungen nach Artikel 336 vom Europäischen Parlament und vom Rat gemäß dem ordentlichen Gesetzgebungsverfahren durch Verordnungen erlassen.

Die Informationstechnologie hat für die Organe, Einrichtungen und sonstigen Stellen der Union neue Möglichkeiten der Zusammenarbeit, der Interaktion mit den Bürgerinnen und Bürgern und zur Verbesserung der allgemeinen Abläufe geschaffen. Während sich die Technologie ständig weiterentwickelt, entwickelt sich gleichzeitig auch die Cyberbedrohungslandschaft weiter. Die Organe, Einrichtungen und sonstigen Stellen der Union sind zu äußerst attraktiven Zielen ausgefeilter Cyberangriffe geworden. Die Einrichtung von Systemen zur Gewährleistung der Cybersicherheit und die Festlegung entsprechender Anforderungen dürfte zur Effizienz und Unabhängigkeit der europäischen Verwaltung beitragen, sodass die Organe, Einrichtungen und sonstigen Stellen der Union bei der Wahrnehmung ihrer Aufgaben in einer digitalen Welt effizienter arbeiten können.

Darüber hinaus stellen, wie in Abschnitt 3 erläutert, die derzeit unterschiedlichen Reifegrade, die in den Organen, Einrichtungen und sonstigen Stellen der Union in Bezug auf den Cybersicherheitsstand und die Konzepte in Fragen der Cybersicherheit bestehen, weitere Hindernisse für eine offene, effiziente und unabhängige europäische Verwaltung dar. Ohne einen gemeinsamen Ansatz würde sich der Cybersicherheitsstand der Organe, Einrichtungen und sonstigen Stellen der Union weiterhin in unterschiedliche Richtungen entwickeln. Diese Rechtsgrundlage ist daher angemessen, da mit der Verordnung ein gemeinsamer Rechtsrahmen für die Cybersicherheit innerhalb der Organe, Einrichtungen und sonstigen Stellen der Union geschaffen werden soll.

- **Subsidiarität**

Die Verordnung zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union fällt in die ausschließliche Zuständigkeit der Union.

- **Verhältnismäßigkeit**

Die in dieser Verordnung vorgeschlagenen Regeln gehen nicht über das für die zufriedenstellende Verwirklichung der spezifischen Ziele erforderliche Maß hinaus. Die geplanten Maßnahmen werden dazu beitragen, ein hohes gemeinsames Cybersicherheitsniveau zu erreichen, ohne über das hinauszugehen, was angesichts der zunehmend hohen Risiken, denen sie ausgesetzt sind, zum Erreichen des verfolgten Ziels erforderlich ist.

- **Wahl des Instruments**

Die Wahl einer Verordnung, die unmittelbar gilt, wird als geeignetes Rechtsinstrument angesehen, um die Verpflichtungen der Organe, Einrichtungen und sonstigen Stellen der Union festzulegen und zu optimieren. Um gezielte Verbesserungen zu ermöglichen, ist eine Verordnung das am besten geeignete Rechtsinstrument.

3. ERGEBNISSE DER EX-ANTE-BEWERTUNGEN, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Ex-ante-Bewertungen**

Das CERT-EU hat eine Bewertung der wichtigsten Cyberbedrohungen durchgeführt, denen die Organe, Einrichtungen und sonstigen Stellen der Union derzeit ausgesetzt sind oder in absehbarer Zeit voraussichtlich ausgesetzt sein werden.

Bei der Analyse wurden drei Kategorien von Beobachtungen herangezogen:

- Versuche, die IT-Infrastruktur der Organe, Einrichtungen und sonstigen Stellen der Union zu verletzen (sind die Versuche erfolgreich, werden sie als Sicherheitsvorfälle behandelt, in den anderen Fällen werden sie als festgestellte Versuche erfasst),
- Bedrohungen, die im Umfeld der Organe, Einrichtungen und sonstigen Stellen der Union festgestellt werden (z. B. in mit ihnen verbundenen Sektoren, bei ihren Interessengruppen oder in Europa),
- die wichtigsten weltweit beobachteten Bedrohungstendenzen.

Darüber hinaus wurde in der Analyse untersucht, wie sich größere aktuelle Veränderungen auf die Art und Weise auswirken, in der die Organe der Union ihre IT-Infrastrukturen und -Dienste verwalten und nutzen. Hierzu zählen unter anderem:

- Zunahme der Telearbeit,
- Migration der Systeme in die Cloud,
- Zunehmende Auslagerung von IT-Diensten.

Zwischen 2019 und 2021 ist bei den Organen, Einrichtungen und sonstigen Stellen der Union die Zahl der erheblichen Sicherheitsvorfälle[1], die von Verursachern ausgingen, die als „fortgeschrittene andauernde Bedrohung“ (Advanced Persistent Threat, APT) eingestuft wurden, dramatisch gestiegen. Im ersten Halbjahr 2021 gab es so viele erhebliche Sicherheitsvorfälle wie im gesamten Jahr 2020. Dies spiegelt sich auch in der Zahl der 2020 vom CERT-EU analysierten forensischen Abbilder (Momentaufnahmen der betroffenen Systeme oder Geräte) wider, die sich im Vergleich zu 2019 mehr als verdreifacht hat, während die Zahl der erheblichen Sicherheitsvorfälle seit 2018 sogar um mehr als das Zehnfache gestiegen ist.

Im Jahr 2020 legte der Lenkungsausschuss des CERT-EU ein neues strategisches Ziel für das CERT-EU fest, um für alle Organe, Einrichtungen und sonstigen Stellen ein umfassendes Cyberabwehrniveau angemessener Breite und Tiefe zu gewährleisten und eine kontinuierliche Anpassung an aktuelle oder sich abzeichnende Bedrohungen, einschließlich Angriffen auf mobile Geräte, Cloud-Umgebungen und Geräte des Internets der Dinge, zu ermöglichen.

Ergänzend zur Bedrohungsanalyse des CERT-EU hat die Kommission eine Evaluierung der Funktionsweise von 20 Organen, Einrichtungen und sonstigen Stellen der Union im Bereich der Cybersicherheit vorgenommen. Dies hat Einblicke in die etablierten Cybersicherheitspraktiken und die Kapazitäten für das Cybersicherheitsmanagement unter Rückgriff auf externes Benchmarking bei einigen technischen Sicherheitskontrollen geliefert.

Diese Evaluierung stützte sich auf Fragebögen, die von diesen Organen, Einrichtungen und Agenturen beantwortet wurden, auf öffentlich zugängliche Daten und auf von den Organen, Einrichtungen und sonstigen Stellen der Union selbst bereitgestellte Daten. Sie liefert ausreichende Einblicke in die derzeitige Situation, um zu folgendem Schluss zu gelangen:

- In Bezug auf die Cybersicherheitsreife sowie auf Größe und Umfang der IT-Infrastruktur gibt es zwischen den Organen, Einrichtungen und sonstigen Stellen der Union, die evaluiert wurden, erhebliche Unterschiede.
- Während viele Organe, Einrichtungen und Agenturen der Union insgesamt über ausgereifte Erkennungs- und Reaktionsfähigkeiten verfügen, gibt es im Rahmen ihrer Cybersicherheits-Governancekapazitäten Unterschiede beim Niveau des integrierten Risikomanagements.
- Während die Cybersicherheitsrahmen (Strategie, Politik und grundlegende Vorschriften) der in der Evaluierung berücksichtigten Organe, Einrichtungen und sonstigen Stellen der Union in den Schlüsselbereichen der Cybersicherheit, die in Anhang I der Verordnung aufgeführt sind, im Allgemeinen gut etabliert sind, ist in einigen Organen, Einrichtungen und sonstigen Stellen der Union kein ausgereiftes Betriebskontinuitätsmanagement vorhanden und es wurden Mängel in Bezug auf die Einhaltung der Vorschriften, die Prüfung und die kontinuierliche Verbesserung erkannt.
- Zudem wurde festgestellt, dass technische Maßnahmen, die als bewährte Verfahren gelten, von den evaluierten Organen, Einrichtungen und sonstigen Stellen der Union uneinheitlich angewandt werden.

[1] „Erheblicher Sicherheitsvorfall“ bezeichnet jeden Sicherheitsvorfall mit Ausnahme derjenigen, die begrenzte Auswirkungen haben und deren Methoden oder Technologien wahrscheinlich bereits bekannt sind.

Zusammenfassend geht aus der Analyse der 20 Organe, Einrichtungen und sonstigen Stellen der Union hervor, dass es in Bezug auf Governance und Cyberhygiene sowie auf die Fähigkeiten und den Reifegrad breit gefächerte Unterschiede gibt. Daher ist es von entscheidender Bedeutung, alle Organe, Einrichtungen und sonstigen Stellen der Union dazu zu verpflichten, gewisse grundlegende Cybersicherheitsmaßnahmen umzusetzen, um diese Unterschiede bei den Reifegraden auszuräumen und alle Organe, Einrichtungen und sonstigen Stellen der Union auf ein hohes gemeinsames Cybersicherheitsniveau zu bringen.

Bislang gibt es keine Rechtsvorschriften der Union, bei denen die Cybersicherheit der Organe, Einrichtungen und sonstigen Stellen der Union im Mittelpunkt steht und mit denen die Bedrohungslage im Bereich der Cybersicherheit und die durch die Digitalisierung entstehenden IT-Risiken umfassend angegangen werden.

- **Konsultation der Interessenträger**

Die Kommission hat Interessenträger aus allen Organen, Einrichtungen und sonstigen Stellen der Union sowie Vertreter der Mitgliedstaaten im Rat und Interessenträger im Europäischen Parlament konsultiert. Am 25. Juni 2021 nahmen Vertreter der Mitgliedstaaten und einschlägige Akteure aus den Organen, Einrichtungen und sonstigen Stellen der Union an einem von der Kommission organisierten Workshop teil, um den Inhalt des künftigen Verordnungsvorschlags zu erörtern.

- **Folgenabschätzung**

Der vorliegende Vorschlag wird sich auf die Organe, Einrichtungen und sonstigen Stellen der Union auswirken. Eine spezifische Folgenabschätzung erübrigt sich, da er nicht für die Mitgliedstaaten gelten wird.

- **Grundrechte**

Die Europäische Union setzt alles daran, hohe Standards für den Schutz der Grundrechte zu gewährleisten. Der gesamte Informationsaustausch auf der Grundlage dieser Verordnung fände in vertrauenswürdiger Umgebung unter uneingeschränkter Achtung des Rechts auf den Schutz personenbezogener Daten gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union und der einschlägigen Datenschutzvorschriften, insbesondere der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates, statt.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Aus Marktbenchmarks und -studien geht hervor, dass die direkten Ausgaben für Cybersicherheit in der Regel zwischen 4 % und 7 % der aggregierten IT-Ausgaben von Organisationen schwanken[2]. Die vom CERT-EU zur Unterstützung dieses Legislativvorschlags durchgeführte Bedrohungsanalyse zeigt jedoch, dass internationale Einrichtungen und politische Organisationen mit erhöhten Risiken konfrontiert sind, und daher für Cybersicherheitsausgaben ein Niveau von 10 % der gesamten IT-Ausgaben angemessener erscheint. Da keine ausreichend detaillierten Informationen zu den IT-Ausgaben der Organe, Einrichtungen und sonstigen Stellen der Union und dem jeweiligen

[2] Quelle: Gartner, „Identifying the Real Information Security Budget“ (2016). Diese kommen zu den indirekten Ausgaben für IT-Sicherheit hinzu, beispielweise den Ausgaben für die Netzsicherheit wie Firewalls, Virenschutzprogramme und die vom Systemeigentümer zu erfüllenden Aufgaben wie Risikobewertung und Durchführung von Sicherheitskontrollen. In einer Veröffentlichung aus dem Jahr 2020 werden die Ausgaben für Cybersicherheit bei Finanzinstituten auf 10–11 % der IT-Ausgaben geschätzt, Quelle: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

Anteil der Ausgaben für Cybersicherheit vorliegen, können die genauen Kosten für diese Maßnahmen nicht bestimmt werden.

Auch wenn es daher wahrscheinlich ist, dass viele Organe, Einrichtungen und Agenturen der Union derzeit weniger für Cybersicherheit ausgeben, als sie es tun sollten, wird diese Verordnung als solche nicht zu einem Anstieg der entsprechenden laufenden Ausgaben führen. Auch ohne die Verordnung müssten alle diese Stellen ein angemessenes Cybersicherheitsniveau gewährleisten. Die Verordnung sieht die Fortsetzung der bisherigen Zusammenarbeit im Lenkungsausschuss des CERT-EU vor und formalisiert eine zum Teil bereits bestehende Ebene des Informationsaustauschs. Wie im Finanzbogen zu Rechtsakten dargelegt, wird das CERT-EU zusätzliche Ressourcen benötigen, um seine erweiterte Rolle zu erfüllen, und diese Ressourcen sollten von den Organen, Einrichtungen und sonstigen Stellen der Union, die die Dienste des CERT-EU in Anspruch nehmen, umgeschichtet werden.

5. WEITERE ANGABEN

- **Durchführungs-, Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Der Interinstitutionelle Cybersicherheitsbeirat (IICB) sollte mit Unterstützung des CERT-EU die Funktionsweise dieser Verordnung überprüfen, Bewertungen durchführen und der Kommission einen Bericht mit seinen Ergebnissen vorlegen. Die Kommission sollte dem Europäischen Parlament, dem Rat, dem Europäischen Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen regelmäßig Bericht erstatten.

Das CERT-EU kann Vorschläge für Leitlinien oder Empfehlungen ausarbeiten, über deren Annahme der IICB beschließen kann. Leitlinien dienen als Orientierungshilfe für alle Organe, Einrichtungen und sonstigen Stellen der Union oder für eine Untergruppe von ihnen, während sich Empfehlungen an einzelne Organe, Einrichtungen und sonstige Stellen der Union richten. Bei einem Aufruf zum Tätigwerden handelt es sich um eine Orientierungshilfe des CERT-EU, in dem dringende Sicherheitsmaßnahmen beschrieben werden, zu deren Ergreifung innerhalb einer vorgegebenen Frist die Organe, Einrichtungen und sonstigen Stellen der Union dringend aufgefordert werden.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Allgemeine Bestimmungen

In der Verordnung werden Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus festgelegt und sie gilt für die Organe, Einrichtungen und sonstigen Stellen der Union, damit sie ihre jeweiligen Aufgaben offen, wirksam und unabhängig wahrnehmen können. (Artikel 1-3, 23-25)

Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau

Die Organe, Einrichtungen und sonstigen Stellen der Union sind verpflichtet, einen internen Rahmen für Risikomanagement, Governance und Kontrolle im Bereich der Cybersicherheit einzurichten, der ein wirksames und umsichtiges Management aller Cybersicherheitsrisiken gewährleistet. Darüber hinaus legen die Organe, Einrichtungen und sonstigen Stellen Cybersicherheitsgrundregeln fest, um den im Wege des Rahmens ermittelten Risiken zu begegnen, führen regelmäßige Bewertungen des Cybersicherheitsreifegrads durch und nehmen einen Cybersicherheitsplan an. (Artikel 4-8)

Interinstitutioneller Cybersicherheitsbeirat

Der Interinstitutionelle Cybersicherheitsbeirat wird eingerichtet und ist zuständig für die Überwachung der Durchführung dieser Verordnung durch die Organe, Einrichtungen und

sonstigen Stellen der Union sowie für die Beaufsichtigung der Umsetzung der allgemeinen Prioritäten und Ziele durch das CERT-EU und die strategische Leitung des CERT-EU. (Artikel 9-11)

CERT-EU

Das CERT-EU trägt zur Sicherheit der IT-Umgebung aller Organe, Einrichtungen und sonstigen Stellen der Union bei, indem es diese berät, sie bei der Prävention, Erkennung, Abschwächung und Bewältigung von Sicherheitsvorfällen unterstützt und als zentrale Stelle für den Austausch von Informationen zur Cybersicherheit und die Koordinierung der Reaktion auf Sicherheitsvorfälle dient. (Artikel 12-17)

Zusammenarbeit und Berichterstattungspflichten

Die Verordnung gewährleistet die Zusammenarbeit zwischen dem CERT-EU und den Organen, Einrichtungen und sonstigen Stellen der Union und den Informationsaustausch unter ihnen zum Aufbau von Vertrauen. Zu diesem Zweck kann das CERT-EU die Organe, Einrichtungen und sonstigen Stellen der Union auffordern, ihm einschlägige Informationen zur Verfügung zu stellen, und es kann mit den Organen, Einrichtungen und sonstigen Stellen der Union sicherheitsspezifische Informationen austauschen, um die Erkennung ähnlicher Cyberbedrohungen oder -sicherheitsvorfälle ohne Einwilligung des betroffenen Konstituenten zu erleichtern. Das CERT-EU darf Informationen über spezifische Sicherheitsvorfälle, aus denen die Identität der Zielgruppe des Cybersicherheitsvorfalls hervorgeht, nur mit Einwilligung des betroffenen Konstituenten weitergeben.

Insbesondere müssen alle Organe, Einrichtungen und sonstigen Stellen dem CERT-EU erhebliche Cyberbedrohungen, erhebliche Sicherheitslücken und erhebliche Sicherheitsvorfälle unverzüglich melden, spätestens jedoch 24 Stunden nachdem sie von ihnen Kenntnis erlangt haben. (Artikel 18-22)

2022/0085 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 298,

gestützt auf den Vertrag zur Gründung der Europäischen Atomgemeinschaft, insbesondere auf Artikel 106a,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Im digitalen Zeitalter ist die Informations- und Kommunikationstechnik der Grundstein einer offenen, effizienten und unabhängigen Verwaltung der Union. Die Cybersicherheitsrisiken werden durch die Weiterentwicklung der Technologie und die zunehmende Komplexität und Vernetzung digitaler Systeme weiter verstärkt, wodurch die Verwaltung der Union anfälliger für Cyberbedrohungen und -sicherheitsvorfälle wird, die letztlich die Aufrechterhaltung des Dienstbetriebs und die Fähigkeit der Verwaltung zur Sicherung ihrer Daten gefährden können. Während die zunehmende Inanspruchnahme von Cloud-Diensten, die allgegenwärtige Nutzung von IT, eine hochgradige Digitalisierung, Telearbeit sowie die sich weiterentwickelnde Technologie und Konnektivität heute zentrale Merkmale aller Tätigkeiten der Verwaltungsstellen der Union sind, wird der digitalen Resilienz noch nicht ausreichend Rechnung getragen.

(2) Die Cyberbedrohungslandschaft, mit der die Organe, Einrichtungen und sonstigen Stellen der Union konfrontiert sind, entwickelt sich ständig weiter. Die Taktiken, Techniken und Verfahren, die von den Verursachern der Bedrohungen eingesetzt werden, entwickeln sich ständig weiter, während die wesentlichen Motive für solche Angriffe weitgehend unverändert bleiben – vom Diebstahl wertvoller vertraulicher Informationen über Gewinnerzielung Manipulation der öffentlichen Meinung bis hin zur Schwächung der digitalen Infrastruktur. Das Tempo, in dem die Verursacher ihre Cyberangriffe durchführen, nimmt weiter zu, während ihre Operationen zunehmend ausgefeilt und automatisiert und auf exponierte Angriffsflächen ausgerichtet sind, immer weiter expandieren und rasch Schwachstellen ausnutzen.

(3) Die IT-Umgebungen der Organe, Einrichtungen und sonstigen Stellen der Union sind von gegenseitigen Abhängigkeiten und integrierten Datenströmen gekennzeichnet und ihre Nutzer arbeiten eng zusammen. Wegen dieser Verflechtungen kann jede Störung, auch wenn sie anfänglich auf nur ein Organ, eine Einrichtung oder eine sonstige Stelle der Union beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und

lang anhaltende negative Auswirkungen auf die anderen Organe, Einrichtungen oder sonstigen Stellen haben können. Darüber hinaus sind die IT-Umgebungen bestimmter Organe, Einrichtungen und sonstiger Stellen mit den IT-Umgebungen der Mitgliedstaaten verbunden, was dazu führt, dass ein Sicherheitsvorfall in einer Einrichtung der Union ein Risiko für die Cybersicherheit der IT-Umgebungen der Mitgliedstaaten darstellt, und umgekehrt.

(4) Die Organe, Einrichtungen und sonstigen Stellen der Union sind attraktive Ziele, die sowohl mit hoch qualifizierten und gut ausgestatteten Angreifern als auch mit anderen Bedrohungen konfrontiert sind. Gleichzeitig gibt es in Bezug auf das Niveau und den Reifegrad der Cyberresilienz und die Fähigkeit, böswillige Cyberaktivitäten zu erkennen und darauf zu reagieren, erhebliche Unterschiede zwischen diesen Organen, Einrichtungen und Stellen. Für das Funktionieren der europäischen Verwaltung ist es daher erforderlich, dass die Organe, Einrichtungen und sonstigen Stellen der Union ein hohes gemeinsames Cybersicherheitsniveau erreichen, indem Cybersicherheitsgrundregeln (eine Reihe von Mindestvorschriften für die Cybersicherheit, denen Netz- und Informationssysteme und deren Betreiber und Nutzer entsprechen müssen, um Cybersicherheitsrisiken zu minimieren) festgelegt werden, sowie durch Informationsaustausch und Zusammenarbeit.

(5) Die Richtlinie [NIS-2-Vorschlag] über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union zielt darauf ab, die Cyberresilienz öffentlicher und privater Einrichtungen, der zuständigen nationalen Behörden und Einrichtungen sowie der Union insgesamt weiter zu verbessern und ihre Kapazitäten zur Reaktion auf Sicherheitsvorfälle zu stärken. Daher ist es notwendig, dass die Organe, Einrichtungen und sonstigen Stellen der Union sich dem anschließen, indem sie dafür sorgen dass die betreffenden Vorschriften mit der Richtlinie [NIS-2-Vorschlag] im Einklang stehen und deren ehrgeizige Ziele widerspiegeln.

(6) Um ein hohes gemeinsames Cybersicherheitsniveau zu erreichen, ist es erforderlich, dass jedes Organ, jede Einrichtung und jede sonstige Stelle der Union einen internen Rahmen für Risikomanagement, Governance und Kontrolle im Bereich der Cybersicherheit festlegt, der ein wirksames und umsichtiges Management aller Cybersicherheitsrisiken gewährleistet und die Sicherung der Betriebskontinuität und das Krisenmanagement berücksichtigt.

(7) Angesichts der Unterschiede zwischen den Organen, Einrichtungen und sonstigen Stellen der Union ist bei der Umsetzung Flexibilität erforderlich, da die Lösungen jeweils bedarfsgerecht zugeschnitten sein müssen. Die Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau sollten keine Verpflichtungen umfassen, die einen unmittelbaren Eingriff in die Wahrnehmung der Aufgaben der Organe, Einrichtungen und sonstigen Stellen der Union darstellen oder deren institutionelle Autonomie beeinträchtigen. Daher sollten diese Organe, Einrichtungen und sonstigen Stellen ihren eigenen Rahmen für das Risikomanagement, die Governance und die Kontrolle im Bereich der Cybersicherheit festlegen und ihre eigenen Cybersicherheitsgrundregeln und Cybersicherheitspläne annehmen.

(8) Damit keine unverhältnismäßige finanzielle und administrative Belastung für die Organe, Einrichtungen und sonstigen Stellen der Union entsteht, sollten die Anforderungen an das Cybersicherheitsrisikomanagement in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei ist dem neuesten Stand solcher Maßnahmen Rechnung zu tragen. Jedes Organ, jede Einrichtung und jede sonstige Stelle der Union

sollte bestrebt sein, einen angemessenen Prozentsatz seines bzw. ihres IT-Haushalts für die Verbesserung seines bzw. ihres Cybersicherheitsniveaus zuzuweisen; längerfristig sollte ein Ziel in der Größenordnung von 10 % angestrebt werden.

(9) Ein hohes gemeinsames Cybersicherheitsniveau setzt voraus, dass die Cybersicherheit der Aufsicht der höchsten Managementebene des jeweiligen Organs, der jeweiligen Einrichtung oder sonstigen Stelle der Union unterstellt wird, die Cybersicherheitsgrundregeln billigen sollte, um die Risiken anzugehen, die in dem jeweiligen von dem betreffenden Organ bzw. der betreffenden Einrichtung oder sonstigen Stelle festzulegenden Rahmen ermittelt werden. Die Pflege der Cybersicherheitskultur, d. h. die Cybersicherheit in der täglichen Praxis, ist Bestandteil der Cybersicherheitsgrundregeln in allen Organen, Einrichtungen und sonstigen Stellen der Union.

(10) Die Organe, Einrichtungen und sonstigen Stellen der Union sollten Risiken im Zusammenhang mit den Beziehungen zu Anbietern und Diensteanbietern, einschließlich Anbietern von Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten, bewerten und geeignete Maßnahmen ergreifen, um diese Risiken anzugehen. Diese Maßnahmen sollten Teil der Cybersicherheitsgrundregeln sein und in Leitlinien oder Empfehlungen des CERT-EU näher ausgeführt werden. Bei der Festlegung von Maßnahmen und der Ausarbeitung von Leitlinien sollten die einschlägigen Rechtsvorschriften und Strategien der EU, einschließlich der Risikobewertungen und Empfehlungen der NIS-Kooperationsgruppe, wie etwa die koordinierte Risikobewertung der EU und das EU-Instrumentarium für die 5G-Cybersicherheit, gebührend berücksichtigt werden. Darüber hinaus könnte die Zertifizierung relevanter IKT-Produkte, -Dienste und -Prozesse im Rahmen spezifischer EU-Systeme für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, vorgeschrieben werden.

(11) Im Mai 2011 beschlossen die Generalsekretäre der Organe und Einrichtungen der Union die Einsetzung eines Vorbereitungsteams für ein Reaktionsteam für IT-Sicherheitsvorfälle für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) unter der Aufsicht eines interinstitutionellen Lenkungsausschusses. Im Juli 2012 bestätigten die Generalsekretäre die praktischen Vorkehrungen und vereinbarten, das CERT-EU als ständige Einrichtung beizubehalten; als Beispiel für eine sichtbare interinstitutionelle Zusammenarbeit auf dem Gebiet der Cybersicherheit sollte es weiterhin zur Verbesserung der allgemeinen Sicherheit der IT-Systeme der Organe, Einrichtungen und sonstigen Stellen der Union beitragen. Im September 2012 wurde das CERT-EU als Taskforce der Europäischen Kommission mit einem interinstitutionellen Mandat eingerichtet. Im Dezember 2017 schlossen die Organe und Einrichtungen der Union eine interinstitutionelle Vereinbarung über die Organisation und den Betrieb des CERT-EU[3]. Diese Vereinbarung sollte laufend weiterentwickelt werden, um die Durchführung dieser Verordnung zu unterstützen.

(12) Das CERT-EU sollte von „Reaktionsteam für IT-Sicherheitsvorfälle (Computer Emergency Response Team – CERT) in „Cybersicherheitszentrum“ für die Organe, Einrichtungen und sonstigen Stellen der Union umbenannt werden, was im Einklang mit den Entwicklungen in den Mitgliedstaaten und weltweit steht, wo viele CERTs in

[3] ABl. C 12 vom 13.1.2018, S. 1.

Cybersicherheitszentren umbenannt werden; die Kurzbezeichnung „CERT-EU“ sollte jedoch aufgrund ihres Wiedererkennungswerts beibehalten werden.

(13) Viele Cyberangriffe sind Teil umfassenderer Operationen, die auf Gruppen von Organen, Einrichtungen und sonstigen Stellen der Union oder Interessengemeinschaften, zu denen auch die Organe, Einrichtungen und sonstigen Stellen der Union gehören, ausgerichtet sind. Um eine proaktive Erkennung von Sicherheitsvorfällen sowie Maßnahmen zu ihrer Bewältigung und Abschwächung zu ermöglichen, sollten die Organe, Einrichtungen und sonstigen Stellen der Union das CERT-EU über erhebliche Cyberbedrohungen, erhebliche Sicherheitslücken und erhebliche Sicherheitsvorfälle informieren und geeignete technische Einzelheiten übermitteln, die die Erkennung bzw. Abschwächung sowie die Bewältigung ähnlicher Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfälle in anderen Organen, Einrichtungen und sonstigen Stellen der Union ermöglichen. Nach demselben Ansatz wie in der Richtlinie [NIS-2-Vorschlag] sollten Einrichtungen, die von einem erheblichen Sicherheitsvorfall Kenntnis erhalten, verpflichtet sein, innerhalb von 24 Stunden eine erste Meldung an das CERT-EU zu übermitteln. Dieser Informationsaustausch sollte es dem CERT-EU ermöglichen, die Informationen an andere Organe, Einrichtungen und sonstige Stellen der Union sowie an entsprechende Partner weiterzugeben, um dazu beizutragen, die IT-Umgebungen der Union und die IT-Umgebungen der Partner der Union vor ähnlichen Sicherheitsvorfällen, Bedrohungen und Sicherheitslücken zu schützen.

(14) Neben den zusätzlichen Aufgaben und der erweiterten Rolle, die für das CERT-EU vorgesehen werden, sollte auch ein Interinstitutioneller Cybersicherheitsbeirat (IICB) eingerichtet werden, der ein hohes gemeinsames Cybersicherheitsniveau der Organe, Einrichtungen und sonstigen Stellen der Union fördern soll, indem er die Umsetzung dieser Verordnung durch die Organe, Einrichtungen und sonstigen Stellen der Union überwacht, die Umsetzung der allgemeinen Prioritäten und Ziele durch das CERT-EU beaufsichtigt und strategische Leitlinien für das CERT-EU festlegt. In dem IICB sollte die Vertretung der Organe gewährleistet sein und dem Beirat sollten über das Netzwerk der Agenturen der Union auch Vertreter von Agenturen und Einrichtungen angehören.

(15) Das CERT-EU sollte die Umsetzung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau durch Vorschläge für Leitfäden und Empfehlungen an den IICB oder durch Aufrufe zum Tätigwerden unterstützen. Diese Leitlinien und Empfehlungen sollten vom IICB genehmigt werden. Wenn erforderlich, sollte das CERT-EU Aufrufe zum Tätigwerden herausgeben, in denen dringende Sicherheitsmaßnahmen beschrieben werden, zu deren Ergreifung innerhalb einer vorgegebenen Frist die Organe, Einrichtungen und sonstigen Stellen der Union dringend aufgefordert werden.

(16) Der IICB sollte die Einhaltung dieser Verordnung sowie die Maßnahmen zur Befolgung von Leitlinien und Empfehlungen und der vom CERT-EU lancierten Aufrufe zum Tätigwerden überwachen. Der IICB sollte in technischen Fragen von fachlichen Beratungsgruppen unterstützt werden, deren Zusammensetzung im Ermessen des IICB liegt und die bei Bedarf eng mit dem CERT-EU, den Organen, Einrichtungen und sonstigen Stellen der Union sowie mit anderen Interessenträgern zusammenarbeiten sollten. Erforderlichenfalls sollte der IICB unverbindliche Warnungen aussprechen und Audits empfehlen.

(17) Das CERT-EU sollte den Auftrag haben, zur Sicherheit der IT-Umgebung aller Organe, Einrichtungen und sonstigen Stellen der Union beizutragen. Das CERT-EU sollte für die Zwecke der koordinierten Offenlegung von Sicherheitslücken beim europäischen Schwachstellenregister gemäß Artikel 6 der Richtlinie [NIS-2-Vorschlag] als Äquivalent des benannten Koordinators für die Organe, Einrichtungen und sonstigen Stellen der Union fungieren.

(18) Im Jahr 2020 legte der Lenkungsausschuss des CERT-EU ein neues strategisches Ziel für das CERT-EU fest, um für alle Organe, Einrichtungen und sonstigen Stellen der Union ein umfassendes Cyberabwehrniveau angemessener Breite und Tiefe zu gewährleisten und eine kontinuierliche Anpassung an aktuelle oder sich abzeichnende Bedrohungen, einschließlich Angriffen auf mobile Geräte, Cloud-Umgebungen und Geräte des Internets der Dinge, zu ermöglichen. Das strategische Ziel umfasst auch Sicherheitseinsatzzentren (SOCs) mit breit angelegtem Aufgabenbereich, die für die Netzüberwachung zuständig sind, sowie eine Rund-um-die-Uhr-Überwachung zur Erkennung hochgradiger Sicherheitsbedrohungen. Bei den größeren Organen, Einrichtungen und sonstigen Stellen der Union sollte das CERT-EU die IT-Sicherheitsteams dieser Stellen unterstützen, insbesondere durch Rund-um-die-Uhr-Überwachung auf der ersten Ebene. Für kleinere Organe, Einrichtungen und sonstige Stellen der Union und einige Organe, Einrichtungen und sonstige Stellen der Union mittlerer Größe sollte das CERT-EU alle Dienste erbringen.

(19) Das CERT-EU sollte zudem die Rolle übernehmen, die ihm nach der Richtlinie [NIS-2-Vorschlag] bei der Zusammenarbeit und beim Informationsaustausch mit dem Netzwerk der Computer-Notfallteams (CSIRTs-Netzwerk) zukommt. Darüber hinaus sollte das CERT-EU im Einklang mit der Empfehlung (EU) 2017/1584 der Kommission[4] mit den einschlägigen Interessenträgern zusammenarbeiten und sich bezüglich der Reaktionsmaßnahmen mit diesen abstimmen. Um zu einem hohen Cybersicherheitsniveau in der gesamten Union beizutragen, sollte das CERT-EU Informationen zu den einzelnen Sicherheitsvorfällen an die nationalen Partner weiterleiten. Das CERT-EU sollte vorbehaltlich der vorherigen Genehmigung durch den IICB auch mit anderen öffentlichen und privaten Partnern, einschließlich der NATO, zusammenarbeiten.

(20) Bei der Unterstützung der operativen Cybersicherheit sollte das CERT-EU das verfügbare Fachwissen der Agentur der Europäischen Union für Cybersicherheit im Wege der strukturierten Zusammenarbeit gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[5] nutzen. Für die Festlegung der praktischen Aspekte einer solchen Kooperation und zur Vermeidung von Doppelarbeit sollten gegebenenfalls gesonderte Vereinbarungen zwischen den beiden Stellen getroffen werden. Das CERT-EU sollte mit der Agentur der Europäischen Union für Cybersicherheit bei der Analyse der Bedrohungslage zusammenarbeiten und der Agentur seinen Bericht zur Bedrohungslage regelmäßig übermitteln.

---

4 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).

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

(21) Zur Unterstützung der im Einklang mit der Empfehlung der Kommission vom 23. Juni 2021[6] eingerichteten Gemeinsamen Cyber-Einheit sollte das CERT-EU mit Interessenträgern zusammenarbeiten und Informationen mit diesen austauschen, um die operative Zusammenarbeit zu fördern und die bestehenden Netzwerke in die Lage zu versetzen, ihr volles Potenzial für den Schutz der Union zu entfalten.

(22) Alle im Rahmen dieser Verordnung verarbeiteten personenbezogenen Daten sollten im Einklang mit den Datenschutzvorschriften, einschließlich der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[7], verarbeitet werden.

(23) Der Umgang des CERT-EU und der Organe, Einrichtungen und sonstigen Stellen der Union mit Informationen sollte gemäß der Verordnung [vorgeschlagene Verordnung über die Informationssicherheit] erfolgen. Zur Gewährleistung der Koordinierung in Sicherheitsangelegenheiten sollten alle Fälle, in denen sich nationale Sicherheits- und Nachrichtendienste aus eigener Initiative oder auf eigenes Bestreben an das CERT-EU werden, der Direktion Sicherheit der Kommission und dem Vorsitz des IICB unverzüglich mitgeteilt werden.

(24) Da die Dienste und Aufgaben des CERT-EU im Interesse aller Organe, Einrichtungen und sonstigen Stellen der Union erbracht werden bzw. liegen, sollten alle Organe, Einrichtungen und sonstigen Stellen der Union, die über einen Etat für IT-Ausgaben verfügen, einen angemessenen Beitrag für diese Dienste und Aufgaben leisten. Diese Beiträge lassen die Haushaltsautonomie der Organe, Einrichtungen und sonstigen Stellen der Union unberührt.

(25) Der IICB sollte die Durchführung dieser Verordnung mit Unterstützung des CERT-EU überprüfen und bewerten und der Kommission über seine Feststellungen Bericht erstatten. Die Kommission sollte dem Europäischen Parlament, dem Rat, dem Europäischen Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen regelmäßig Bericht erstatten.

HABEN FOLGENDE VERORDNUNG ERLASSEN:

Kapitel I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand

Mit dieser Verordnung wird Folgendes festgelegt:

a) Verpflichtungen für die Organe, Einrichtungen und sonstigen Stellen der Union zur Schaffung eines internen Rahmens für das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken,

b) Cybersicherheitsrisikomanagements- und Berichterstattungspflichten für die Organe, Einrichtungen und sonstigen Stellen der Union,

---

6 Empfehlung C(2021) 4520 der Kommission vom 23. Juni 2021 zum Aufbau einer gemeinsamen Cyber-Einheit.

7 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

c) Vorschriften über die Organisation und Arbeitsweise des Cybersicherheitszentrums für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) und über die Organisation und Arbeitsweise des Interinstitutionellen Cybersicherheitsbeirats (IICB).

Artikel 2
Anwendungsbereich

Diese Verordnung gilt für das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken durch alle Organe, Einrichtungen und sonstigen Stellen der Union und für die Organisation und den Betrieb des CERT-EU und des IICB.

Artikel 3
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Organe, Einrichtungen und sonstige Stellen der Union“ die Organe, Einrichtungen und sonstigen Stellen der Union, die durch den Vertrag über die Europäische Union, den Vertrag über die Arbeitsweise der Europäischen Union oder den Vertrag zur Gründung der Europäischen Atomgemeinschaft oder auf deren Grundlage geschaffen wurden,
2. „Netz- und Informationssystem“ ein Netz- und Informationssystem im Sinne des Artikels 4 Nummer 1 der Richtlinie [NIS-2-Vorschlag];
3. „Sicherheit von Netz- und Informationssystemen“ die Sicherheit von Netz- und Informationssystemen im Sinne des Artikels 4 Nummer 2 der Richtlinie [NIS-2-Vorschlag];
4. „Cybersicherheit“ Cybersicherheit im Sinne des Artikels 4 Nummer 3 der Richtlinie [NIS-2-Vorschlag];
5. „höchste Managementebene“ eine Führungskraft, ein Management-, Koordinierungs- oder Aufsichtsgremium auf der höchsten Verwaltungsebene, unter Berücksichtigung der Governance-Regelungen für die höchsten Ebenen in den einzelnen Organen, Einrichtungen und sonstigen Stellen der Union,
6. „Sicherheitsvorfall“ einen Sicherheitsvorfall im Sinne des Artikels 4 Nummer 5 der Richtlinie [NIS-2-Vorschlag];
7. „erheblicher Sicherheitsvorfall“ jeden Sicherheitsvorfall mit Ausnahme derjenigen, die begrenzte Auswirkungen haben und deren Methoden oder Technologien wahrscheinlich bereits bekannt sind;
8. „größerer Angriff“ jeden Sicherheitsvorfall, der mehr Ressourcen erfordert als bei den betroffenen Organen, Einrichtungen oder sonstigen Stellen der Union und beim CERT-EU zur Verfügung stehen;
9. „Bewältigung von Sicherheitsvorfällen“ die Bewältigung von Sicherheitsvorfällen im Sinne des Artikels 4 Nummer 6 der Richtlinie [NIS-2-Vorschlag];
10. „Cyberbedrohung“ eine Cyberbedrohung im Sinne von Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;
11. „erhebliche Cyberbedrohung“ eine Cyberbedrohung mit der Absicht, der Möglichkeit und der Fähigkeit, einen erheblichen Sicherheitsvorfall zu verursachen;

12. „Sicherheitslücke“ eine Sicherheitslücke im Sinne des Artikels 4 Nummer 8 der Richtlinie [NIS-2-Vorschlag];

13. „erhebliche Sicherheitslücke“ eine Sicherheitslücke, die wahrscheinlich zu einem erheblichen Sicherheitsvorfall führen wird, wenn sie genutzt wird;

14. „Cybersicherheitsrisiko“ alle mit vertretbarem Aufwand feststellbaren Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben;

15. „Gemeinsame Cyber-Einheit“ eine virtuelle und physische Plattform für die Zusammenarbeit der verschiedenen Cybersicherheitsgemeinschaften in der Union mit Schwerpunkt auf der operativen und technischen Koordinierung im Falle größerer grenzübergreifender Cyberbedrohungen und Cybersicherheitsvorfälle im Sinne der Empfehlung der Kommission vom 23. Juni 2021,

16. „Cybersicherheitsgrundregeln“ eine Reihe von Mindestvorschriften für die Cybersicherheit, denen Netz- und Informationssysteme und deren Betreiber und Nutzer entsprechen müssen, um Cybersicherheitsrisiken zu minimieren.

Kapitel II
MAßNAHMEN FÜR EIN HOHES GEMEINSAMES CYBERSICHERHEITSNIVEAU

Artikel 4
Risikomanagement, Governance und Kontrolle

(1) Alle Organe, Einrichtungen und sonstigen Stellen der Union legen in Unterstützung ihres jeweiligen Auftrags und in Ausübung ihrer institutionellen Autonomie ihren eigenen internen Rahmen für das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken (im Folgenden „Rahmen“) fest. Diese Arbeit erfolgt unter der Aufsicht der jeweiligen höchsten Managementebene, um ein wirksames und umsichtiges Management aller Cybersicherheitsrisiken zu gewährleisten. Der Rahmen ist bis spätestens ... [15 Monate nach dem Inkrafttreten dieser Verordnung] einzuführen.

(2) Der Rahmen deckt jeweils die gesamte IT-Umgebung der betreffenden Organe, Einrichtungen oder sonstigen Stellen ab, insbesondere die IT-Umgebung in den Räumlichkeiten der betreffenden Organe, Einrichtungen oder sonstigen Stellen, in Cloud-Computing-Umgebungen ausgelagerte oder von Dritten gehostete Anlagen und Dienste, mobile Geräte, Firmennetze, nicht mit dem Internet verbundene Geschäftsnetze und alle mit der IT-Umgebung verbundenen Geräte. Der Rahmen berücksichtigt die Sicherung der Betriebskontinuität und das Krisenmanagement und deckt die Sicherheit der Lieferkette und den Umgang mit menschlichen Risiken ab, die Auswirkungen auf die Cybersicherheit des betreffenden Organs oder der betreffenden Einrichtung der Union haben könnten.

(3) Die höchste Managementebene jedes Organs, jeder Einrichtung und jeder sonstigen Stelle der Union überwacht die Einhaltung der mit dem Risikomanagement, der Governance und der Kontrolle im Bereich der Cybersicherheit verbundenen Verpflichtungen durch ihre Organisation unbeschadet der formalen Zuständigkeit anderer Managementebenen in Bezug auf die Einhaltung der Vorschriften und das Risikomanagement in deren jeweiligen Zuständigkeitsbereichen.

(4) Alle Organe, Einrichtungen und sonstigen Stellen der Union müssen über wirksame Mechanismen verfügen, um sicherzustellen, dass ein angemessener Prozentsatz des IT-Budgets für Cybersicherheit ausgegeben wird.

(5) Alle Organe, Einrichtungen und sonstigen Stellen der Union ernennen einen lokalen Cybersicherheitsbeauftragten oder eine Kontaktperson mit gleichwertiger Funktion, der oder die als zentrale Anlaufstelle für alle Cybersicherheitsfragen fungiert.

Artikel 5
Cybersicherheitsgrundregeln

(1) Die jeweilige höchste Managementebene der Organe, Einrichtungen und sonstigen Stellen der Union genehmigt die jeweiligen eigenen Cybersicherheitsgrundregeln, um die Risiken anzugehen, die in dem in Artikel 4 Absatz 1 genannten Rahmen ermittelt werden. Sie tut dies in Unterstützung ihres jeweiligen Auftrags und in Ausübung ihrer institutionellen Autonomie. Die Cybersicherheitsgrundregeln müssen bis spätestens …. [18 Monate nach Inkrafttreten dieser Verordnung] vorliegen und sich auf die in Anhang I aufgeführten Bereiche und die in Anhang II aufgeführten Maßnahmen erstrecken.

(2) Die jeweiligen Führungskräfte der Organe, Einrichtungen und sonstigen Stellen der Union absolvieren regelmäßig spezifische Schulungen, um ausreichende Kenntnisse und Fähigkeiten zu erwerben, damit sie Cybersicherheitsrisiken und -managementverfahren und deren Auswirkungen auf den Betrieb der Organisation erfassen und bewerten können.

Artikel 6
Bewertung des Reifegrads

Alle Organe, Einrichtungen und sonstigen Stellen der Union führen mindestens alle drei Jahre eine Bewertung des Cybersicherheitsreifegrads durch, bei der alle in Artikel 4 genannten Elemente ihrer IT-Umgebung einbezogen und die gemäß Artikel 13 angenommenen einschlägigen Leitlinien und Empfehlungen berücksichtigt werden.

Artikel 7
Cybersicherheitspläne

(1) Auf der Grundlage der Schlussfolgerungen der Bewertung des Reifegrads und unter Berücksichtigung der gemäß Artikel 4 ermittelten Anlagen und Risiken genehmigt die höchste Managementebene jedes Organs, jeder Einrichtung und jeder sonstigen Stelle der Union unverzüglich nach der Festlegung des Rahmens für Risikomanagement, Governance und Kontrolle und der Cybersicherheitsgrundregeln einen Cybersicherheitsplan. Der Plan zielt darauf ab, die Cybersicherheit des betreffenden Organs bzw. der betreffenden Einrichtung oder Stelle insgesamt zu erhöhen und trägt somit zur Erreichung oder Verbesserung eines hohen gemeinsamen Cybersicherheitsniveaus aller Organe, Einrichtungen und sonstigen Stellen der Union bei. Um den Auftrag des Organs bzw. der Einrichtung oder Stelle auf der Basis ihrer institutionellen Autonomie zu unterstützen, deckt der Plan mindestens die in Anhang I genannten Bereiche und die in Anhang II genannten Maßnahmen ab und sieht Maßnahmen zur Abwehrbereitschaft, Reaktion und Folgenbewältigung wie Sicherheitsüberwachung und -protokollierung vor. Der Plan

wird mindestens alle drei Jahre im Anschluss an die gemäß Artikel 6 durchgeführten Bewertungen des Reifegrads überarbeitet.

(2) In dem Cybersicherheitsplan sind auch die Aufgaben und Zuständigkeiten des mit seiner Umsetzung befassten Personals festgelegt.

(3) Der Cybersicherheitsplan trägt allen einschlägigen Leitfäden und Empfehlungen des CERT-EU Rechnung.

Artikel 8
Durchführung

(1) Nach Abschluss der Bewertungen des Reifegrads übermitteln die Organe, Einrichtungen und sonstigen Stellen der Union diese dem Interinstitutionellen Cybersicherheitsbeirat. Nach Fertigstellung der Sicherheitspläne teilen die Organe, Einrichtungen und sonstigen Stellen der Union dies dem Interinstitutionellen Cybersicherheitsbeirat mit. Auf Verlangen des Beirats erstatten sie Bericht über spezifische Aspekte der Umsetzung dieses Kapitels.

(2) Gemäß Artikel 13 erstellte Leitfäden und Empfehlungen unterstützen die Umsetzung dieses Kapitels.

Kapitel III
INTERINSTITUTIONELLER CYBERSICHERHEITSBEIRAT

Artikel 9
Interinstitutioneller Cybersicherheitsbeirat

(1) Es wird ein Interinstitutioneller Cybersicherheitsbeirat (IICB) eingesetzt.

(2) Der IICB ist zuständig für

a) die Überwachung der Durchführung dieser Verordnung durch die Organe, Einrichtungen und sonstigen Stellen der Union und

b) die Beaufsichtigung der Umsetzung der allgemeinen Prioritäten und Ziele durch das CERT-EU und die Festlegung strategischer Vorgaben für das CERT-EU.

(3) Dem IICB gehören drei Vertreter an, die vom Netz der Agenturen der Union (EUAN) auf Vorschlag seines IKT-Beratungsausschusses benannt werden, um die Interessen der Agenturen und Einrichtungen zu vertreten, die ihre eigene IT-Umgebung betreiben, sowie je ein von den folgenden Organen, Einrichtungen und Stellen benannter Vertreter:

a) Europäisches Parlament,

b) Rat der Europäischen Union,

c) Europäische Kommission;

d) Gerichtshof der Europäischen Union;

e) Europäische Zentralbank;

f) Europäischer Rechnungshof;

g) Europäischer Auswärtiger Dienst;

h) Europäischer Wirtschafts- und Sozialausschuss;

i) Europäischer Ausschuss der Regionen;

j) Europäische Investitionsbank;

k) Agentur der Europäischen Union für Cybersicherheit.

Jedes Mitglied kann einen Stellvertreter haben. Der Vorsitzende kann weitere Vertreter bzw. Vertreterinnen der vorstehend genannten Organe, Einrichtungen und Stellen der Union zur Teilnahme an IICB-Sitzungen einladen, die kein Stimmrecht haben.

(4) Der IICB gibt sich eine Geschäftsordnung.

(5) Der IICB benennt im Einklang mit seiner Geschäftsordnung aus den Reihen seiner Mitglieder einen Vorsitzenden für einen Zeitraum von vier Jahren. Der Stellvertreter des Vorsitzenden wird für denselben Zeitraum Vollmitglied des IICB.

(6) Der IICB tritt auf Initiative seines Vorsitzes, auf Ersuchen des CERT-EU oder auf Antrag eines seiner Mitglieder zusammen.

(7) Jedes Mitglied des IICB hat eine Stimme. Die Beschlüsse des IICB werden mit einfacher Mehrheit gefasst, soweit in dieser Verordnung nichts anderes bestimmt ist. Der Vorsitz beteiligt sich nicht an den Abstimmungen, außer bei Stimmengleichheit, bei der seine Stimme den Ausschlag gibt.

(8) Der IICB kann im Wege eines vereinfachten schriftlichen Verfahrens tätig werden, das im Einklang mit der Geschäftsordnung des IICB eingeleitet wird. Gemäß diesem Verfahren gilt die entsprechende Entscheidung als innerhalb des vom Vorsitz vorgegebenen Zeitrahmens gebilligt, sofern kein Mitglied Einwände erhebt.

(9) Der Leiter des CERT-EU oder sein Stellvertreter nimmt an den IICB-Sitzungen teil, sofern der IICB nichts anderes beschließt.

(10) Die Sekretariatsgeschäfte des IICB werden von der Kommission wahrgenommen.

(11) Die vom EUAN auf Vorschlag des IKT-Beratungsausschusses benannten Vertreter und Vertreterinnen leiten die Beschlüsse des IICB an die Agenturen und gemeinsamen Unternehmen der Union weiter. Alle Agenturen und Stellen der Union haben das Recht, die Vertreter und Vertreterinnen oder den Vorsitz des IICB mit Angelegenheiten zu befassen, die ihrer Ansicht nach dem IICB zur Kenntnis gebracht werden sollten.

(12) Der IICB kann im Wege eines vom Vorsitz eingeleiteten vereinfachten schriftlichen Verfahrens tätig werden, gemäß dem die entsprechende Entscheidung als innerhalb des vom Vorsitz vorgegebenen Zeitrahmens gebilligt gilt, es sei denn, ein Mitglied erhebt Einwände.

(13) Der IICB kann einen Exekutivausschuss einsetzen, der ihn bei seiner Arbeit unterstützt, und ihm einige seiner Aufgaben und Befugnisse übertragen. Der IICB legt die Geschäftsordnung sowie die Aufgaben und Befugnisse des Exekutivausschusses und die Amtszeit seiner Mitglieder fest.

Artikel 10

Aufgaben des IICB

Bei der Ausübung seiner Zuständigkeiten nimmt der IICB insbesondere folgende Aufgaben wahr:

a) Prüfung aller vom CERT-EU angeforderten Berichte über den Stand der Durchführung dieser Verordnung durch die Organe, Einrichtungen und sonstigen Stellen der Union,

b) Genehmigung, auf der Grundlage eines Vorschlags der Leitung des CERT-EU, des jährlichen Arbeitsprogramms des CERT-EU und Überwachung seiner Umsetzung,

c) Genehmigung, auf der Grundlage eines Vorschlags der Leitung des CERT-EU, des Leistungskatalogs des CERT-EU,

d) Genehmigung, auf der Grundlage eines von der Leitung des CERT-EU vorgelegten Vorschlags, der jährlichen Finanzplanung der Einnahmen und Ausgaben, einschließlich Personalkosten, für die Tätigkeiten des CERT-EU,

e) Genehmigung, auf der Grundlage eines Vorschlags der Leitung des CERT-EU, der Modalitäten für Leistungsvereinbarungen,

f) Prüfung und Genehmigung des Jahresberichts der Leitung des CERT-EU über die Tätigkeiten des CERT-EU und die Mittelverwaltung durch das CERT-EU,

g) Genehmigung und Überwachung der auf Vorschlag der Leitung des CERT-EU festgelegten wesentlichen Leistungsindikatoren für das CERT-EU,

h) Genehmigung von Kooperationsvereinbarungen und Leistungsvereinbarungen oder Verträgen zwischen dem CERT-EU und anderen Stellen gemäß Artikel 17,

i) Einsetzung von zur Unterstützung der Arbeit des IICB notwendigen Fachberatungsgruppen, Genehmigung ihrer Mandate und Ernennung ihrer jeweiligen Vorsitze.

Artikel 11
Einhaltung

Der IICB überwacht die Durchführung dieser Verordnung und die Umsetzung der angenommenen Leitlinien, Empfehlungen und Aufrufe zum Tätigwerden durch die Organe, Einrichtungen und sonstigen Stellen der Union. Stellt der IICB fest, dass Organe, Einrichtungen oder sonstige Stellen der Union diese Verordnung oder auf der Grundlage dieser Verordnung angenommene Leitlinien, Empfehlungen oder Aufrufe zum Tätigwerden nicht wirksam angewandt oder durchgeführt bzw. umgesetzt haben, so kann er unbeschadet der internen Verfahren der betreffenden Organe, Einrichtungen oder sonstigen Stellen der Union

a) eine Verwarnung aussprechen; sofern angesichts eines zwingenden Cybersicherheitsrisikos notwendig wird der Empfängerkreis der Verwarnung in geeigneter Weise eingeschränkt,

b) empfehlen, dass der zuständige interne Auditdienst eine Prüfung durchführt.

KAPITEL IV
CERT-EU

Artikel 12
Auftrag und Aufgaben des CERT-EU

(1) Der Auftrag des CERT-EU, des autonomen interinstitutionellen Cybersicherheitszentrums für alle Organe, Einrichtungen und sonstigen Stellen der

Union, besteht darin, zur Sicherheit der nichtvertraulichen IT-Umgebung aller Organe, Einrichtungen und sonstigen Stellen der Union beizutragen, indem es diese in Cybersicherheitsangelegenheiten berät, bei der Prävention, Erkennung, Abschwächung und Bewältigung von Sicherheitsvorfällen unterstützt und als zentrale Stelle für den Austausch von Informationen zur Cybersicherheit und die Koordinierung der Reaktion auf Sicherheitsvorfälle fungiert.

(2) Das CERT-EU nimmt folgende Aufgaben für die Organe, Einrichtungen und sonstigen Stellen der Union wahr:

a) Unterstützung der Organe, Einrichtungen und sonstigen Stellen der Union bei der Durchführung dieser Verordnung und Beitrag zur Koordinierung der Anwendung dieser Verordnung durch die in Artikel 13 Absatz 1 aufgeführten Maßnahmen oder durch vom IICB angeforderte Ad-hoc-Berichte,

b) Unterstützung der Organe, Einrichtungen und sonstigen Stellen der Union mit Cybersicherheitsdiensten, die in seinem Leistungskatalog beschrieben sind (im Folgenden „Basisdienste“),

c) Pflege eines Netzes entsprechender Stellen und Partner zur Unterstützung der in den Artikeln 16 und 17 genannten Dienste,

d) Unterrichtung des IICB über Fragen im Zusammenhang mit der Durchführung dieser Verordnung und der Umsetzung der Leitlinien, Empfehlungen und Aufrufe zum Tätigwerden,

e) Berichterstattung über die Cyberbedrohungen, denen die Organe, Einrichtungen und sonstigen Stellen der Union ausgesetzt sind, und Beitrag zur Erfassung der Cyberlage in der EU.

(3) Das CERT-EU trägt zur gemäß der Empfehlung der Kommission vom 23. Juni 2021 errichteten Gemeinsamen Cyber-Einheit bei, unter anderem in den folgenden Bereichen:

a) Abwehrbereitschaft, Koordinierung bei Sicherheitsvorfällen, Informationsaustausch und Krisenreaktion auf der technischen Ebene in Fällen, in denen Organe, Einrichtungen und sonstige Stellen der Union betroffen sind,

b) operative Zusammenarbeit in Bezug auf das Netz der Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs), auch zur gegenseitigen Unterstützung, und die breitere Cybersicherheitsgemeinschaft,

c) Informationen über Cyberbedrohungen, einschließlich Lageerfassung,

d) alle Themen, die das Cybersicherheitsfachwissen des CERT-EU erfordern.

(4) Das CERT-EU kooperiert in strukturierter Weise mit der Agentur der Europäischen Union für Cybersicherheit in den Bereichen Kapazitätsaufbau, operative Zusammenarbeit und langfristige strategische Analysen von Cyberbedrohungen im Einklang mit der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates.

(5) Das CERT-EU kann folgende, nicht in seinem Dienstekatalog aufgeführten Dienste erbringen (im Folgenden „kostenpflichtige Dienste“):

a) andere als die in Absatz 2 genannten Dienste, die die Cybersicherheit der IT-Umgebung von Organen, Einrichtungen und sonstigen Stellen der Union

unterstützen, auf der Grundlage von Leistungsvereinbarungen und vorbehaltlich verfügbarer Ressourcen,

b) Dienste, die andere als zum Schutz der jeweiligen IT-Umgebung durchgeführte Cybersicherheitsmaßnahmen oder -projekte von Organen, Einrichtungen und sonstigen Stellen der Union unterstützen, auf der Grundlage schriftlicher Vereinbarungen und nach vorheriger Genehmigung des IICB,

c) Dienste, die die Sicherheit der jeweiligen IT-Umgebung unterstützen, für andere Organisationen als die Organe, Einrichtungen und sonstigen Stellen der Union, die eng mit den Organen, Einrichtungen und sonstigen Stellen der Union zusammenarbeiten, z. B. weil ihnen im Rahmen des Unionsrechts Aufgaben und Zuständigkeiten übertragen wurden, auf der Grundlage schriftlicher Vereinbarungen und nach vorheriger Genehmigung des IICB.

(6) Das CERT-EU kann Cybersicherheitsübungen organisieren oder die Teilnahme an bestehenden Übungen empfehlen, gegebenenfalls in enger Zusammenarbeit mit der Agentur der Europäischen Union für Cybersicherheit, um das Cybersicherheitsniveau der Organe, Einrichtungen und sonstigen Stellen der Union zu prüfen.

(7) Das CERT-EU kann Organe, Einrichtungen und sonstigen Stellen der Union in Bezug auf Sicherheitsvorfälle in nicht frei zugänglichen IT-Umgebungen unterstützen, wenn es von dem betreffenden Konstituenten ausdrücklich dazu aufgefordert wird.

Artikel 13
Leitlinien, Empfehlungen und Aufrufe zum Tätigwerden

(1) Das CERT-EU unterstützt die Durchführung dieser Verordnung, indem er

a) Aufrufe zum Tätigwerden vorlegt, in denen dringende Sicherheitsmaßnahmen beschrieben werden, zu deren Ergreifung innerhalb einer vorgegebenen Frist die Organe, Einrichtungen und sonstigen Stellen der Union aufgefordert werden;

b) dem IICB Vorschläge für Leitlinien unterbreitet, die an alle oder einen Teil der Organe, Einrichtungen und sonstigen Stellen der Union gerichtet sind,

c) dem IICB Vorschläge für Empfehlungen unterbreitet, die an alle oder einen Teil der Organe, Einrichtungen und sonstigen Stellen der Union gerichtet sind.

(2) Die Leitlinien und Empfehlungen können Folgendes umfassen:

a) Modalitäten für das Cybersicherheitsrisikomanagement und die Cybersicherheitsgrundregeln oder diesbezügliche Verbesserungen

b) Modalitäten für die Bewertungen des Reifegrads und die Cybersicherheitspläne; und

c) gegebenenfalls den Einsatz gemeinsamer Technologie, Architektur und dazugehöriger bewährter Verfahren mit dem Ziel, Interoperabilität und gemeinsame Normen im Sinne des Artikels 4 Absatz 10 der Richtlinie [NIS-2-Vorschlag] zu erreichen.

(3) Der IICB kann vom CERT-EU vorgeschlagene Leitlinien und Empfehlungen annehmen.

(4) Der IICB kann das CERT-EU anweisen, einen Vorschlag für Leitlinien oder Empfehlungen oder einen Aufruf zum Tätigwerden vorzulegen, zurückzuziehen oder zu ändern.

Artikel 14
Der Leiter des CERT-EU

Die Leitung des CERT-EU legt dem IICB regelmäßig Berichte über die Leistung des CERT-EU, die Finanzplanung, die Einnahmen, die Ausführung des Haushaltsplans, Leistungsvereinbarungen und schriftliche Vereinbarungen, die Zusammenarbeit mit entsprechenden Stellen und Partnern und Dienstreisen des Personals vor, einschließlich der in Artikel 10 Absatz 1 genannten Berichte.

Artikel 15
Finanzen und Personal

(1) Die Kommission ernennt nach einstimmiger Billigung des IICB die Leitung des CERT-EU. Der IICB wird in allen Phasen des Verfahrens vor der Ernennung der Leitung des CERT-EU konsultiert, insbesondere bei der Ausarbeitung von Stellenausschreibungen, der Prüfung von Bewerbungen und der Ernennung von Auswahlausschüssen im Zusammenhang mit diesem Posten.

(2) Bei der Anwendung der Verwaltungs- und Finanzverfahren handelt die Leitung des CERT-EU unter Aufsicht der Kommission.

(3) Aufgaben und Tätigkeiten des CERT-EU, einschließlich der Dienste, die vom CERT-EU gemäß Artikel 12 Absätze 2, 3, 4 und 6 sowie gemäß Artikel 13 Absatz 1 für aus der Rubrik „Europäische öffentliche Verwaltung“ des mehrjährigen Finanzrahmens finanzierte Organe, Einrichtungen und sonstige Stellen der Union erbracht werden, werden aus einer gesonderten Haushaltslinie des Haushaltsplans der Kommission finanziert. Dem CERT-EU zugewiesene Stellen werden in einer Fußnote des Stellenplans der Kommission angegeben.

(4) Andere als die in Absatz 3 genannten Organe, Einrichtungen und sonstigen Stellen der Union leisten einen jährlichen finanziellen Beitrag zum CERT-EU zur Deckung der vom CERT-EU gemäß Absatz 3 erbrachten Dienste. Die jeweiligen Beiträge beruhen auf Vorgaben des IICB und werden jeweils zwischen den einzelnen Organen, Einrichtungen oder sonstigen Stellen und dem CERT-EU in Leistungsvereinbarungen festgelegt. Die Beiträge entsprechen einem angemessenen und verhältnismäßigen Anteil an den Gesamtkosten der erbrachten Dienste. Sie werden gemäß Artikel 21 Absatz 3 Buchstabe c der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates[8] als zweckgebundene Einnahmen in die in Absatz 3 genannte gesonderte Haushaltslinie eingestellt.

(5) Die Kosten für die in Artikel 12 Absatz 5 festgelegten Aufgaben werden bei den Organen, Einrichtungen und sonstigen Stellen der Union eingezogen, denen die

[8] Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

CERT-EU-Dienste erbracht werden. Die Einnahmen werden in die Haushaltslinien eingestellt, in denen die Kosten angesetzt wurden.

Artikel 16

Zusammenarbeit des CERT-EU mit den entsprechenden Stellen der Mitgliedstaaten

(1) Das CERT-EU arbeitet mit den entsprechenden Stellen der Mitgliedstaaten, einschließlich CERTs, nationalen Cybersicherheitszentren, CSIRTs und den in Artikel 8 der Richtlinie [NIS-2-Vorschlag] genannten zentralen Anlaufstellen zusammen und tauscht Informationen mit ihnen aus über Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfälle sowie über alle Angelegenheiten, die für die Verbesserung des Schutzes der IT-Umgebungen der Organe, Einrichtungen und sonstigen Stellen der Union relevant sind, auch durch das in Artikel 13 der Richtlinie [NIS-2-Vorschlag] genannte CSIRTs-Netz.

(2) Das CERT-EU kann spezifische Informationen über Sicherheitsvorfälle ohne Einwilligung des betroffenen Konstituenten an diese entsprechenden nationalen Stellen weitergeben, um die Aufdeckung ähnlicher Cyberbedrohungen oder Sicherheitsvorfälle zu erleichtern. Das CERT-EU kann spezifische Informationen über Sicherheitsvorfälle, aus denen die Identität der Zielgruppe des Cybersicherheitsvorfalls hervorgeht, nur mit Einwilligung des betroffenen Konstituenten weitergeben.

Artikel 17

Zusammenarbeit des CERT-EU mit den entsprechenden Stellen von Nichtmitgliedstaaten

(1) Das CERT-EU kann in Bezug auf Instrumente und Methoden wie Techniken, Taktiken, Verfahren und bewährte Verfahren sowie in Bezug auf Cyberbedrohungen und Sicherheitslücken mit den entsprechenden Stellen, einschließlich branchenspezifischer Stellen, von Nichtmitgliedstaaten zusammenarbeiten. Für jede Zusammenarbeit mit diesen Stellen, auch in Rahmen, in denen Nicht-EU-Stellen mit nationalen Stellen von Mitgliedstaaten zusammenarbeiten, holt das CERT-EU vorab die Zustimmung des IICB ein.

(2) Das CERT-EU kann mit anderen Partnern wie Unternehmen, internationalen Organisationen und nationalen Einrichtungen oder einzelnen Sachverständigen aus Nichtmitgliedstaaten der Europäischen Union zusammenarbeiten, um Informationen über allgemeine und spezifische Cyberbedrohungen, Sicherheitslücken und mögliche Gegenmaßnahmen einzuholen. Für eine umfassendere Zusammenarbeit mit diesen Partnern holt CERT-EU vorab die Zustimmung des IICB ein.

(3) Das CERT-EU kann, mit Einwilligung des von einem Sicherheitsvorfall betroffenen Konstituenten, Informationen über diesen Sicherheitsvorfall an Partner weitergeben, die zu seiner Analyse beitragen können.

KAPITEL V
ZUSAMMENARBEIT UND BERICHTERSTATTUNGSPFLICHTEN

Artikel 18

Umgang mit Informationen

(1) Das CERT-EU und die Organe, Einrichtungen und sonstigen Stellen der Union kommen der Verpflichtung zur Wahrung des Berufsgeheimnisses gemäß Artikel 339

des Vertrags über die Arbeitsweise der Europäischen Union oder gleichwertigen geltenden Rahmenregelungen nach.

(2) Die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates[9] gilt hinsichtlich der Anträge auf Zugang der Öffentlichkeit zu Dokumenten, die sich im Besitz des CERT-EU befinden, einschließlich der in jener Verordnung festgelegten Pflicht zur Anhörung anderer Organe, Einrichtungen und Stellen der Union, wenn eine Anfrage deren Dokumente betrifft.

(3) Die Verarbeitung personenbezogener Daten im Rahmen dieser Verordnung unterliegt der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates.

(4) Der Umgang des CERT-EU und der Organe, Einrichtungen und sonstigen Stellen der Union mit Informationen erfolgt im Einklang mit der [vorgeschlagenen Verordnung über die Informationssicherheit].

(5) Wenden sich nationale Sicherheits- und Nachrichtendienste aus eigener Initiative oder auf eigenes Bestreben an das CERT-EU, so ist dies der Direktion Sicherheit der Kommission und dem Vorsitz des IICB unverzüglich mitzuteilen.

Artikel 19
Weitergabepflichten

(1) Damit das CERT-EU in der Lage ist, das Management von Sicherheitslücken und die Bewältigung von Sicherheitsvorfällen zu koordinieren, kann es von den Organen, Einrichtungen und sonstigen Stellen der Union verlangen, ihm Informationen aus ihren jeweiligen IT-Systemverzeichnissen zu übermitteln, die für die Unterstützung durch das CERT-EU relevant sind. Die betreffenden Organe, Einrichtungen oder Stellen übermitteln die verlangten Informationen und alle späteren Aktualisierungen unverzüglich.

(2) Die Organe, Einrichtungen und sonstigen Stellen der Union übermitteln dem CERT-EU auf Anfrage unverzüglich die digitalen Informationen, die bei der Nutzung von den an den jeweiligen Sicherheitsvorfällen beteiligten Geräten erzeugt wurden. Das CERT-EU kann weiter präzisieren, welche Arten solcher digitalen Informationen es für die Lageerfassung und die Reaktion auf den Sicherheitsvorfall benötigt.

(3) Das CERT-EU darf spezifische Informationen über Sicherheitsvorfälle, aus denen die Identität der von dem Sicherheitsvorfall betroffenen Organe, Einrichtungen oder Stellen der Union hervorgeht, nur mit Einwilligung der betroffenen Organe, Einrichtungen oder Stellen weitergeben. Das CERT-EU darf spezifische Informationen über Sicherheitsvorfälle, aus denen die Identität der Zielgruppe des Cybersicherheitsvorfalls hervorgeht, nur mit Einwilligung der betroffenen Gruppe weitergeben.

(4) Die Weitergabepflichten erstrecken sich nicht auf EU-Verschlusssachen (EU-VS) und nicht auf Informationen, die Organe, Einrichtungen oder sonstige Stelle der Union von einem Sicherheits- oder Nachrichtendienst oder einer

[9] Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

Strafverfolgungsbehörde eines Mitgliedstaats unter dem ausdrücklichen Vorbehalt erhalten haben, dass sie nicht an das CERT-EU weitergegeben werden.

Artikel 20
Meldepflichten

(1) Alle Organe, Einrichtungen und sonstigen Stellen der Union übermitteln dem CERT-EU unverzüglich und in jedem Fall spätestens 24 Stunden nachdem sie von ihnen Kenntnis erlangt haben, eine erste Meldung über erhebliche Cyberbedrohungen, erhebliche Sicherheitslücken und erhebliche Sicherheitsvorfälle.

In hinreichend begründeten Fällen und im Einvernehmen mit dem CERT-EU können die betreffenden Organe, Einrichtungen und sonstigen Stellen der Union von der im vorstehenden Absatz festgelegten Frist abweichen.

(2) Ferner melden die Organe, Einrichtungen und sonstigen Stellen der Union dem CERT-EU unverzüglich sachdienliche technische Einzelheiten über Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfälle, die eine Erkennung, eine Reaktion oder Abhilfemaßnahmen ermöglichen. Sofern verfügbar umfasst die Meldung:

a) relevante Gefährdungsindikatoren,

b) relevante Erkennungsmechanismen;

c) potenzielle Auswirkungen;

d) relevante Abhilfemaßnahmen.

(3) Das CERT-EU legt der ENISA monatlich einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu erheblichen Cyberbedrohungen, erheblichen Sicherheitslücken und erheblichen Sicherheitsvorfällen enthält, die gemäß Absatz 1 gemeldet wurden.

(4) Der IICB kann Leitlinien und Empfehlungen zu den Modalitäten und dem Inhalt der Meldung herausgeben. Das CERT-EU verbreitet die sachdienlichen technischen Einzelheiten, um eine proaktive Erkennung und Reaktion oder Abhilfemaßnahmen durch die Organe, Einrichtungen und sonstigen Stellen der Union zu ermöglichen.

(5) Die Meldepflichten erstrecken sich nicht auf EU-Verschlusssachen (EU-VS) und nicht auf Informationen, die Organe, Einrichtungen oder sonstige Stelle der Union von einem Sicherheits- oder Nachrichtendienst oder einer Strafverfolgungsbehörde eines Mitgliedstaats unter dem ausdrücklichen Vorbehalt erhalten haben, dass sie nicht an das CERT-EU weitergegeben werden.

Artikel 21
Koordinierung der Reaktion auf Sicherheitsvorfälle und Zusammenarbeit bei erheblichen Sicherheitsvorfällen

(1) Als zentrale Stelle für den Austausch von Informationen zur Cybersicherheit und die Koordinierung der Reaktion auf Vorfälle erleichtert das CERT-EU den Austausch von Informationen über Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfälle zwischen:

a) Organen, Einrichtungen und sonstigen Stellen der Union,

b) den in den Artikeln 16 und 17 genannten Stellen.

(2) Das CERT-EU erleichtert die Koordinierung zwischen den Organen, Einrichtungen und sonstigen Stellen der Union bei der Reaktion auf Sicherheitsvorfälle, unter anderem durch

a) einen Beitrag zur kontinuierlichen externen Kommunikation,

b) gegenseitige Hilfe;

c) optimale Nutzung der operativen Ressourcen;

d) die Koordinierung mit anderen Krisenreaktionsmechanismen auf Unionsebene.

(3) Das CERT-EU unterstützt die Organe, Einrichtungen und sonstigen Stellen der Union bei der Lageerfassung im Falle von Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfällen.

(4) Der IICB legt Leitlinien für die Koordinierung der Reaktion auf Sicherheitsvorfälle und die Zusammenarbeit bei erheblichen Sicherheitsvorfällen vor. Wenn ein Sicherheitsvorfall mutmaßlich einen kriminellen Hintergrund hat, formuliert das CERT-EU Ratschläge für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

Artikel 22
Größere Angriffe

(1) Das CERT-EU koordiniert die Maßnahmen der Organe, Einrichtungen und sonstigen Stellen der Union zur Bewältigung größerer Angriffe. Es führt ein Verzeichnis der technischen Fachkenntnisse, die für die Reaktion auf solche Angriffe notwendig sind.

(2) Die Organe, Einrichtungen und sonstigen Stellen der Union tragen zu dem Verzeichnis der technischen Fachkenntnisse bei, indem sie eine jährlich aktualisierte Liste ihrer jeweiligen Sachverständigen mit Angaben zu deren spezifischen technischen Qualifikationen übermitteln.

(3) Mit Zustimmung der betroffenen Organe, Einrichtungen und sonstigen Stellen der Union kann das CERT-EU gemäß den Arbeitsanweisungen der Gemeinsamen Cyber-Einheit auch Sachverständige aus der in Absatz 2 genannten Liste für einen Beitrag zu der Reaktion auf einen größeren Angriff in einem Mitgliedstaat hinzuziehen.

Kapitel VI
SCHLUSSBESTIMMUNGEN

Artikel 23
Erste Umschichtung von Haushaltsmitteln

Die Kommission schlägt die Umschichtung personeller und finanzieller Ressourcen von den entsprechenden Organen, Einrichtungen und sonstigen Stellen der Union zum Haushaltsplan der Kommission vor. Die Umschichtung wird zum Zeitpunkt der Annahme des ersten Haushaltsplans nach dem Inkrafttreten dieser Verordnung wirksam.

Artikel 24
Überprüfung

(1) Der IICB erstattet der Kommission mit Unterstützung des CERT-EU regelmäßig Bericht über die Durchführung dieser Verordnung. Der IICB kann auch Empfehlungen an die Kommission richten, Änderungen dieser Verordnung vorzuschlagen.

(2) Die Kommission erstattet dem Europäischen Parlament und dem Rat spätestens 48 Monate nach dem Inkrafttreten dieser Verordnung und danach alle drei Jahre Bericht über die Durchführung dieser Verordnung.

(3) Die Kommission evaluiert die Funktionsweise dieser Verordnung und erstattet dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen frühestens fünf Jahren nach dem Inkrafttreten Bericht.

Artikel 25
Inkrafttreten

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

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

Geschehen zu Brüssel am […]

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

FINANZBOGEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

1.2. Politikbereich(e)

1.3. Der Vorschlag/Die Initiative betrifft

1.4. Ziele

1.4.1. Allgemeine(s) Ziel(e)

1.4.2. Einzelziel(e)

1.4.3. Erwartete Ergebnisse und Auswirkungen

1.4.4. Leistungsindikatoren

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich eines ausführlichen Zeitplans für die Durchführung der Initiative.

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

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

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

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

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

2.2. Verwaltungs- und Kontrollsystem(e)

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

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

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

2.3. Prävention von Betrug und Unregelmäßigkeiten

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

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

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

3.2.5. Finanzierungsbeteiligung Dritter

3.3. Geschätzte Auswirkungen auf die Einnahmen

FINANZBOGEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

1.2. Politikbereich(e)

Europäische öffentliche Verwaltung

Der Vorschlag betrifft Maßnahmen, die ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union gewährleisten.

1.3. Der Vorschlag/Die Initiative betrifft

☑ eine neue Maßnahme

☐ eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme[10]

☐ die Verlängerung einer bestehenden Maßnahme

☑ die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme

1.4. Ziele

1.4.1. Allgemeine(s) Ziel(e)

– Schaffung eines Rahmens zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in den Organen, Einrichtungen und sonstigen Stellen der Union

– Schaffung einer neuen Rechtsgrundlage für das CERT-EU zur Stärkung seines Mandats und seiner Finanzausstattung.

1.4.2. Einzelziel(e)

1. Verpflichtung der Organe, Einrichtungen und sonstigen Stellen der Union zur Schaffung eines internen Rahmens für das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken
2. Verpflichtung der Organe, Einrichtungen und sonstigen Stellen der Union zur Berichterstattung über ihren jeweiligen Rahmen für das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken und über Cybersicherheitsvorfälle
3. Festlegung von Vorschriften über die Organisation und Arbeitsweise des Cybersicherheitszentrums für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) und über die Organisation und Arbeitsweise des Interinstitutionellen Cybersicherheitsbeirats (IICB)

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

4. Beitrag zur Gemeinsamen Cyber-Einheit

1.4.3. Erwartete Ergebnisse und Auswirkungen

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

– Interne Rahmen für das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken, Cybersicherheitsgrundregeln, regelmäßige Bewertungen des Reifegrads und Cybersicherheitspläne der Organe, Einrichtungen und sonstigen Stellen der Union
– Ausbau der Cyberresilienz und der Kapazitäten zur Reaktion auf Sicherheitsvorfälle der Organe, Einrichtungen und sonstigen Stellen der Union
– Modernisierung des CERT-EU
– Beitrag zur Gemeinsamen Cyber-Einheit

1.4.4. Leistungsindikatoren

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

– Rahmen und Grundregeln eingeführt, regelmäßige Bewertungen des Reifegrads und Durchführung der Cybersicherheitspläne in den Organen, Einrichtungen und sonstigen Stellen der Union
– Verbesserter Umgang mit Sicherheitsvorfällen
– Stärkere Sensibilisierung der Führungskräfte der Organe, Einrichtungen und sonstigen Stellen der Union für Cybersicherheitsrisiken
– Angleichung der Ausgaben für IKT-Sicherheit als Prozentsatz der gesamten IKT-Ausgaben
– Starke Führungsrolle des IICB und des CERT-EU
– Vermehrter Informationsaustausch zwischen den Organen, Einrichtungen und sonstigen Stellen der Union und mit einschlägigen Stellen und Interessenträgern in der EU
– Verstärkte Zusammenarbeit im Bereich der Cybersicherheit mit einschlägigen Stellen und Interessenträgern in der EU über das CERT-EU und die ENISA

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich eines ausführlichen Zeitplans für die Durchführung der Initiative.

Der Vorschlag zielt darauf ab, die Cyberresilienz der Organe, Einrichtungen und sonstigen Stellen der Union zu erhöhen, Ungleichheiten in der Resilienz zwischen ihnen zu verringern sowie die gemeinsame Lageerfassung und die kollektive Vorsorge- und Reaktionsfähigkeit zu verbessern. Der Vorschlag steht voll und ganz im Einklang mit anderen einschlägigen Initiativen und insbesondere dem Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 [NIS-2-Vorschlag]. Der Vorschlag ist ein wesentlicher Bestandteil der EU-Strategie für die Sicherheitsunion und der Cybersicherheitsstrategie der EU für die digitale Dekade.

Der Verordnungsvorschlag soll von der Europäischen Kommission im Oktober 2021 vorgelegt werden; die Annahme der Verordnung durch das Europäische Parlament und den Rat wird voraussichtlich 2022 erfolgen, und die Bestimmungen werden ab dem Inkrafttreten der Verordnung gelten. Die in diesem Finanzbogen beschriebenen finanziellen und personellen Auswirkungen werden voraussichtlich 2023 einsetzen. 2021 wurde bereits eine Vorbereitungsphase eingeleitet, aber die Vorarbeiten in den Jahren 2021 und 2022 fallen nicht unter die finanziellen Auswirkungen des Vorschlags.

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

Gründe für Maßnahmen auf europäischer Ebene (ex ante)

Von 2019 bis 2021 stieg die Zahl der gegen die Organe, Einrichtungen und sonstigen Stellen der Union gerichteten erheblichen Sicherheitsvorfälle dramatisch, die von Verursachern ausgingen, die als „fortgeschrittene andauernde Bedrohung" (Advanced Persistent Threat, APT) eingestuft wurden. Im ersten Halbjahr 2021 waren bereits ebenso viele erhebliche Sicherheitsvorfälle zu verzeichnen wie 2020 insgesamt. Dies spiegelt sich auch in der Zahl der 2020 vom CERT-EU analysierten forensischen Abbilder (Momentaufnahmen der Inhalte betroffener Systeme oder Geräte) wider, die sich im Vergleich zu 2019 verdreifacht hat, während die Zahl der erheblichen Sicherheitsvorfälle seit 2018 sogar um mehr als das Zehnfache gestiegen ist.

Die Cybersicherheitsreife variiert erheblich zwischen den Organen, Einrichtungen und sonstigen Stellen.[11] Diese Verordnung gewährleistet, dass alle Organe, Einrichtungen und sonstigen Stellen der Union grundlegende Sicherheitsmaßnahmen umsetzen und zusammenarbeiten im Interesse einer offenen und effizienten europäischen Verwaltung.

Die zu erhaltenden Systeme fallen unter die Autonomie der Organe, Einrichtungen und sonstigen Stellen der Union und werden von ihnen betrieben; die vorgeschlagenen Maßnahmen könnten von den Mitgliedstaaten nicht aufgestellt werden.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Die NIS-Richtlinie war das erste horizontale Binnenmarktinstrument, mit dem die Resilienz von Netzen und Systemen in der Union gegen Cybersicherheitsrisiken verbessert werden sollte. Seit ihrem Inkrafttreten im Jahr 2016 hat sie erheblich zur Anhebung des gemeinsamen Cybersicherheitsniveaus in den Mitgliedstaaten beigetragen. Der Vorschlag für die NIS2-Richtlinie soll diese Maßnahmen weiter verbessern.

Die Verordnung sieht vergleichbare Maßnahmen für die Organe, Einrichtungen und sonstigen Stellen der Union vor.

[11] Quelle: [Sonderbericht des EuRH über Cybersicherheit in den Organen, Einrichtungen und sonstigen Stellen der Union].

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

Der Vorschlag ist mit dem Mehrjährigen Finanzrahmen vereinbar und ein wesentlicher Bestandteil der EU-Strategie für die Sicherheitsunion und der Cybersicherheitsstrategie der EU für die digitale Dekade.

Gemäß dem Vorschlag sollen Maßnahmen angewandt werden, die ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union gewährleisten. Der Vorschlag steht im Einklang mit dem Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 [NIS-2-Vorschlag].

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

Die Wahrnehmung der Aufgaben durch das CERT-EU erfordert spezifische Profile und bringt zusätzliche Arbeitsbelastung, die ohne eine Aufstockung der personellen und finanziellen Ressourcen nicht aufgefangen werden kann.

1.6. Laufzeit und finanzielle Auswirkungen des Vorschlags/der Initiative

☐ **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**

– Die finanziellen Auswirkungen dürften mit dem ersten, nach dem Inkrafttreten dieser Verordnung angenommenen Haushaltsplan beginnen. Eine Umschichtung von Ressourcen von den Organen und wichtigsten Einrichtungen der Union zur Kommission würde im ersten Jahr erfolgen, das als Übergangsjahr gilt; diese Umschichtung sowie andere Mittelzuweisungen und Umschichtungen erfolgen im Rahmen der jährlichen Haushaltspläne. Wenn die Verordnung 2022 angenommen wird, ist das Haushaltsjahr 2023 das Übergangsjahr, und 2024 läuft die Haushaltsausführung planmäßig.

1.7. Vorgeschlagene Methode(n) der Mittelverwaltung[12]

☑ **Direkte Mittelverwaltung** durch die Kommission und die einzelnen Organe, Einrichtungen und sonstigen Stellen der Union

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

– ☐ durch Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit den Mitgliedstaaten

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

– ☐ Drittländer oder die von ihnen benannten Einrichtungen;

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben);

– ☐ die EIB und den Europäischen Investitionsfonds;

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

– ☐ öffentlich-rechtliche Körperschaften;

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern 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.*

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

Anmerkungen

Bei Anwendung der Verwaltungs- und Finanzverfahren handelt das CERT-EU unter Aufsicht der Kommission.

Im Verordnungsentwurf vorgesehene zusätzliche Mittel:

Durch die Umsetzung der Artikel 12 und 13 des Verordnungsentwurfs wird der Dienstekatalog um zusätzliche Basisdienste erweitert. Bei planmäßiger Durchführung werden die folgenden zusätzlichen Ressourcen benötigt (bis zum Ende des MFR Ende 2027): 21 VZÄ und 14,05 Mio. EUR.

Die zusätzlichen Haushaltsmittel verteilen sich wie folgt auf die verschiedenen Aufgaben:

a) Für die Wahrnehmung der in Artikel 12 Absatz 2 Buchstaben a, b, c und e genannten Aufgaben für die Organe, Einrichtungen und sonstigen Stellen der Union: 13,75 VZÄ und 11,275 Mio. EUR;

b) Für die Wahrnehmung der in Artikel 12 Absatz 3 genannten Aufgaben (Beitrag zur Gemeinsamen Cyber-Einheit): 2 VZÄ und 381 000 EUR;

c) Für die Wahrnehmung der in Artikel 12 Absatz 4 genannten Aufgaben (strukturierte Zusammenarbeit mit ENISA): 0,25 VZÄ und 236 000 EUR;

d) Für die Wahrnehmung der in Artikel 12 Absatz 6 genannten Aufgaben (Cybersicherheitsübungen): 0,25 VZÄ und 79 000 EUR;

e) Für die Wahrnehmung der in Artikel 12 Absatz 2 Buchstabe d und Artikel 13 genannten Aufgaben (Analyse und Berichterstattung über die Durchführung der Verordnung, Vorbereitung von Leitlinien, Empfehlungen und Aufrufen zum Tätigwerden): 3,75 VZÄ und 2,079 Mio. EUR.

f) Für die Wahrnehmung von Aufgaben zur Unterstützung des Sekretariats des Interinstitutionellen Cybersicherheitsbeirats (IICB): 1 VZÄ.

Überblick über die derzeitigen Ressourcen und Übergang zur planmäßigen Umsetzung

Im September 2021 arbeitete das CERT-EU mit den folgenden Ressourcen:

– Planstellen und Stellen für abgeordnete Bedienstete: 14 VZÄ,

– im Rahmen von Leistungsvereinbarungen finanzierte Vertragsbedienstete: 24 VZÄ,

– insgesamt 38 VZÄ.

Der Etat des CERT-EU belief sich 2020 auf: 250 000 EUR aus dem Haushalt der Kommission, 3,5 Mio. EUR durch zweckgebundene Einnahmen aus Leistungsvereinbarungen. Insgesamt: 3,75 Mio. EUR. Bei diesem Betrag handelte es sich um den Gesamtetat des CERT-EU, der Schulungen, Hardware, Software, Dienstreisen, Unterstützung, Vertragsbedienstete und Konferenzen abdeckte.

Sobald die Verordnung in Kraft getreten ist, sind folgende Ressourcen für das CERT-EU vorgesehen:

– Planstellen: 34 VZÄ,

– Vertragsbedienstete: 15 VZÄ,

– insgesamt 49 VZÄ, d. h. netto 11 VZÄ mehr.

Durch das neue Verhältnis zwischen Planstellen und Vertragsbediensteten wird das Problem angegangen, erfahrene Cybersicherheitsfachkräfte, die auf dem Arbeitsmarkt selten zu finden sind, einzustellen und zu halten.

Außerdem wird in der Generaldirektion für Informatik der Kommission ein Vertragsbediensteter oder eine Vertragsbedienstete (VZÄ) für die Unterstützung des IICB (Interinstitutioneller Cybersicherheitsbeirat) benötigt.

Insgesamt werden für die Durchführung der Verordnung also 21 zusätzliche VZÄ benötigt (20 VZÄ für das CERT-EU und 1 VZÄ für Generaldirektion für Informatik der Kommission). Ausgeglichen wird dies durch den gleichzeitigen Abbau von 9 Vertragsbediensteten-VZÄ im CERT-EU, die zuvor durch zweckgebundene Einnahmen aus Leistungsvereinbarungen finanziert wurden.

2024, nach dem Übergangszeitraum, wird der Etat des CERT-EU für andere als personelle Ressourcen die vorstehend unter den Buchstaben a bis e genannten Aufgaben abdecken und soll wie folgt finanziert werden:

– 8,921 Mio. EUR pro Jahr von den Organen der Union aus der Rubrik 7 des Unionshaushalts,

– 2,459 Mio. EUR von den Organen, Einrichtungen und sonstigen Stellen der Union aus den Rubriken 1 bis 6 des Unionshaushalts,

– 2,670 Mio. EUR von selbstfinanzierten Organen, Einrichtungen und sonstigen Stellen der Union.

– Etat des CERT-EU insgesamt: 14,05 Mio. EUR.

Die in Artikel 12 Absatz 5 genannten Aufgaben sind in seinem Dienstekatalog nicht aufgeführt; sie sind kostenpflichtige Leistungen. Dabei handelt es sich um relativ geringe Nebenkosten, die überwiegend vorübergehender Natur sind, und die Kosten dieser Dienste werden von den Leistungsempfängern im Wege von Leistungsvereinbarungen oder schriftlichen Vereinbarungen zurückgefordert.

Beiträge zum Personal des CERT-EU: die Organe und wichtigsten Einrichtungen der Union leisten einen angemessenen Beitrag, der im Verhältnis zum jeweiligen Anteil der AD-Planstellen der Organisation steht. Es sollte geprüft werden, ob die EZB und die EIB ebenfalls einen angemessenen Beitrag leisten können, indem sie ständiges Personal entsenden.

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

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

Die Kommission wird mit der Hilfe des IICB und des CERT-EU in regelmäßigen Abständen überprüfen, wie die Verordnung funktioniert, und dem Europäischen Parlament und dem Rat zum ersten Mal spätestens 48 Monate nach Inkrafttreten dieser Verordnung und anschließend alle drei Jahre darüber Bericht erstatten.

Für die Überprüfungen werden im Wesentlichen die Datenquellen des IICB und des CERT-EU herangezogen. Abgesehen davon können bei Bedarf spezifische Datenerhebungsinstrumente verwendet werden wie z. B. Erhebungen der Organe, Einrichtungen und sonstigen Stellen der Union, der ENISA oder des CSIRTs-Netzwerks.

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

Maßnahmen auf der Grundlage der Verordnung werden von den betreffenden Organen, Einrichtungen und sonstigen Stellen der Union im Einklang mit den jeweils geltenden Regeln und Vorschriften verwaltet.

Die administrative und finanzielle Verwaltung der CERT-EU-Tätigkeiten ist in die Verwaltung der Kommission eingebettet und unterliegt ihren geltenden Verwaltungs- und Durchführungsmechanismen, Zahlungsmodalitäten und Kontrollen.

Der interne Rechnungsprüfer der Kommission übt gegenüber dem CERT-EU dieselben Befugnisse aus wie gegenüber den Kommissionsdienststellen.

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

Die Risiken sind sehr gering, da das CERT-EU verwaltungstechnisch als Taskforce der Kommission dem Generaldirektor für Informatik unterstellt ist, und der IICB ist dem derzeitigen CERT-EU-Lenkungsausschuss nachgebildet. Das Ökosystem für die Haushaltsführung und interne Kontrolle ist daher bereits vorhanden.

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 Verfahren für Auftragsvergabe, Haushaltsführung und Kontrolle sind bereits vorhanden und haben sich bewährt. Die Kostenwirksamkeit der Kontrollen und das Fehlerrisiko entsprechen denen aller Organe, Einrichtungen und sonstigen Stellen der Union bzw. im Falle der CERT-EU-Tätigkeiten denen der Kommission.

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.

Für die CERT-EU-Tätigkeiten gelten die Haushaltsführungs- und internen Kontrollsysteme der Kommission.

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 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) uneingeschränkt Anwendung.

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 Ausgabe	Beitrag			
	Nummer	GM/NGM [13]	von EFTA-Ländern[14]	von Kandidatenländern[15]	von Drittstaaten	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
1 bis 6	Haushaltslinien für die Beiträge der Union zu dezentralen Agenturen und Einrichtungen	GM	NEIN	NEIN	NEIN	NEIN
7	Haushaltslinien für Dienstbezüge, IT-Ausgaben und sonstige Verwaltungsausgaben in den verschiedenen Einzelplänen des EU-Haushalts	NGM	NEIN	NEIN	NEIN	NEIN

- Neu zu schaffende Haushaltslinien

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

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Beitrag			
	Nummer	GM/NGM	von EFTA-Ländern	von Kandidatenländern	von Drittstaaten	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
	Kein Eintrag.		JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN

[13] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.
[14] EFTA: Europäische Freihandelsassoziation.
[15] Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1. Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

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

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

in Mio. EUR (3 Dezimalstellen)

Rubrik des mehrjährigen Finanzrahmens	1 bis 6	Haushaltslinien für die Beiträge der Union zu dezentralen Agenturen und Einrichtungen

GD: Verschiedene			Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	Jahr **2027**	**INSGESAMT**
○ Operative Mittel								
Haushaltslinien für die Beiträge der Union zu dezentralen Agenturen und Einrichtungen (xx 10 xx xx)[16]	Verpflichtungen	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Zahlungen	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben[17]								
Haushaltslinie		(3)						
Mittel INSGESAMT für GD: Verschiedene	Verpflichtungen	=1a + 1b + 3	2,459	2,459	2,459	2,459	2,459	12,293
	Zahlungen	= 2a + 2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Gemäß dem offiziellen Eingliederungsplan.

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

○ Operative Mittel INSGESAMT	Verpflichtungen	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Zahlungen	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT		(6)						
Mittel INSGESAMT unter den RUBRIKEN 1 bis 6 des Mehrjährigen Finanzrahmens	Verpflichtungen	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Zahlungen	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

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

○ Operative Mittel INSGESAMT (alle operativen Rubriken)	Verpflichtungen	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Zahlungen	(5)	2,459	2,459	2,459	2,459	2,459	12,293
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsausgaben INSGESAMT (alle operativen Rubriken)		(6)						
Mittel INSGESAMT unter den RUBRIKEN 1 bis 6 des Mehrjährigen Finanzrahmens (Referenzbetrag)	Verpflichtungen	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Zahlungen	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Rubrik des mehrjährigen Finanzrahmens	7	„Verwaltungsausgaben“

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

in Mio. EUR (3 Dezimalstellen)

		Jahr **2023**	Jahr **2024**	Jahr **2025**	Jahr **2026**	**Jahr 2027**	**INSGESAMT**
GD: DIGIT (CERT-EU)							
○ Personal		1,184	2,126	2,754	3,225	3,225	12,514
○ Sonstige Verwaltungsmittel		7,938	8,921	8,921	8,921	8,921	43,622
INSGESAMT GD DIGIT (CERT-EU)	Mittel	9,122	11,047	11,675	12,146	12,146	56,136

Mittel INSGESAMT unter der RUBRIK 7 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	9,122	11,047	11,675	12,146	12,146	**56,136**

in Mio. EUR (3 Dezimalstellen)

		Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	**INSGESAMT**
Mittel INSGESAMT unter den RUBRIKEN 1 bis 7 des Mehrjährigen Finanzrahmens	Verpflichtungen	11,581	13,506	14,134	14,605	14,605	68,429
	Zahlungen	11,581	13,506	14,134	14,605	14,605	68,429

(*) Die Beiträge von eigenfinanzierten Organen, Einrichtungen und sonstige Stellen der Union werden auf 2,670 Mio. EUR pro Jahr geschätzt (für die fünf Jahre insgesamt 13,350 Mio. EUR). Die Beiträge werden zweckgebundene Einnahmen für das CERT-EU sein. Die vorstehenden Tabellen enthalten nur die geschätzten Gesamtauswirkungen auf den Unionshaushalt; sie enthalten nicht diese Beiträge.

3.2.2. Geschätzte Ergebnisse, die mit operativen Mitteln finanziert werden

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

Ziele und Ergebnisse angeben ⇩			Jahr **N**		Jahr **N+1**		Jahr **N+2**		Jahr **N+3**		Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.						**INSGESAMT**	
	ERGEBNISSE																	
	Art[18]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[19]...																		
– Ergebnis																		
– Ergebnis																		
– Ergebnis																		
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2 ...																		
– Ergebnis																		
Zwischensumme für Einzelziel Nr. 2																		
INSGESAMT																		

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

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

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

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

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

in Mio. EUR (3 Dezimalstellen)

	Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027	**INSGESAMT**
RUBRIK 7 des Mehrjährigen Finanzrahmens						
Personal						
Dauerplanstellen (AD)	1,099	2,041	2,669	3,14	3,14	12,089
Vertragsbedienstete	0,085	0,085	0,085	0,085	0,085	0,425
Sonstige Verwaltungsausgaben	7,938	8,921	8,921	8,921	8,921	43,622
Zwischensumme RUBRIK 7 des Mehrjährigen Finanzrahmens	9,122	11,047	11,675	12,146	12,146	56,136

Außerhalb der RUBRIK 7[20] des Mehrjährigen Finanzrahmens						
Personal						
Sonstige Verwaltungsausgaben						
Zwischensumme außerhalb der Rubrik 7 des Mehrjährigen Finanzrahmens						

INSGESAMT	9,122	11,047	11,675	12,146	12,146	56,136

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.

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

3.2.3.1. Geschätzter Personalbedarf

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

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

Schätzung in Vollzeitäquivalenten

		Jahr 2023	Jahr 2024	Jahr 2025	Jahr 2026	Jahr 2027		
O Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)								
20 01 02 01 (am Sitz und in den Vertretungen der Kommission)		7	13	17	20	20		
20 01 02 03 (in den Delegationen)								
01 01 01 01 (indirekte Forschung)								
01 01 01 11 (direkte Forschung)								
Sonstige Haushaltslinien (bitte angeben)								
O Externes Personal (in Vollzeitäquivalenten: VZÄ)[21]								
20 02 01 (VB, ANS und LAK der Globaldotation)		1	1	1	1	1		
20 02 03 (VB, ÖB, ANS, LAK und JFD in den Delegationen)								
XX 01 xx **yy zz** [22]	– am Sitz der Kommission							
	– in den Delegationen							
01 01 01 02 (VB, ANS und LAK – indirekte Forschung)								
01 01 01 12 (VB, ANS und LAK – direkte Forschung)								
Sonstige Haushaltslinien (bitte angeben)								
INSGESAMT		**8**	**14**	**18**	**21**	**21**		

XX steht für den jeweiligen Politikbereich bzw. Haushaltstitel.

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumschichtungen 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	Die Aufgaben und Tätigkeiten des CERT-EU gemäß der Verordnung, Kapitel IV und V, werden von Beamten wahrgenommen.
Externes Personal	Der oder die Vertragsbedienstete wird die Sekretariatsaufgaben des Interinstitutionellen Cybersicherheitsbeirat wahrnehmen.

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

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

3.2.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen

Der Vorschlag/Die Initiative

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

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

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

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

– ☐ erfordert eine Revision des MFR.

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

3.2.5. Finanzierungsbeteiligung Dritter

Der Vorschlag/Die Initiative

– ☑ sieht keine Kofinanzierung durch Dritte vor.[23]

– ☐ sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr **N**[24]	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.			Insgesamt
Kofinanzierende Einrichtung (bitte angeben)								
Kofinanzierung INSGESAMT								

[23] Die zweckgebundenen Einnahmen aus der sporadischen Erbringung von Diensten für nichtkonstituente Organisationen gemäß Artikel 12 Absatz 5 Buchstabe c wurden nicht veranschlagt, weil sie geringfügig sein dürften.

[24] 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.

3.3. 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[25]						
		Jahr **N**	Jahr **N+1**	Jahr **N+2**	Jahr **N+3**	Bei länger andauernden Auswirkungen (siehe 1.6.) bitte weitere Spalten einfügen.		
Artikel ….								

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

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

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

EUROPÄISCHE
KOMMISSION

Brüssel, den 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ANHÄNGE

des

Vorschlags für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ANHANG I

Die Cybersicherheitsgrundregeln betreffen folgende Bereiche:

(1) Cybersicherheitspolitik, einschließlich der Ziele und Prioritäten für die Sicherheit von Netz- und Informationssystemen, insbesondere hinsichtlich der Nutzung von Cloud-Computing-Diensten (im Sinne des Artikels 4 Nummer 19 der Richtlinie [NIS-2-Vorschlag]) und technischer Vorkehrungen zur Ermöglichung der Telearbeit;

(2) Organisation der Cybersicherheit, einschließlich Festlegung der Aufgaben und Zuständigkeiten;

(3) Verwaltung der Vermögenswerte, einschließlich IT-Bestandsverzeichnis und IT-Netzkartografie;

(4) Zugangskontrolle;

(5) Betriebssicherheit;

(6) Kommunikationssicherheit;

(7) Beschaffung, Entwicklung und Wartung von Systemen;

(8) Lieferantenbeziehungen;

(9) Management von Sicherheitsvorfällen, einschließlich der Konzepte zur Verbesserung der Abwehrbereitschaft, Reaktion und Folgenbewältigung bei Sicherheitsvorfällen und der Zusammenarbeit mit dem CERT-EU, z. B. bei der Aufrechterhaltung der Sicherheitsüberwachung und -protokollierung;

(10) Betriebskontinuitätsmanagement und Krisenmanagement;

(11) Ausbildungs-, Aufklärungs- und Schulungsprogramme im Bereich der Cybersicherheit.

ANHANG II

Im Einklang mit den Leitlinien und Empfehlungen des IICB berücksichtigen die Organe, Einrichtungen und sonstigen Stellen der Union bei der Umsetzung der Cybersicherheitsgrundregeln und in ihren Cybersicherheitsplänen zumindest die folgenden besonderen Cybersicherheitsmaßnahmen:

(1) konkrete Schritte für den Übergang zu einer „Zero-Trust-Architektur“ (d. h. zu einem Sicherheitsmodell mit einer Reihe von Grundsätzen für die Systemgestaltung und eine koordinierte Cybersicherheits- und Systemmanagementstrategie, die auf der Anerkennung beruhen, dass sowohl innerhalb als auch außerhalb der herkömmlichen Netzgrenzen Bedrohungen bestehen);

(2) Einführung der Multifaktor-Authentifizierung als Norm in allen Netz- und Informationssystemen;

(3) Schaffung von Sicherheit in der Software-Lieferkette durch Kriterien für die sichere Softwareentwicklung und -bewertung;

(4) Erweiterung der Vorschriften für die Auftragsvergabe, um ein hohes gemeinsames Cybersicherheitsniveau zu erleichtern, und zwar durch

   (a) die Beseitigung vertraglicher Hindernisse, die den Informationsaustausch der IT-Dienstleister über Sicherheitsvorfälle, Schwachstellen und Cyberbedrohungen mit dem CERT-EU einschränken;

   (b) die vertragliche Pflicht zur Meldung von Sicherheitsvorfällen, Sicherheitslücken und Cyberbedrohungen sowie zur angemessenen Bewältigung und Überwachung von Sicherheitsvorfällen.