EUROPÄISCHE UNION

DAS EUROPÄISCHE PARLAMENT **DER RAT**

Brüssel, den 29. November 2023
(OR. en)

2022/0085 (COD) **PE-CONS 57/23**

CYBER 215
TELECOM 267
INST 341
CSC 445
CSCI 163
INF 206
FIN 928
BUDGET 27
DATAPROTECT 236
CODEC 1607

GESETZGEBUNGSAKTE UND ANDERE RECHTSINSTRUMENTE

Betr.:	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

VERORDNUNG (EU, Euratom) 2023/…
DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom …

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[1],

[1] Standpunkt des Europäischen Parlaments vom 21. November 2023 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom ….

in Erwägung nachstehender Gründe:

(1) Im digitalen Zeitalter ist die Informations- und Kommunikationstechnik der Grundstein einer offenen, effizienten und unabhängigen europäischen Verwaltung. Die Cybersicherheitsrisiken werden durch die Weiterentwicklung der Technologie und die zunehmende Komplexität und Vernetzung digitaler Systeme verstärkt, wodurch die Einrichtungen der Union anfälliger für Cyberbedrohungen und Sicherheitsvorfälle werden, was die Aufrechterhaltung ihres Dienstbetriebs und ihre Fähigkeit zur Sicherung ihrer Daten gefährdet. Während die zunehmende Inanspruchnahme von Cloud-Diensten, die allgegenwärtige Nutzung der Informations- und Kommunikationstechnik (im Folgenden „IKT“), der hohe Digitalisierungsgrad, Telearbeit sowie die sich weiterentwickelnde Technologie und Konnektivität zentrale Merkmale aller Tätigkeiten der Einrichtungen der Union sind, wird der digitalen Resilienz noch nicht ausreichend Rechnung getragen.

(2) Die Cyberbedrohungslange, mit der die Einrichtungen 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 der Bedrohungen 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 IKT-Umgebungen der Einrichtungen 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 eine einzige Einrichtung der Union beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und langanhaltende negative Auswirkungen auf andere Einrichtungen der Union haben können. Darüber hinaus sind die IKT-Umgebungen bestimmter Einrichtungen der Union mit den IKT-Umgebungen der Mitgliedstaaten verbunden, was dazu führt, dass ein Sicherheitsvorfall in einer Einrichtung der Union ein Cybersicherheitsrisiko für die IKT-Umgebungen der Mitgliedstaaten darstellt, und umgekehrt. Der Austausch spezifischer Informationen über Sicherheitsvorfälle kann die Aufdeckung ähnlicher Cyberbedrohungen oder Sicherheitsvorfälle, die Mitgliedstaaten betreffen, erleichtern.

(4) Die Einrichtungen 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 Einrichtungen. Für das Funktionieren der Einrichtungen der Union ist es daher erforderlich, dass sie ein hohes gemeinsames Cybersicherheitsniveau erreichen, indem Cybersicherheitsmaßnahmen durchgeführt werden, die den ermittelten Cybersicherheitsrisiken angemessen sind, sowie durch Informationsaustausch und Zusammenarbeit.

(5) Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[1] zielt darauf ab, die Cyberresilienz öffentlicher und privater Einrichtungen, der zuständigen Behörden und Einrichtungen sowie der Union insgesamt weiter zu verbessern und ihre Kapazitäten zur Reaktion auf Sicherheitsvorfälle zu stärken. Daher muss sichergestellt werden, dass die Einrichtungen der Union sich dem anschließen, indem sie Vorschriften festlegen, die mit der Richtlinie (EU) 2022/2555 im Einklang stehen und deren ehrgeizige Ziele widerspiegeln.

(6) Um ein hohes gemeinsames Cybersicherheitsniveau zu erreichen, ist es erforderlich, dass jede Einrichtung der Union einen internen Rahmen für Risikomanagement, Governance und Kontrolle im Bereich der Cybersicherheit (im Folgenden „Rahmen“) festlegt, der ein wirksames und umsichtiges Management aller Cybersicherheitsrisiken gewährleistet und die Sicherung der Betriebskontinuität und das Krisenmanagement berücksichtigt. In dem Rahmen sollten Cybersicherheitsstrategien, einschließlich Ziele und Prioritäten, für die Sicherheit von Netz- und Informationssystemen festgelegt werden, die die gesamte nicht für Verschlusssachen genutzte IKT-Umgebung abdecken. Der Rahmen sollte auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, Netz- und Informationssysteme und die physische Umgebung dieser Systeme vor Ereignissen wie Diebstahl, Brand, Überschwemmungen, Telekommunikations- oder Stromausfällen oder unbefugtem physischem Zugang zu, Beschädigung von und Eingriffen in Informationen und Informationsverarbeitungsanlagen von Einrichtungen der Union zu schützen, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von mittels Netz- und Informationssystemen gespeicherten, übermittelten, verarbeiteten oder zugänglichen Daten beeinträchtigen könnten.

---

[1] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

(7) Zur Bewältigung der in dem Rahmen ermittelten Cybersicherheitsrisiken sollte jede Einrichtung der Union geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen. Diese Maßnahmen sollten sich auf die in dieser Verordnung festgelegten Bereiche und Maßnahmen zum Management von Cybersicherheitsrisiken erstrecken, um die Cybersicherheit jeder Einrichtung der Union zu stärken.

(8) Die in dem Rahmen ermittelten Anlagen und Cybersicherheitsrisiken sowie die Schlussfolgerungen aus den regelmäßigen Bewertungen des Cybersicherheitsreifegrads sollten in den von jeder Einrichtung der Union erstellten Cybersicherheitsplan einfließen. Der Cybersicherheitsplan sollte die angenommenen Maßnahmen zum Management von Cybersicherheitsrisiken enthalten.

(9) Da es sich bei der Sicherstellung der Cybersicherheit um einen kontinuierlichen Prozess handelt, sollten die Eignung und Wirksamkeit der gemäß dieser Verordnung ergriffenen Maßnahmen regelmäßig im Lichte der sich verändernden Cybersicherheitsrisiken, Anlagen und Cybersicherheitsreifegrade der Einrichtungen der Union überprüft werden. Der Rahmen sollte regelmäßig und mindestens alle vier Jahre überprüft werden, während der Cybersicherheitsplan alle zwei Jahre oder erforderlichenfalls häufiger, im Anschluss an die Bewertungen des Cybersicherheitsreifegrads oder jeder gründlichen Überprüfung des Rahmens, überarbeitet werden sollte.

(10) Die von Einrichtungen der Union eingeführten Maßnahmen zum Management von Cybersicherheitsrisiken sollten Strategien umfassen, die darauf abzielen, den Quellcode nach Möglichkeit transparent zu machen, wobei Garantien für die Rechte von Dritten oder von Einrichtungen der Union zu berücksichtigen sind. Diese Strategien sollten in einem angemessenen Verhältnis zum Cybersicherheitsrisiko stehen und zielen darauf ab, die Analyse von Cyberbedrohungen zu erleichtern, ohne jedoch über die geltenden vertraglichen Bedingungen hinaus Offenlegungspflichten oder Rechte auf Zugang zu Code von Dritten zu schaffen.

(11) Open-Source-Cybersicherheitswerkzeuge und -anwendungen können zu einem höheren Maß an Offenheit beitragen. Offene Standards erleichtern die Interoperabilität zwischen Sicherheitswerkzeugen, was der Sicherheit der Interessenträger zugutekommt. Open-Source-Cybersicherheitswerkzeuge und -anwendungen können von einer größeren Entwicklergemeinschaft profitieren und damit eine Diversifizierung der Anbieter ermöglichen. Open Source kann zu einem transparenteren Verfahren für die Überprüfung von Werkzeugen für die Cybersicherheit und zu einem von der Gemeinschaft gesteuerten Prozess der Erkennung von Schwachstellen führen. Die Einrichtungen der Union sollten daher den Einsatz von Open-Source-Software und offenen Standards fördern können, indem sie Strategien verfolgen, die auf die Nutzung offener Daten und von Open Source als Teil der Sicherheit durch Transparenz abzielen.

(12) Aufgrund der Unterschiede zwischen den Einrichtungen der Union ist bei der Umsetzung dieser Verordnung Flexibilität erforderlich, da die Lösungen jeweils bedarfsgerecht zugeschnitten sein müssen. Die in dieser Verordnung festgelegten Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau sollten keine Verpflichtungen umfassen, die einen unmittelbaren Eingriff in die Wahrnehmung der Aufgaben der Einrichtungen der Union darstellen oder deren institutionelle Autonomie beeinträchtigen. Daher sollten diese Einrichtungen ihren eigenen Rahmen festlegen und ihre eigenen Maßnahmen zum Management von Cybersicherheitsrisiken und ihre eigenen Cybersicherheitspläne annehmen. Bei der Durchführung solcher Maßnahmen sollten – mit dem Ziel einer ordnungsgemäßen Verwaltung der Ressourcen und einer Kostenoptimierung – bestehende Synergieeffekte zwischen den Einrichtungen der Union gebührend berücksichtigt werden. Ferner sollte gebührend darauf geachtet werden, dass sich die Maßnahmen nicht negativ auf den effizienten Informationsaustausch und die Zusammenarbeit zwischen Einrichtungen der Union sowie zwischen Einrichtungen der Union und den entsprechenden Stellen in den Mitgliedstaaten auswirken.

(13) Im Interesse einer optimalen Nutzung der Ressourcen sollte in dieser Verordnung die Möglichkeit vorgesehen werden, dass zwei oder mehr Einrichtungen der Union mit ähnlichen Strukturen bei der Durchführung der Bewertungen des Cybersicherheitsreifegrads ihrer jeweiligen Einrichtungen zusammenarbeiten.

(14) Damit keine unverhältnismäßige finanzielle und administrative Belastung für die Einrichtungen der Union entsteht, sollten die Anforderungen an das Management von Cybersicherheitsrisiken in einem angemessenen Verhältnis zu den Cybersicherheitsrisiken stehen, denen die betreffenden Netz- und Informationssysteme ausgesetzt sind; dabei ist dem neuesten Stand solcher Maßnahmen Rechnung zu tragen. Jede Einrichtung der Union sollte bestrebt sein, einen angemessenen Prozentsatz ihres IKT-Haushalts für die Verbesserung ihres Cybersicherheitsniveaus zuzuweisen; längerfristig sollte ein Richtziel in der Größenordnung von mindestens 10 % angestrebt werden. Bei der Bewertung des Cybersicherheitsreifegrads sollte bewertet werden, ob die Ausgaben der Einrichtung der Union für Cybersicherheit in einem angemessenen Verhältnis zu den Cybersicherheitsrisiken stehen, denen sie ausgesetzt ist. Unbeschadet der Vorschriften über den Jahreshaushaltsplan der Union gemäß den Verträgen sollte die Kommission in ihrem Vorschlag für den ersten Jahreshaushaltsplan, der nach dem Inkrafttreten dieser Verordnung angenommen wird, bei der Bewertung des Haushalts- und Personalbedarfs der Einrichtungen der Union, wie er sich aus ihrem Ausgabenvoranschlag ergibt, den sich aus dieser Verordnung ergebenden Verpflichtungen Rechnung tragen.

(15) Ein hohes gemeinsames Cybersicherheitsniveau setzt voraus, dass die Cybersicherheit der Aufsicht der höchsten Managementebene der jeweiligen Einrichtung der Union unterstellt wird. Die höchste Managementebene der jeweiligen Einrichtung der Union sollte für die Durchführung dieser Verordnung verantwortlich sein, wozu auch die Festlegung des Rahmens, das Ergreifen von Maßnahmen zum Management von Cybersicherheitsrisiken und die Genehmigung des Cybersicherheitsplans gehört. Die Pflege der Cybersicherheitskultur, d. h. die Cybersicherheit in der täglichen Praxis, ist Bestandteil des Rahmens und der entsprechenden Maßnahmen zum Management von Cybersicherheitsrisiken in allen Einrichtungen der Union.

(16) Die Sicherheit von Netz- und Informationssystemen, in denen EU-Verschlusssachen (EU-VS) bearbeitet werden, ist von entscheidender Bedeutung. Einrichtungen der Union, die EU-VS bearbeiten, sind verpflichtet, die für den Schutz solcher Informationen geltenden umfassenden Rechtsrahmen, einschließlich spezifischer Verfahren für Governance, Strategien und Risikomanagement, anzuwenden. Netz- und Informationssysteme, in denen EU-VS bearbeitet werden, müssen strengeren Sicherheitsstandards entsprechen als nicht für Verschlusssachen genutzte Netz- und Informationssysteme. Daher sind Netz- und Informationssysteme, in denen EU-VS bearbeitet werden, widerstandsfähiger gegenüber Cyberbedrohungen und Sicherheitsvorfällen. Folglich sollte diese Verordnung nicht für Netz- und Informationssysteme gelten, in denen EU-VS bearbeitet werden, obgleich anerkannt wird, dass es diesbezüglich eines gemeinsamen Rahmens bedarf. Auf ausdrückliches Ersuchen einer Einrichtung der Union sollte das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) jedoch in der Lage sein, die jeweilige Einrichtung der Union bei Sicherheitsvorfällen in für Verschlusssachen genutzte IKT-Umgebungen zu unterstützen.

(17) Die Einrichtungen der Union sollten Cybersicherheitsrisiken im Zusammenhang mit den Beziehungen zu Anbietern und Dienstleistern, einschließlich Anbietern von Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten, bewerten und geeignete Maßnahmen ergreifen, um diese Risiken anzugehen. Cybersicherheitsmaßnahmen sollten in Leitlinien oder Empfehlungen des CERT-EU näher ausgeführt werden. Bei der Festlegung von Maßnahmen und der Ausarbeitung von Leitlinien sollten der Stand der Technik und gegebenenfalls einschlägige europäische und internationale Normen sowie das einschlägige Unionsrecht und die einschlägigen Strategien der Union, einschließlich der Bewertungen der Cybersicherheitsrisiken und der Empfehlungen der gemäß Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe, wie etwa die koordinierte Risikobewertung der EU zur Cybersicherheit in 5G-Netzen und das EU-Instrumentarium für die 5G-Cybersicherheit, gebührend berücksichtigt werden. Darüber hinaus könnte angesichts der Cyberbedrohungslage und der Bedeutung der Stärkung der Cyberresilienz für die Einrichtungen der Union die Zertifizierung relevanter IKT- Produkte, IKT- Dienste und IKT- Prozesse im Rahmen von gemäß Artikel 49 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[1] angenommener spezifischer europäischer Systeme für die Cybersicherheitszertifizierung vorgeschrieben werden.

[1] 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).

(18) Im Mai 2011 beschlossen die Generalsekretäre der Organe und Einrichtungen der Union die Einrichtung eines Vorbereitungsteams des 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 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[1]. Diese Verordnung sollte ein umfassendes Regelwerk für die Organisation, die Funktionsweise und den Betrieb des CERT-EU vorsehen. Die Bestimmungen dieser Verordnung haben Vorrang vor den Bestimmungen der im Dezember 2017 geschlossenen Interinstitutionellen Vereinbarung über die Organisation und den Betrieb des CERT-EU.

(19) Das CERT-EU sollte in „Cybersicherheitsdienst für die Organe, Einrichtungen und sonstigen Stellen der Union“ umbenannt werden; die Kurzbezeichnung „CERT-EU“ sollte jedoch aufgrund ihres Wiedererkennungswerts beibehalten werden.

---

[1] Vereinbarung zwischen dem Europäischen Parlament, dem Europäischen Rat, dem Rat der Europäischen Union, der Europäischen Kommission, dem Gerichtshof der Europäischen Union, der Europäischen Zentralbank, dem Europäischen Rechnungshof, dem Europäischen Auswärtigen Dienst, dem Europäischen Wirtschafts- und Sozialausschuss, dem Europäischen Ausschuss der Regionen und der Europäischen Investitionsbank über die Organisation und die Funktionsweise eines IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) (ABl. C 12 vom 13.1.2018, S. 1).

(20) Neben den zusätzlichen Aufgaben und der erweiterten Rolle, die für das CERT-EU vorgesehen werden, wird mit dieser Verordnung der Interinstitutionelle Cybersicherheitsbeirat (Interinstitutional Cybersecurity Board – IICB) eingerichtet, um ein hohes gemeinsames Cybersicherheitsniveau der Einrichtungen der Union zu fördern. Der IICB sollte eine ausschließliche Rolle bei der Überwachung und Unterstützung der Umsetzung dieser Verordnung durch die Einrichtungen der Union und bei der Beaufsichtigung der Umsetzung der allgemeinen Prioritäten und Ziele des CERT-EU sowie bei der Festlegung strategischer Leitlinien für das CERT-EU übernehmen. In dem IICB sollte daher die Vertretung der Organe der Union gewährleistet sein, und über das Netzwerk der Agenturen der Union (EUAN) sollten ihm auch Vertreter von Organen, Einrichtungen und sonstigen Stellen der Union angehören. Die Organisation und die Funktionsweise des IICB sollten durch seine interne Geschäftsordnung weiter geregelt werden, die eine weitere Spezifizierung regelmäßiger Sitzungen des IICB umfassen kann, einschließlich jährlicher Treffen der politischen Ebene, bei denen Vertreter der höchsten Managementebene jedes Mitglieds des IICB es dem IICB ermöglichen würden, strategische Diskussionen zu führen und strategische Leitlinien für das IICB vorzugeben. Darüber hinaus sollte das IICB einen Exekutivausschuss einsetzen, der es bei seiner Arbeit unterstützt, und ihm einige seiner Aufgaben und Befugnisse übertragen können, insbesondere in Bezug auf Aufgaben, die spezifisches Fachwissen seiner Mitglieder erfordern, z. B. die Billigung des Dienstleistungskatalogs und etwaiger späterer Aktualisierungen desselben, Vorkehrungen für Leistungsvereinbarungen, Bewertungen von Dokumenten und Berichten, die dem IICB von den Einrichtungen der Union gemäß dieser Verordnung vorgelegt werden, oder Aufgaben im Zusammenhang mit der Ausarbeitung von Beschlüssen über Compliance-Maßnahmen des IICB und der Überwachung ihrer Umsetzung. Der IICB sollte die Geschäftsordnung sowie die Aufgaben und Befugnisse des Exekutivausschusses festlegen.

(21) Ziel des IICB ist es, die Einrichtungen der Union dabei zu unterstützen, ihre jeweilige Cybersicherheitslage durch die Durchführung dieser Verordnung zu verbessern. Zur Unterstützung der Einrichtungen der Union sollte der IICB der Leitung des CERT-EU Leitlinien an die Hand geben, eine mehrjährige Strategie zur Erhöhung des Cybersicherheitsniveaus in den Einrichtungen der Union annehmen, die Methodik und andere Aspekte freiwilliger Peer-Reviews festlegen und die Einsetzung einer informellen Gruppe lokaler Cybersicherheitsbeauftragter erleichtern, die von der Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützt wird, um bewährte Verfahren und Informationen im Zusammenhang mit der Durchführung dieser Verordnung auszutauschen.

(22) Um in allen Einrichtungen der Union ein hohes Cybersicherheitsniveau zu erreichen, sollten innerhalb des IICB drei vom EUAN benannte Vertreter die Interessen der Organe, Einrichtungen und sonstigen Stellen der Union, die ihre eigene IKT-Umgebung betreiben, vertreten. Die Sicherheit der Verarbeitung personenbezogener Daten und damit auch deren Cybersicherheit sind ein Grundstein des Datenschutzes. Angesichts der Synergieeffekte zwischen Datenschutz und Cybersicherheit sollte der Europäische Datenschutzbeauftragte in seiner Eigenschaft als Einrichtung der Union, die dieser Verordnung unterliegt und über spezifisches Fachwissen im Bereich des Datenschutzes, einschließlich der Sicherheit elektronischer Kommunikationsnetze, verfügt, im IICB vertreten sein. In Anbetracht der Bedeutung von Innovation und Wettbewerbsfähigkeit im Bereich der Cybersicherheit sollte das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung im IICB vertreten sein. Angesichts der Rolle der ENISA als Kompetenzzentrum für Cybersicherheit und der Unterstützung, die die ENISA leistet, und angesichts der Bedeutung der Cybersicherheit von Weltrauminfrastrukturen und -diensten der Union sollten die ENISA und die Agentur der Europäischen Union für das Weltraumprogramm im IICB vertreten sein. Angesichts der Rolle, die dem CERT-EU im Rahmen dieser Verordnung übertragen wird, sollte die Leitung des CERT-EU vom Vorsitzenden des IICB zu allen Sitzungen des IICB eingeladen werden, es sei denn, der IICB erörtert Fragen, die unmittelbar die Leitung des CERT-EU betreffen.

(23) Der IICB sollte die Einhaltung dieser Verordnung sowie die Umsetzung von Leitlinien und Empfehlungen und von Aufrufen zum Tätigwerden überwachen. Der IICB sollte in technischen Fragen von fachlichen Beratungsgruppen unterstützt werden, deren Zusammensetzung im Ermessen des IICB liegt. Bei Bedarf sollten diese fachlichen Beratungsgruppen eng mit dem CERT-EU, den Einrichtungen der Union sowie mit anderen Interessenträgern zusammenarbeiten.

(24) Stellt der IICB fest, dass eine Einrichtung der Union diese Verordnung oder gemäß dieser Verordnung erlassene Leitlinien, Empfehlungen oder Aufrufe zum Tätigwerden nicht wirksam durchgeführt bzw. umgesetzt hat, so sollte der IICB unbeschadet der internen Verfahren der betreffenden Einrichtung der Union Compliance-Maßnahmen treffen können. Der IICB sollte die Compliance-Maßnahmen schrittweise anwenden, d. h., er sollte zunächst die am wenigsten strenge Maßnahme – nämlich eine mit Gründen versehene Stellungnahme – treffen und – nur wenn erforderlich – immer strengere Maßnahmen bis hin zu der schwerwiegendsten Maßnahme – nämlich einer Empfehlung zur vorübergehenden Aussetzung der Datenübermittlung an die betreffende Einrichtung der Union – ergreifen. Eine solche Empfehlung sollte nur in Ausnahmefällen abgegeben werden, in denen die betreffende Einrichtung der Union langfristig, vorsätzlich wiederholt oder in schwerwiegender Weise gegen diese Verordnung verstößt.

(25) Eine mit Gründen versehene Stellungnahme ist die am wenigsten strenge Maßnahme zur Behebung festgestellter Mängel bei der Durchführung dieser Verordnung. Der IICB sollte im Anschluss an eine mit Gründen versehene Stellungnahme die Möglichkeit haben, Leitlinien abzugeben, um die Einrichtung der Union dabei zu unterstützen, dafür zu sorgen, dass ihr Rahmen, ihre Maßnahmen zum Management von Cybersicherheitsrisiken, ihr Cybersicherheitsplan und ihre Berichterstattung mit dieser Verordnung im Einklang stehen; danach sollte er die Möglichkeit haben, eine Verwarnung auszusprechen, in der die Einrichtung der Union aufgefordert wird, die festgestellten Mängel innerhalb einer bestimmten Frist zu beheben. Wurden die in der Verwarnung festgestellten Mängel nicht ausreichend behoben, so sollte der IICB die Möglichkeit haben, eine begründete Mitteilung abzugeben.

(26) Der IICB sollte die Durchführung eines Audits bei einer Einrichtung der Union empfehlen können. Die Einrichtung der Union sollte zu diesem Zweck ihre interne Auditfunktion nutzen können. Der IICB sollte ferner verlangen können, dass ein Audit von einem externen Prüfungsdienst – auch von einem gemeinsam vereinbarten privaten Dienstleister – durchgeführt wird.

(27) In Ausnahmefällen, in denen eine Einrichtung der Union langfristig, vorsätzlich, wiederholt oder in schwerwiegender Weise gegen diese Verordnung verstößt, sollte der IICB als letztes Mittel eine Empfehlung an alle Mitgliedstaaten und Einrichtungen der Union zur vorübergehenden Aussetzung der Datenübermittlung an diese Einrichtung der Union richten können, die so lange gilt, bis die Einrichtung der Union nicht mehr gegen diese Verordnung verstößt. Eine solche Empfehlung sollte über geeignete und sichere Kommunikationskanäle übermittelt werden.

(28) Um die ordnungsgemäße Durchführung dieser Verordnung sicherzustellen, sollte der IICB, wenn er der Auffassung ist, dass eine anhaltende Verletzung gegen diese Verordnung durch eine Einrichtung der Union unmittelbar durch Handlungen oder Unterlassungen eines Mitglieds seines Personals – einschließlich der obersten Führungsebene – verursacht wurde, die betreffende Einrichtung der Union auffordern, im Einklang mit den Vorschriften und Verfahren des Statuts der Beamten der Europäischen Union und den Beschäftigungsbedingungen für die sonstigen Bediensteten der Union, die in der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates[1] (im Folgenden „Statut“) festgelegt sind, sowie im Einklang mit sonstigen geltenden Vorschriften und Verfahren geeignete Maßnahmen zu ergreifen und disziplinarrechtliche Maßnahmen in Erwägung zu ziehen.

(29) Das CERT-EU sollte zur Sicherheit der IKT-Umgebung aller Einrichtungen der Union beitragen. Bei der Prüfung der Frage, ob auf Ersuchen einer Einrichtung der Union technische Beratung oder Beiträge zu relevanten politischen Fragen geleistet werden sollen, sollte das CERT-EU sicherstellen, dass dies die Erfüllung der übrigen ihm gemäß dieser Verordnung übertragenen Aufgaben nicht behindert. Das CERT-EU sollte auf Seiten der Einrichtungen der Union als Äquivalent des für die Zwecke der koordinierten Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 benannten Koordinators fungieren.

---

[1] Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates vom 29. Februar 1968 zur Festlegung des Statuts der Beamten der Europäischen Gemeinschaften und der Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften sowie zur Einführung von Sondermaßnahmen, die vorübergehend auf die Beamten der Kommission anwendbar sind (ABl. L 56 vom 4.3.1968, S. 1).

(30) Das CERT-EU sollte die Umsetzung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau durch Vorschläge für Leitlinien 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 Einrichtungen der Union dringend aufgefordert werden. Der IICB sollte das CERT-EU anweisen, einen Vorschlag für Leitlinien oder für eine Empfehlung oder einen Aufruf zum Tätigwerden vorzulegen, zurückzuziehen oder zu ändern.

(31) Das CERT-EU sollte zudem die Rolle übernehmen, die ihm nach der Richtlinie (EU) 2022/2555 bei der Zusammenarbeit und beim Informationsaustausch mit dem gemäß Artikel 15 jener Richtlinie errichteten Netzwerk der Computer-Notfallteams (CSIRTs-Netzwerk) zukommt. Darüber hinaus sollte das CERT-EU im Einklang mit der Empfehlung (EU) 2017/1584 der Kommission[1] mit den einschlägigen Interessenträgern zusammenarbeiten und sich bezüglich 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 entsprechenden Stellen in den Mitgliedstaaten weiterleiten. Das CERT-EU sollte vorbehaltlich der vorherigen Zustimmung durch den IICB auch mit anderen öffentlichen und privaten entsprechenden Stellen, einschließlich der Nordatlantikvertrags-Organisation, zusammenarbeiten.

---

[1] 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).

(32) Bei der Unterstützung der operativen Cybersicherheit sollte das CERT-EU das verfügbare Fachwissen der ENISA im Wege der strukturierten Zusammenarbeit gemäß der Verordnung (EU) 2019/881 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 bei der Analyse der Cyberbedrohungslage mit der ENISA zusammenarbeiten und der ENISA seinen Bericht zur Bedrohungslage regelmäßig übermitteln.

(33) Das CERT-EU sollte mit den einschlägigen Cybersicherheitsgemeinschaften in der Union und ihren Mitgliedstaaten zusammenarbeiten und Informationen austauschen können, 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.

(34) Da die Dienste und Aufgaben des CERT-EU im Interesse der Einrichtungen der Union liegen, sollte jede Einrichtung der Union, die IKT-Ausgaben tätigt, einen angemessenen Beitrag für diese Dienste und Aufgaben leisten. Diese Beiträge lassen die Haushaltsautonomie der Einrichtungen der Union unberührt.

(35) Viele Cyberangriffe sind Teil umfassenderer Operationen, die auf Gruppen von Einrichtungen der Union oder Interessengemeinschaften, zu denen auch die Einrichtungen der Union gehören, ausgerichtet sind. Um eine proaktive Erkennung von Sicherheitsvorfällen, Maßnahmen zu ihrer Bewältigung und Eindämmung und die Bewältigung ihrer Folgen zu ermöglichen, sollten die Einrichtungen der Union die Möglichkeit haben, das CERT-EU über Sicherheitsvorfälle, Cyberbedrohungen, Schwachstellen und Beinahe-Vorfälle zu informieren und geeignete technische Einzelheiten zu übermitteln, die die Erkennung bzw. Eindämmung sowie die Bewältigung ähnlicher Sicherheitsvorfälle, Cyberbedrohungen, Schwachstellen und Beinahe-Vorfälle in anderen Einrichtungen der Union ermöglichen. Nach demselben Ansatz wie in der Richtlinie (EU) 2022/2555 sollten Einrichtungen der Union verpflichtet sein, innerhalb von 24 Stunden nachdem sie von einem erheblichen Sicherheitsvorfall Kenntnis erhalten haben eine Frühwarnung an das CERT-EU zu übermitteln. Dieser Informationsaustausch sollte es dem CERT-EU ermöglichen, die Informationen an andere Einrichtungen der Union sowie an geeignete entsprechende Stellen weiterzugeben, um dazu beizutragen, die IKT-Umgebungen der Einrichtungen der Union und die IKT-Umgebungen der den Einrichtungen der Union entsprechenden Stellen vor ähnlichen Sicherheitsvorfällen zu schützen.

(36) Mit dieser Verordnung wird ein mehrstufiger Ansatz für die Meldung erheblicher Sicherheitsvorfälle festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung erheblicher Sicherheitsvorfälle entgegenwirkt und den Einrichtungen der Union die Möglichkeit bietet, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Einrichtungen der Union ihre Cyberresilienz im Laufe der Zeit verbessern können und zu einer Verbesserung ihrer Cybersicherheitslage insgesamt beigetragen wird. Diesbezüglich sollte diese Verordnung die Meldung von Sicherheitsvorfällen umfassen, die – auf Grundlage einer von der betreffenden Einrichtung der Union durchgeführten ersten Bewertung – schwerwiegende Störungen des Betriebs der betreffenden Einrichtung der Union oder finanzielle Verluste für die betreffende Einrichtung der Union verursachen könnten oder anderen natürlichen oder juristischen Personen erheblichen immateriellen Schaden verursachen könnten. Bei dieser ersten Bewertung sollten unter anderem die betroffenen Netz- und Informationssysteme – insbesondere ihre Bedeutung für den Betrieb der Einrichtung der Union –, die Schwere und die technischen Merkmale einer Cyberbedrohung und alle zugrunde liegenden Schwachstellen, die ausgenutzt werden, sowie die Erfahrungen der Einrichtung der Union mit ähnlichen Sicherheitsvorfällen berücksichtigt werden. Indikatoren wie das Ausmaß, in dem der Betrieb der Einrichtung der Union beeinträchtigt wird, die Dauer eines Sicherheitsvorfalls oder die Zahl der betroffenen natürlichen oder juristischen Personen könnten eine wichtige Rolle bei der Feststellung spielen, ob die Betriebsstörung schwerwiegend ist.

(37) Da die Infrastruktur und die Netz- und Informationssysteme der betreffenden Einrichtung der Union und des Mitgliedstaats, in dem diese Einrichtung ansässig ist, miteinander verbunden sind, ist es von entscheidender Bedeutung, dass dieser Mitgliedstaat unverzüglich von einem erheblichen Sicherheitsvorfall innerhalb dieser Einrichtung der Union in Kenntnis gesetzt wird. Zu diesem Zweck sollte die betroffene Einrichtung der Union alle einschlägigen entsprechenden Stellen der Mitgliedstaaten, die gemäß den Artikeln 8 und 10 der Richtlinie (EU) 2022/2555 benannt oder eingerichtet wurden, über das Auftreten eines erheblichen Sicherheitsvorfalls informieren, den sie dem CERT-EU meldet. Wenn das CERT-EU Kenntnis von einem erheblichen Sicherheitsvorfall in einem Mitgliedstaat erhält, sollte es unverzüglich alle einschlägigen entsprechenden Stellen dieses Mitgliedstaats unterrichten.

(38) Es sollte ein Mechanismus eingeführt werden, der im Falle schwerwiegender Sicherheitsvorfälle einen wirksamen Informationsaustausch, eine wirksame Koordinierung und eine wirksame Zusammenarbeit zwischen den Einrichtungen der Union gewährleistet, einschließlich einer klaren Festlegung der Aufgaben und Zuständigkeiten der beteiligten Einrichtungen der Union. Der Vertreter der Kommission im IICB sollte vorbehaltlich des Plans für das Cyberkrisenmanagement als Anlaufstelle fungieren, um den Austausch einschlägiger Informationen über schwerwiegende Sicherheitsvorfälle mit dem europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) als Beitrag zur gemeinsamen Lageerfassung zu erleichtern. Die Rolle des Vertreters der Kommission im IICB als Anlaufstelle sollte die spezifische und gesonderte Rolle der Kommission in EU-CyCLONe gemäß Artikel 16 Absatz 2 der Richtlinie (EU) 2022/2555 unberührt lassen.

(39) Für jede Verarbeitung personenbezogener Daten gemäß dieser Verordnung gilt die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[1]. Die Verarbeitung personenbezogener Daten könnte in Bezug auf Maßnahmen erfolgen, die im Zusammenhang mit dem Management von Cybersicherheitsrisiken, dem Umgang mit Schwachstellen und der Bewältigung von Sicherheitsvorfällen, dem Informationsaustausch über Sicherheitsvorfälle, Cyberbedrohungen und Schwachstellen sowie der Koordinierung der Reaktion auf Sicherheitsvorfälle und der entsprechenden Zusammenarbeit ergriffen werden. Solche Maßnahmen könnten die Verarbeitung bestimmter Kategorien personenbezogener Daten erfordern – etwa IP-Adressen, URL-Adressen, Domainnamen, E-Mail-Adressen, organisatorische Rollen der betroffenen Person, Zeitstempel, Themen von E-Mails oder Dateinamen. Alle gemäß dieser Verordnung ergriffenen Maßnahmen sollten mit dem Rahmen für Datenschutz und den Schutz der Privatsphäre im Einklang stehen, und die Einrichtungen der Union, das CERT-EU und gegebenenfalls der IICB sollten alle einschlägigen technischen und organisatorischen Schutzvorkehrungen ergreifen, um diesen Einklang in verantwortungsvoller Weise herzustellen.

(40) Mit dieser Verordnung wird im Einklang mit Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2018/1725 die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Einrichtungen der Union, das CERT-EU und gegebenenfalls den IICB zum Zwecke der Wahrnehmung ihrer Aufgaben und Pflichten gemäß dieser Verordnung geschaffen. Das CERT-EU kann gemäß der Verordnung (EU) 2018/1725 je nach der Aufgabe, die es wahrnimmt, als Auftragsverarbeiter oder Verantwortlicher fungieren.

---

[1] 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).

(41) In bestimmten Fällen kann es erforderlich sein, dass Einrichtungen der Union und das CERT-EU besondere Kategorien personenbezogener Daten gemäß Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 verarbeiten, um ihren Verpflichtungen aus dieser Verordnung zur Sicherstellung eines hohen Cybersicherheitsniveaus nachzukommen, insbesondere im Zusammenhang mit dem Umgang mit Schwachstellen und der Bewältigung von Sicherheitsvorfällen. Mit dieser Verordnung wird die Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten durch Einrichtungen der Union und das CERT-EU gemäß Artikel 10 Absatz 2 Buchstabe g der Verordnung (EU) 2018/1725 geschaffen. Die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen dieser Verordnung sollte unbedingt in einem angemessenen Verhältnis zu dem verfolgten Ziel stehen. Vorbehaltlich der in Artikel 10 Absatz 2 Buchstabe g der genannten Verordnung festgelegten Bedingungen sollten die Einrichtungen der Union und das CERT-EU solche Daten nur im erforderlichen Umfang und nur dann verarbeiten können, wenn dies in dieser Verordnung ausdrücklich vorgesehen ist. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten sollten die Einrichtungen der Union und das CERT-EU den Wesensgehalt des Rechts auf Datenschutz wahren und geeignete und spezifische Maßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Personen vorsehen.

(42) Gemäß Artikel 33 der Verordnung (EU) 2018/1725 sollten die Einrichtungen der Union und das CERT-EU unter Berücksichtigung des Stands der Technik, der Durchführungskosten und der Art, des Umfangs, des Kontexts und des Zwecks der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit des Eintretens von Risiken für die Rechte und Freiheiten natürlicher Personen und deren Schwere geeignete technische und organisatorische Maßnahmen umsetzen, um ein angemessenes Maß an Sicherheit personenbezogener Daten sicherzustellen, wie etwa die Gewährung beschränkter Zugriffsrechte nach dem Grundsatz „Kenntnis nur, wenn nötig“, die Anwendung der Grundsätze des Prüfpfads, die Einrichtung einer Überwachungskette, die Speicherung inaktiver Daten in einer kontrollierten und überprüfbaren Umgebung, standardisierte betriebliche Verfahren und Maßnahmen zum Schutz der Privatsphäre wie Pseudonymisierung oder Verschlüsselung. Diese Maßnahmen sollten nicht in einer Weise umgesetzt werden, die die Zwecke der Bewältigung von Sicherheitsvorfällen und die Integrität der Beweismittel beeinträchtigt. Wenn eine Einrichtung der Union oder das CERT-EU personenbezogene Daten im Zusammenhang mit einem Sicherheitsvorfall, einschließlich besonderer Kategorien personenbezogener Daten, für die Zwecke dieser Verordnung an eine entsprechende Stelle oder einen Partner übermittelt, sollte die Übermittlung mit der Verordnung (EU) 2018/1725 im Einklang stehen. Werden besondere Kategorien personenbezogener Daten an Dritte übermittelt, sollten die Einrichtungen der Union und das CERT-EU sicherstellen, dass der jeweilige Dritte Maßnahmen zum Schutz personenbezogener Daten anwendet, die dem Niveau der Verordnung (EU) 2018/1725 entsprechen.

(43) Für die Zwecke dieser Verordnung verarbeitete personenbezogene Daten sollten nur so lange gespeichert werden, wie dies gemäß der Verordnung (EU) 2018/1725 erforderlich ist. Einrichtungen der Union und gegebenenfalls das CERT-EU, das als Verantwortlicher fungiert, sollten Speicherfristen festlegen, die auf das zur Erreichung der festgelegten Zwecke erforderliche Maß beschränkt sind. Insbesondere in Bezug auf personenbezogene Daten, die für die Bewältigung von Sicherheitsvorfällen erhoben werden, sollten die Einrichtungen der Union und das CERT-EU zwischen personenbezogenen Daten, die zur Erkennung einer Cyberbedrohung in ihren IKT-Umgebungen erhoben werden, um einen Sicherheitsvorfall zu verhindern, und personenbezogenen Daten, die zur Eindämmung eines Sicherheitsvorfalls, zur Reaktion darauf und zur Bewältigung seiner Folgen erhoben werden, unterscheiden. Bei der Erkennung einer Cyberbedrohung ist zu berücksichtigen, wie lange der Verursacher einer Bedrohung in einem System unentdeckt bleiben kann. Zur Eindämmung eines Sicherheitsvorfalls, zur Reaktion darauf und zur Bewältigung seiner Folgen ist zu prüfen, ob die personenbezogenen Daten erforderlich sind, um einen wiederkehrenden Sicherheitsvorfall oder einen Sicherheitsvorfall ähnlicher Art, bei dem ein Zusammenhang nachgewiesen werden konnte, aufzuspüren und zu bewältigen.

(44) Der Umgang der Einrichtungen der Union und des CERT-EU mit Informationen sollte im Einklang mit den geltenden Vorschriften über die Informationssicherheit erfolgen. Die Aufnahme der Sicherheit des Personals in die Maßnahmen zum Management von Cybersicherheitsrisiken sollte auch mit den geltenden Vorschriften im Einklang stehen.

(45) Für die Zwecke des Informationsaustauschs werden sichtbare Kennzeichnungen verwendet, um anzuzeigen, dass die Weitergabebeschränkungen von den Empfängern der Informationen auf der Grundlage von insbesondere Geheimhaltungsvereinbarungen oder informellen Geheimhaltungsvereinbarungen wie dem Ampelprotokoll („Traffic Light Protocol“) oder anderen eindeutigen Hinweisen seitens der Quelle anzuwenden sind. Das Ampelprotokoll ist als ein Mittel zu verstehen, um Informationen über etwaige Einschränkungen in Bezug auf die weitere Verbreitung von Informationen bereitzustellen. Es wird in fast allen CSIRTs und in einigen Informationsanalyse- und Informationsaustauschzentren eingesetzt.

(46) Diese Verordnung sollte im Hinblick auf künftige Verhandlungen über mehrjährige Finanzrahmen, aufgrund derer weitere Beschlüsse im Zusammenhang mit der Arbeitsweise und der institutionellen Rolle des CERT-EU – einschließlich der möglichen Einrichtung des CERT-EU als Amt der Union – gefasst werden können, regelmäßig evaluiert werden.

(47) Der IICB sollte die Durchführung dieser Verordnung mit Unterstützung des CERT-EU überprüfen und bewerten und der Kommission über seine Feststellungen Bericht erstatten. Aufbauend auf diesem Bericht sollte die Kommission dem Europäischen Parlament, dem Rat, dem Europäischen Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen regelmäßig Bericht erstatten. In diesem Bericht, an dem auch der IICB mitwirkt, sollte bewertet werden, ob Netz- und Informationssysteme, in denen EU-VS bearbeitet werden, in den Anwendungsbereich dieser Verordnung aufgenommen werden sollten, insbesondere wenn es keine für alle Einrichtungen der Union geltenden gemeinsamen Vorschriften für die Informationssicherheit gibt.

(48) Nach dem Grundsatz der Verhältnismäßigkeit ist es erforderlich und angemessen, zur Erreichung des grundlegenden Ziels, ein hohes gemeinsames Cybersicherheitsniveau in den Einrichtungen der Union zu erreichen, für die Einrichtungen der Union Vorschriften über die Cybersicherheit festzulegen. Die vorliegende Verordnung geht entsprechend Artikel 5 Absatz 4 des Vertrags über die Europäische Union nicht über das zur Erreichung dieses Ziels erforderliche Maß hinaus.

(49) Die vorliegende Verordnung trägt dem Umstand Rechnung, dass sich die Einrichtungen der Union in Bezug auf ihre Größe und ihre Kapazitäten, einschließlich ihrer finanziellen und personellen Ressourcen, unterscheiden.

(50) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und hat am 17. Mai 2022 eine Stellungnahme abgegeben[1] —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

[1] ABl. C 258 vom 5.7.2022, S. 10.

Kapitel I

Allgemeine Bestimmungen

Artikel 1

Gegenstand

Mit dieser Verordnung werden Maßnahmen zur Erreichung eines gemeinsamen hohen Cybersicherheitsniveaus in den Einrichtungen der Union festgelegt, die Folgendes betreffen:

a) die Schaffung eines internen Rahmens für Risikomanagement, Governance und Kontrolle im Bereich der Cybersicherheit durch jede Einrichtung der Union gemäß Artikel 6,

b) das Risikomanagement, die Berichterstattung und den Informationsaustausch im Bereich der Cybersicherheit,

c) die Organisation, den Betrieb und die Arbeitsweise des gemäß Artikel 10 eingerichteten Interinstitutionellen Cybersicherheitsbeirats sowie die Organisation, die Funktionsweise und die Arbeitsweise des Cybersicherheitsdienstes für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU),

d) die Überwachung der Durchführung dieser Verordnung.

Artikel 2

Anwendungsbereich

(1) Diese Verordnung gilt für die Einrichtungen der Union, für den gemäß Artikel 10 eingerichteten Interinstitutionellen Cybersicherheitsbeirat und für das CERT-EU.

(2) Diese Verordnung gilt unbeschadet der institutionellen Autonomie gemäß den Verträgen.

(3) Mit Ausnahme von Artikel 13 Absatz 8 gilt diese Verordnung nicht für Netz- und Informationssysteme, in denen EU-Verschlusssachen (EU-VS) bearbeitet werden.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Einrichtungen 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 (AEUV) oder den Vertrag zur Gründung der Europäischen Atomgemeinschaft oder gemäß diesen Verträgen geschaffen wurden;

2. „Netz- und Informationssystem“ ein Netz- und Informationssystem im Sinne des Artikels 6 Nummer 1 der Richtlinie (EU) 2022/2555;

3. „Sicherheit von Netz- und Informationssystemen“ die Sicherheit von Netz- und Informationssystemen im Sinne des Artikels 6 Nummer 2 der Richtlinie (EU) 2022/2555;

4. „Cybersicherheit“ Cybersicherheit im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2019/881;

5. „höchste Managementebene“ eine Führungskraft, ein Leitungsorgan oder ein Koordinierungs- und Aufsichtsgremium auf der höchsten Verwaltungsebene, die bzw. das – unbeschadet der formalen Zuständigkeit anderer Managementebenen in Bezug auf die Einhaltung der Vorschriften und das Management von Cybersicherheitsrisiken in deren jeweiligen Zuständigkeitsbereichen – für das Funktionieren einer Einrichtung der Union verantwortlich ist und über das Mandat verfügt, Beschlüsse im Einklang mit den Governance-Regelungen für die höchsten Ebenen dieser Einrichtung der Union anzunehmen oder zu billigen;

6. „Beinahe-Vorfall“ einen Beinahe-Vorfall im Sinne des Artikels 6 Nummer 5 der Richtlinie(EU) 2022/2555;

7. „Sicherheitsvorfall“ einen Sicherheitsvorfall im Sinne des Artikels 6 Nummer 6 der Richtlinie (EU) 2022/2555;

8. „schwerwiegender Sicherheitsvorfall“ einen Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit einer Einrichtung der Union und des CERT-EU übersteigt, oder der erhebliche Auswirkungen auf mindestens zwei Einrichtungen der Union hat;

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

10. „Bewältigung von Sicherheitsvorfällen“ die Bewältigung von Sicherheitsvorfällen im Sinne des Artikels 6 Nummer 8 der Richtlinie (EU) 2022/2555;

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

12. „erhebliche Cyberbedrohung“ eine erhebliche Cyberbedrohung im Sinne des Artikels 6 Nummer 11 der Richtlinie (EU) 2022/2555;

13. „Schwachstelle“ eine Schwachstelle im Sinne des Artikels 6 Nummer 15 der Richtlinie (EU) 2022/2555;

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

15. „Cloud-Computing-Dienst“ einen Cloud-Computing-Dienst im Sinne des Artikels 6 Nummer 30 der Richtlinie (EU) 2022/2555.

Artikel 4

Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten im Rahmen dieser Verordnung durch das CERT-EU, den gemäß Artikel 10 eingerichteten Interinstitutionellen Cybersicherheitsbeirat oder Einrichtungen der Union erfolgt gemäß der Verordnung (EU) 2018/1725.

(2) Das CERT-EU, der gemäß Artikel 10 eingerichtete Interinstitutionelle Cybersicherheitsbeirat und die Einrichtungen der Union verarbeiten und tauschen personenbezogene Daten nur insoweit aus, als dies für die Wahrnehmung der Aufgaben oder die Erfüllung der Pflichten gemäß dieser Verordnung erforderlich ist, und ausschließlich zu diesem Zweck.

(3) Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 gilt als aus Gründen eines erheblichen öffentlichen Interesses gemäß Artikel 10 Absatz 2 Buchstabe g der genannten Verordnung erforderlich. Diese Daten dürfen nur in dem Umfang verarbeitet werden, der für die Umsetzung der in den Artikeln 6 und 8 genannten Maßnahmen zum Cybersicherheitsrisikomanagement, die Bereitstellung von Diensten durch das CERT-EU gemäß Artikel 13, den Austausch spezifischer Informationen über Sicherheitsvorfälle gemäß Artikel 17 Absatz 3 und Artikel 18 Absatz 3, den Informationsaustausch gemäß Artikel 20, die Meldepflichten gemäß Artikel 21, die Koordinierung und Zusammenarbeit bei der Reaktion auf Sicherheitsvorfälle gemäß Artikel 22 und die Bewältigung schwerwiegender Sicherheitsvorfälle gemäß Artikel 23 dieser Verordnung erforderlich ist. Wenn die Einrichtungen der Union und das CERT-EU als Verantwortliche fungieren, ergreifen sie technische Maßnahmen, um die Verarbeitung besonderer Kategorien personenbezogener Daten für andere Zwecke zu verhindern, und sie sehen geeignete und spezifische Maßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Personen vor.

Kapitel II

Maßnahmen für ein hohes Gemeinsames Cybersicherheitsniveau

Artikel 5

Durchführung der Maßnahmen

(1) Der gemäß Artikel 10 eingerichtete Interinstitutionelle Cybersicherheitsbeirat gibt nach Konsultation der Agentur der Europäischen Union für Cybersicherheit (ENISA) und nach Erhalt von Leitlinien des CERT-EU bis zum … [acht Monate nach dem Tag des Inkrafttretens dieser Verordnung] Leitlinien für Einrichtungen der Union heraus, damit diese eine erste Überprüfung der Cybersicherheit durchführen und einen internen Rahmen für Risikomanagement, Governance und Kontrolle im Bereich der Cybersicherheit gemäß Artikel 6 festlegen, den Cybersicherheitsreifegrad gemäß Artikel 7 bewerten, Maßnahmen für das Management von Cybersicherheitsrisiken gemäß Artikel 8 ergreifen und den Cybersicherheitsplan gemäß Artikel 9 verabschieden können.

(2) Bei der Anwendung der Artikel 6, bis 9 berücksichtigen die Einrichtungen der Union die in Absatz 1 des vorliegenden Artikels genannten Leitlinien sowie die gemäß den Artikeln 11 und 14 angenommenen einschlägigen Leitlinien und Empfehlungen.

Artikel 6

Rahmen für Risikomanagement, Governance und Kontrolle im Bereich der Cybersicherheit

(1) Alle Einrichtungen der Union legen bis zum … [15 Monate nach dem Tag des Inkrafttretens dieser Verordnung] nach Durchführung einer ersten Cybersicherheitsüberprüfung, wie etwa eines Audits, einen internen Rahmen für Risikomanagement, Governance und Kontrolle im Bereich von Cybersicherheitsrisiken (im Folgenden „Rahmen“) fest. Die Festlegung des Rahmens erfolgt unter der Aufsicht und Verantwortung der jeweiligen höchsten Managementebene der Einrichtung der Union.

(2) Der Rahmen deckt jeweils die gesamte nicht für Verschlusssachen genutzte IKT-Umgebung der betreffenden Einrichtung der Union ab, insbesondere die IKT-Umgebung in den Räumlichkeiten der betreffenden Einrichtung, das operative Technologienetz in den Räumlichkeiten der betreffenden Einrichtung, in Cloud-Computing-Umgebungen ausgelagerte oder von Dritten gehostete Anlagen und Dienste, mobile Geräte, Firmennetze, nicht mit dem Internet verbundene Geschäftsnetze und alle mit diesen Umgebungen verbundenen Geräte (im Folgenden „IKT-Umgebung“). Der Rahmen basiert auf einem gefahrenübergreifenden Ansatz.

(3) Der Rahmen muss für ein hohes Maß an Cybersicherheit sorgen. Mit dem Rahmen werden interne Cybersicherheitsstrategien, einschließlich Zielen und Prioritäten, für die Sicherheit von Netz- und Informationssystemen sowie die Aufgaben und Zuständigkeiten des Personals der Einrichtung der Union festgelegt, das mit der Sicherstellung der wirksamen Durchführung dieser Verordnung betraut ist. Der Rahmen umfasst auch Verfahren, mit denen die Wirksamkeit der Umsetzung gemessen wird.

(4) Der Rahmen muss regelmäßig im Lichte der sich wandelnden Cybersicherheitsrisiken und mindestens alle vier Jahre überprüft werden. Gegebenenfalls wird auf Ersuchen des gemäß Artikel 10 eingerichteten Interinstitutionellen Cybersicherheitsbeirats der Rahmen einer Einrichtung der Union auf der Grundlage einer Orientierungshilfe des CERT-EU zu ermittelten Sicherheitsvorfällen oder etwaigen bei der Durchführung dieser Verordnung festgestellten Unzulänglichkeiten aktualisiert.

(5) Die höchste Managementebene jeder Einrichtung der Union ist für die Durchführung dieser Verordnung verantwortlich und überwacht die Einhaltung der Verpflichtungen im Zusammenhang mit dem Rahmen durch ihre Organisation.

(6) Die höchste Managementebene jeder Einrichtung der Union kann gegebenenfalls und unbeschadet ihrer Verantwortung für die Durchführung dieser Verordnung spezifische Verpflichtungen aus dieser Verordnung an höhere Führungskräfte im Sinne des Artikels 29 Absatz 2 des Statuts der Beamten oder andere gleichrangige Beamte innerhalb der betreffenden Einrichtung der Union delegieren. Unabhängig von einer solchen Übertragung kann die höchste Managementebene für Verstöße der betreffenden Einrichtung der Union gegen diese Verordnung haftbar gemacht werden.

(7) Alle Einrichtungen der Union müssen über wirksame Mechanismen verfügen, um sicherzustellen, dass ein angemessener Prozentsatz des IKT-Haushalts für Cybersicherheit ausgegeben wird. Bei der Festlegung dieses Prozentsatzes ist dem Rahmen gebührend Rechnung zu tragen.

(8) Alle Einrichtungen der Union ernennen einen lokalen Cybersicherheitsbeauftragten oder eine Kontaktperson mit gleichwertiger Funktion, der bzw. die als zentrale Anlaufstelle für alle Cybersicherheitsfragen fungiert. Der lokale Cybersicherheitsbeauftragte erleichtert die Durchführung dieser Verordnung und erstattet der höchsten Managementebene regelmäßig unmittelbar Bericht über den Stand der Durchführung. Obgleich der lokale Cybersicherheitsbeauftragte in jeder Einrichtung der Union als zentrale Anlaufstelle fungiert, kann eine Einrichtung der Union bestimmte Aufgaben des lokalen Cybersicherheitsbeauftragten in Bezug auf die Durchführung dieser Verordnung auf der Grundlage einer Leistungsvereinbarung zwischen dieser Einrichtung der Union und dem CERT-EU auf das CERT-EU übertragen; diese Aufgaben können auch von mehreren Einrichtungen der Union gemeinsam wahrgenommen werden. Werden diese Aufgaben dem CERT-EU übertragen, so entscheidet der gemäß Artikel 10 eingerichtete Interinstitutionelle Cybersicherheitsbeirat unter Berücksichtigung der personellen und finanziellen Ressourcen der betreffenden Einrichtung der Union, ob die Bereitstellung dieses Dienstes Teil der Basisdienste des CERT-EU sein soll. Jede Einrichtung der Union teilt CERT-EU unverzüglich den ernannten lokalen Cybersicherheitsbeauftragten sowie etwaige spätere Änderungen daran mit.

Das CERT-EU führt eine Liste der ernannten lokalen Cybersicherheitsbeauftragten und aktualisiert diese.

(9) Die höheren Führungskräfte im Sinne des Artikels 29 Absatz 2 des Statuts der Beamten oder andere gleichrangige Beamte jeder Einrichtung der Union sowie alle relevanten Bediensteten, die mit der Umsetzung bzw. Erfüllung der in dieser Verordnung festgelegten Maßnahmen bzw. Pflichten im Zusammenhang mit dem Management von Cybersicherheitsrisiken betraut sind, absolvieren regelmäßig spezifische Schulungen, um ausreichende Kenntnisse und Fähigkeiten zu erwerben, damit sie mit den Vorgehensweisen im Bereich des Cybersicherheitsrisikos und des Cybersicherheitsmanagements und deren Auswirkungen auf den Betrieb der jeweiligen Einrichtung der Union vertraut sind und diese bewerten können.

Artikel 7

Bewertung des Cybersicherheitsreifegrads

(1) Jede Einrichtung der Union führt bis zum … [18 Monate nach dem Tag des Inkrafttretens dieser Verordnung] und danach mindestens alle zwei Jahre eine Bewertung des Cybersicherheitsreifegrads durch, bei der alle Elemente ihrer IKT-Umgebung einbezogen werden.

(2) Die Bewertungen des Cybersicherheitsreifegrads werden erforderlichenfalls mit Unterstützung eines spezialisierten Dritten durchgeführt.

(3) Die Einrichtungen der Union, die ähnliche Strukturen aufweisen, können bei der Durchführung von Bewertungen des Cybersicherheitsreifegrads für ihre jeweilige Einrichtung zusammenarbeiten.

(4) Auf Antrag des gemäß Artikel 10 eingerichtete Interinstitutionelle Cybersicherheitsbeirats und mit ausdrücklicher Zustimmung der betreffenden Einrichtung der Union können die Ergebnisse einer Bewertung des Cybersicherheitsreifegrads innerhalb des Beirats oder des informellen Netzes lokaler Cybersicherheitsbeauftragter erörtert werden, um Lehren aus den Erfahrungen zu ziehen und sich über bewährte Verfahren auszutauschen.

Artikel 8

Maßnahmen zum Management von Cybersicherheitsrisiken

(1) Jede Einrichtung der Union ergreift unverzüglich, in jedem Fall aber bis zum … [20 Monate nach dem Tag des Inkrafttretens dieser Verordnung] unter der Aufsicht ihrer höchsten Managementebene geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen, um die im Rahmen des Rechtsrahmens ermittelten Cybersicherheitsrisiken zu bewältigen und um Sicherheitsvorfälle zu verhindern bzw. deren Auswirkungen zu minimieren. Unter Berücksichtigung des Stands der Technik und gegebenenfalls einschlägiger europäischer und internationaler Normen wird mit diesen Maßnahmen für ein Sicherheitsniveau von Netz- und Informationssystemen in der gesamten IKT-Umgebung gesorgt, das den bestehenden Cybersicherheitsrisiken gerecht wird. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Exposition der Einrichtung der Union gegenüber Cybersicherheitsrisiken, ihre Größe und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen, wirtschaftlichen und institutionellen Auswirkungen, gebührend zu berücksichtigen.

(2) Bei der Durchführung von Maßnahmen zum Management von Cybersicherheitsrisiken müssen die Einrichtungen der Union mindestens die folgenden Bereiche berücksichtigen:

a) Cybersicherheitsstrategie, einschließlich der Maßnahmen, die zur Verwirklichung der in Artikel 6 und in Absatz 3 des vorliegenden Artikels genannten Ziele und Prioritäten erforderlich sind,

b) Strategien für die Analyse von Cybersicherheitsrisiken und die Sicherheit von Informationssystemen,

c) Strategische Grundsätze in Bezug auf die Nutzung von Cloud-Computing-Diensten,

d) gegebenenfalls eine Cybersicherheitsprüfung, die eine Bewertung des Cybersicherheitsrisikos, der Anfälligkeit und der Cyberbedrohung sowie regelmäßig von einem vertrauenswürdigen privaten Anbieter durchgeführte Penetrationstests umfassen kann,

e) Umsetzung der Empfehlungen, die sich aus den unter Buchstabe d genannten Cybersicherheitsprüfungen ergeben, durch Aktualisierungen im Bereich der Cybersicherheit und der Strategie,

f) Organisation der Cybersicherheit, einschließlich Festlegung der Aufgaben und Zuständigkeiten,

g) Verwaltung der Vermögenswerte, einschließlich IKT-Bestandsverzeichnis und IKT-Netzkartografie,

h) Sicherheit des Personals und Zugangskontrolle,

i) Betriebssicherheit,

j) Kommunikationssicherheit,

k) Beschaffung, Entwicklung und Wartung von Systemen, einschließlich Vorgaben zur Bewältigung und Offenlegung von Sicherheitslücken,

l) wenn möglich, Strategie zur Transparenz des Quellcodes,

m) Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte im Zusammenhang mit den Beziehungen zwischen den einzelnen Einrichtungen der Union und ihren direkten Anbietern oder Dienstleistern,

n) Bewältigung von Sicherheitsvorfällen und Zusammenarbeit mit dem CERT-EU, z. B. bei der Aufrechterhaltung der Sicherheitsüberwachung und -protokollierung,

o) Kontinuitätsmanagement, etwa Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,

p) Förderung und Entwicklung von Ausbildungs-, Kompetenz-, Aufklärungs-, Übungs- und Schulungsprogrammen im Bereich der Cybersicherheit.

Die Einrichtungen der Union müssen für die Zwecke von Unterabsatz 1 Buchstabe m die spezifischen Schwachstellen der einzelnen direkten Anbieter und Dienstleister und die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Dienstleister, einschließlich ihrer sicheren Entwicklungsprozesse, berücksichtigen.

(3) Die Einrichtungen der Union müssen mindestens die folgenden spezifischen Maßnahmen zum Management von Cybersicherheitsrisiken ergreifen:

a) technische Vorkehrungen zur Ermöglichung und Aufrechterhaltung der Telearbeit,

b) konkrete Schritte für den Übergang zu Zero-Trust-Grundsätzen,

c) Verwendung der Multifaktor-Authentifizierung als Norm in allen Netz- und Informationssystemen,

d) Verwendung von Kryptografie und Verschlüsselung, insbesondere von Ende-zu-Ende-Verschlüsselung sowie von sicheren digitalen Signaturen,

e) erforderlichenfalls Einsatz von gesicherter Sprach-, Video- und Textkommunikation und gesicherter Notrufkommunikationssysteme innerhalb der Einrichtung,

f) proaktive Maßnahmen zur Erkennung und Entfernung von Schadsoftware und Spähsoftware,

g) Schaffung von Sicherheit in der Software-Lieferkette durch Kriterien für sichere Entwicklung und Bewertung von Software,

h) Erstellung und Annahme von Schulungsprogrammen zur Cybersicherheit, die den vorgeschriebenen Aufgaben und den erwarteten Fähigkeiten der höchsten Managementebene und der Bediensteten der Einrichtung der Union, die mit der wirksamen Durchführung dieser Verordnung betraut sind, gerecht werden,

i) regelmäßige Cybersicherheitsschulungen für Mitarbeiter,

j) Beteiligung an Risikoanalysen zur Interkonnektivität zwischen den Einrichtungen der Union, wo relevant,

k) Erweiterung der Vorschriften für die Auftragsvergabe, um ein hohes gemeinsames Cybersicherheitsniveau zu begünstigen, und zwar durch

   i) die Beseitigung vertraglicher Hindernisse, die den Informationsaustausch der IKT-Dienstleister über Sicherheitsvorfälle, Schwachstellen und Cyberbedrohungen mit dem CERT-EU einschränken,

   ii) vertragliche Pflichten zur Meldung von Sicherheitsvorfällen, Schwachstellen und Cyberbedrohungen sowie zur Einrichtung geeigneter Mechanismen zur Bewältigung und Überwachung von Sicherheitsvorfällen.

Artikel 9

Cybersicherheitspläne

(1) Auf der Grundlage der Schlussfolgerungen der gemäß Artikel 7 durchgeführten Bewertung des Cybersicherheitsreifegrads und unter Berücksichtigung der gemäß dem Rahmen ermittelten Anlagen und Cybersicherheitsrisiken sowie der Maßnahmen zum Management von Cybersicherheitsrisiken gemäß Artikel 8 genehmigt die höchste Managementebene jeder Einrichtung der Union unverzüglich und in jedem Fall bis zum … [24 Monate nach dem Tag des Inkrafttretens dieser Verordnung] einen Cybersicherheitsplan. Der Cybersicherheitsplan zielt darauf ab, die Cybersicherheit der Einrichtung der Union insgesamt zu erhöhen und trägt somit zur Verbesserung eines hohen gemeinsamen Cybersicherheitsniveaus in den Einrichtungen der Union bei. Der Cybersicherheitsplan enthält mindestens die gemäß Artikel 8 ergriffenen Maßnahmen zum Management von Cybersicherheitsrisiken. Der Cybersicherheitsplan wird alle zwei Jahre oder erforderlichenfalls häufiger**,** im Anschluss an jede gemäß Artikel 7 durchgeführte Bewertung des Cybersicherheitsreifegrads oder an eine grundlegende Überarbeitung des Rahmens, überarbeitet.

(2) Der Cybersicherheitsplan muss den Plan der Einrichtungen der Union für das Cyberkrisenmanagement bei schwerwiegenden Sicherheitsvorfällen umfassen.

(3) Die Einrichtung der Union übermittelt ihren vervollständigten Cybersicherheitsplan dem gemäß Artikel 10 eingerichteten Interinstitutionellen Cybersicherheitsbeirat.

Kapitel III

Interinstitutioneller Cybersicherheitsbeirat

Artikel 10

Interinstitutioneller Cybersicherheitsbeirat

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

(2) Der IICB ist zuständig für

a) die Überwachung und Unterstützung der Durchführung dieser Verordnung durch die Einrichtungen 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 an:

a) ein von den folgenden Organen, Einrichtungen und Stellen benannter Vertreter:

i) Europäisches Parlament,

ii) Europäischer Rat,

iii) Rat der Europäischen Union,

iv) Kommission,

v) Gerichtshof der Europäischen Union,

vi) Europäische Zentralbank,

vii) Rechnungshof,

viii) Europäischer Auswärtiger Dienst,

ix) Europäischer Wirtschafts- und Sozialausschuss,

x) Europäischer Ausschuss der Regionen,

xi) Europäische Investitionsbank,

xii) Europäisches Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung,

xiii) ENISA,

xiv) Europäischer Datenschutzbeauftragter (EDSB),

xv) Agentur der Europäischen Union für das Weltraumprogramm,

b) drei Vertreter, die vom Netzwerk der Agenturen der Union (EUAN) auf Vorschlag seines IKT-Beratungsausschusses benannt werden, um die Interessen der Organe, Einrichtungen und sonstigen Stellen der Union zu vertreten, die ihre eigene IKT-Umgebung betreiben und nicht unter Buchstabe a genannt sind.

Die im IICB vertretenen Einrichtungen der Union streben ein ausgewogenes Geschlechterverhältnis unter den benannten Vertretern an.

(4) Jedes Mitglied des IICB kann einen Stellvertreter haben. Der Vorsitzende kann weitere Vertreter bzw. Vertreterinnen der in Absatz 3 genannten Einrichtungen der Union oder anderer Einrichtungen der Union zur Teilnahme an IICB-Sitzungen einladen, wobei sie kein Stimmrecht haben.

(5) Der Leiter des CERT-EU und die Vorsitzenden der Kooperationsgruppe, des CSIRTs-Netzes und des EU-CyCLONe, die jeweils gemäß den Artikeln 14, 15 bzw. 16 der Richtlinie (EU) 2022/2555 eingerichtet wurden, bzw. ihre Stellvertreter können an den IICB-Sitzungen als Beobachter teilnehmen. In Ausnahmefällen kann der IICB im Einklang mit seiner Geschäftsordnung etwas anderes beschließen.

(6) Der IICB gibt sich eine Geschäftsordnung.

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

(8) Der IICB tritt auf Initiative seines Vorsitzenden, auf Ersuchen des CERT-EU und/oder auf Antrag eines seiner Mitglieder mindestens dreimal pro Jahr zusammen.

(9) 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 Vorsitzende des IICB beteiligt sich nicht an den Abstimmungen, außer bei Stimmengleichheit, bei der seine Stimme den Ausschlag gibt.

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

(11) Die Sekretariatsgeschäfte des IICB werden von der Kommission wahrgenommen; für die Sekretariatsgeschäfte besteht Rechenschaftspflicht gegenüber dem Vorsitzenden des IICB.

(12) Die vom EUAN benannten Vertreter leiten die Beschlüsse des IICB an die Mitglieder des EUAN weiter. Alle Mitglieder des EUAN haben das Recht, diese Vertreter oder den Vorsitz des IICB mit Angelegenheiten zu befassen, die ihrer Ansicht nach dem IICB zur Kenntnis gebracht werden sollten.

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

(14) Der IICB legt dem Europäischen Parlament und dem Rat bis zum … [12 Monate nach dem Tag des Inkrafttretens dieser Verordnung] und danach jährlich einen Bericht vor, in dem die Fortschritte bei der Durchführung dieser Verordnung im Einzelnen dargelegt werden und in dem insbesondere der Umfang der Zusammenarbeit des CERT-EU mit den entsprechenden Stellen in den einzelnen Mitgliedstaaten angegeben wird. Dieser Bericht bildet einen Beitrag zum Zweijahresbericht über den Stand der Cybersicherheit in der Union, der gemäß Artikel 18 der Richtlinie (EU) 2022/2555 angenommen wird.

Artikel 11

Aufgaben des IICB

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

a) Beratung des Leiters des CERT-EU,

b) wirksame Überwachung und Beaufsichtigung der Durchführung dieser Verordnung und Unterstützung der Einrichtungen der Union bei der Stärkung ihrer Cybersicherheit, gegebenenfalls einschließlich der Anforderung von Ad-hoc-Berichten von Einrichtungen der Union und dem CERT-EU,

c) im Anschluss an eine Strategiediskussion Annahme einer mehrjährigen Strategie zur Erhöhung des Cybersicherheitsniveaus in den Einrichtungen der Union und regelmäßige Bewertung - in jedem Fall aber alle fünf Jahre - und erforderlichenfalls Änderung der Strategie,

d) Festlegung der Methodik und der organisatorischen Aspekte für die Durchführung freiwilliger Peer-Reviews durch Einrichtungen der Union, um aus gemeinsamen Erfahrungen zu lernen, das gegenseitige Vertrauen zu stärken, ein hohes gemeinsames Cybersicherheitsniveau zu erreichen und die Cybersicherheitskapazitäten der Einrichtungen der Union zu verbessern, wobei sicherzustellen ist, dass diese Peer-Reviews von Cybersicherheitsexperten durchgeführt werden, die von einer anderen Einrichtung der Union als der zu überprüfenden Einrichtung der Union benannt wurden, und dass die Methode auf Artikel 19 der Richtlinie (EU) 2022/2555 beruht und gegebenenfalls auf die Einrichtungen der Union angepasst wird,

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

f) Genehmigung – auf der Grundlage eines Vorschlags der Leitung des CERT-EU – des Leistungskatalogs des CERT-EU und etwaiger Änderungen des Leistungskatalogs,

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

h) Genehmigung – auf der Grundlage eines Vorschlags der Leitung des CERT-EU– der Vorkehrungen für Leistungsvereinbarungen,

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

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

k) Genehmigung von Kooperationsvereinbarungen, Leistungsvereinbarungen oder Verträgen zwischen dem CERT-EU und anderen Stellen gemäß Artikel 18,

l) Annahme von Leitlinien und Empfehlungen auf der Grundlage eines Vorschlags des CERT-EU gemäß Artikel 14 und Anweisung des CERT-EU, einen Vorschlag für Leitlinien oder Empfehlungen oder einen Aufruf zum Tätigwerden vorzulegen, zurückzuziehen oder zu ändern,

m) Einsetzung von Fachberatungsgruppen mit konkreten Aufgaben zur Unterstützung der Arbeit des IICB, Genehmigung ihrer Mandate und Ernennung ihrer jeweiligen Vorsitzenden,

n) Erhalt und Bewertung der von den Einrichtungen der Union im Rahmen dieser Verordnung vorgelegten Unterlagen und Berichte, wie der Bewertungen des Cybersicherheitsreifegrads,

o) Förderung der Einsetzung einer informellen Gruppe, in der die lokalen Cybersicherheitsbeauftragten aller Einrichtungen zusammenkommen, auch mit Unterstützung durch die ENISA, wobei das Ziel verfolgt wird, bewährte Verfahren und Informationen im Zusammenhang mit der Durchführung dieser Verordnung auszutauschen,

p) unter Berücksichtigung der vom CERT-EU bereitgestellten Informationen über die ermittelten Cybersicherheitsrisiken und der gewonnenen Erkenntnisse Überwachung der Eignung der Vorkehrungen bezüglich der Interkonnektivität der IKT-Umgebungen der Einrichtungen der Union und Beratung zu möglichen Verbesserungen,

q) Aufstellung eines Plans für das Cyberkrisenmanagement, um auf operativer Ebene die koordinierte Bewältigung schwerwiegender Sicherheitsvorfälle, die Einrichtungen der Union betreffen, zu unterstützen und einen Beitrag zum regelmäßigen Austausch einschlägiger Informationen zu leisten, insbesondere in Bezug auf die Auswirkungen und die Schwere schwerwiegender Sicherheitsvorfälle und die Möglichkeiten zur Abmilderung ihrer Auswirkungen,

r) Koordinierung der Annahme der in Artikel 9 Absatz 2 genannten Pläne der einzelnen Einrichtungen der Union für das Cyberkrisenmanagement,

s) Annahme von Empfehlungen im Zusammenhang mit der Sicherheit der Lieferkette gemäß Artikel 8 Absatz 2 Unterabsatz 1 Buchstabe m unter Berücksichtigung der Ergebnisse der koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf der Ebene der Union gemäß Artikel 22 der Richtlinie (EU) 2022/2555 zur Unterstützung der Einrichtungen der Union bei der Annahme wirksamer und verhältnismäßiger Maßnahmen zum Management von Cybersicherheitsrisiken.

Artikel 12

Einhaltung

(1) Der IICB überwacht gemäß Artikel 10 Absatz 2 und Artikel 11 wirksam die Durchführung dieser Verordnung und die Umsetzung der angenommenen Leitlinien, Empfehlungen und Aufrufe zum Tätigwerden durch die Einrichtungen der Union. Der IICB kann die zu diesem Zweck erforderlichen Informationen oder Unterlagen von den Einrichtungen der Union anfordern. Für die Zwecke der Annahme von Compliance-Maßnahmen nach diesem Artikel hat die betroffene Einrichtung der Union kein Stimmrecht, wenn diese Einrichtung der Union direkt im IICB vertreten ist.

(2) Stellt der IICB fest, dass eine Einrichtung der Union diese Verordnung oder gemäß dieser Verordnung angenommene Leitlinien, Empfehlungen oder Aufrufe zum Tätigwerden nicht wirksam angewandt oder durchgeführt bzw. umgesetzt hat, so kann er – unbeschadet der internen Verfahren der betreffenden Einrichtung der Union und nachdem er der betreffenden Einrichtung der Union Gelegenheit gegeben hat, ihre Feststellungen darzulegen –

a) an die betreffende Einrichtung der Union eine mit Gründen versehene Stellungnahme zu den Defiziten übermitteln, die hinsichtlich der Durchführung dieser Verordnung festgestellt wurden,

b) nach Anhörung des CERT-EU der betreffenden Einrichtung der Union Leitlinien an die Hand geben, damit sie sicherstellen kann, dass ihr jeweiliges Rahmenwerk, ihre Maßnahmen zum Management von Cybersicherheitsrisiken, ihr Cybersicherheitsplan und ihre Berichterstattung innerhalb einer bestimmten Frist den Bestimmungen dieser Verordnung genügen,

c) eine Verwarnung aussprechen, damit festgestellte Mängel innerhalb einer bestimmten Frist behoben werden, einschließlich Empfehlungen zur Änderung von Maßnahmen, die von der betreffenden Einrichtung der Union gemäß dieser Verordnung angenommen wurden,

d) eine begründete Mitteilung an die betreffende Einrichtung der Union zu richten, falls Mängel, die in einer gemäß Buchstabe c ausgesprochenen Verwarnung festgestellt wurden, innerhalb der festgelegten Frist nicht ausreichend behoben wurden,

e) Folgendes tun:

   i) die Durchführung eines Audits empfehlen oder

   ii) verlangen, dass ein Audit von einem externen Prüfungsdienst durchgeführt wird,

f) gegebenenfalls den Rechnungshof im Rahmen seines Mandats über die mutmaßliche Nichteinhaltung unterrichten,

g) eine Empfehlung an alle Mitgliedstaaten und Einrichtungen der Union hinsichtlich einer vorübergehenden Aussetzung der Datenströme an die betreffende Einrichtung der Union abgeben.

Für die Zwecke von Unterabsatz 1 Buchstabe c ist der Adressatenkreis einer Warnung in geeigneter Weise einzuschränken, wenn dies in Anbetracht eines akuten Cybersicherheitsrisikos erforderlich ist.

Die gemäß Unterabsatz 1 ausgegebenen Warnungen und Empfehlungen sind an die höchste Managementebene der betreffenden Einrichtung der Union zu richten.

(3) Hat der IICB Maßnahmen nach Absatz 2 Unterabsatz 1 Buchstaben a bis g ergriffen, so legt die betroffene Einrichtung der Union Einzelheiten zu den Maßnahmen vor, die ergriffen wurden, um die vom IICB festgestellten mutmaßlichen Mängel zu beheben. Die Einrichtung der Union legt diese Einzelheiten innerhalb einer mit dem IIZB zu vereinbarenden angemessenen Frist vor.

(4) Ist der IICB der Auffassung, dass eine anhaltende Verletzung dieser Verordnung durch eine Einrichtung der Union vorliegt, die unmittelbar auf Handlungen oder Unterlassungen eines Beamten oder sonstigen Bediensteten der Union, auch auf der höchsten Managementebene, zurückzuführen ist, so fordert der IICB die betreffende Einrichtung der Union auf, geeignete Maßnahmen zu ergreifen, einschließlich der Aufforderung, disziplinarrechtliche Maßnahmen im Einklang mit den im Statut festgelegten Regeln und Verfahren und sonstigen anwendbaren Regeln und Verfahren in Betracht zu ziehen. Hierzu übermittelt der IICB der betreffenden Einrichtung der Union die erforderlichen Informationen.

(5) Teilen die Einrichtungen der Union mit, dass sie nicht in der Lage sind, die in Artikel 6 Absatz 1 und Artikel 8 Absatz 1 genannten Fristen einzuhalten, so kann der IICB in hinreichend begründeten Fällen und unter Berücksichtigung der Größe der Einrichtung der Union die Verlängerung dieser Fristen gestatten.

Kapitel IV
CERT-EU

Artikel 13

Auftrag und Aufgaben des CERT-EU

(1) Der Auftrag des CERT-EU besteht darin, zur Sicherheit der nicht für Verschlusssachen genutzten IKT-Umgebung von Einrichtungen der Union beizutragen, indem es diese in Cybersicherheitsangelegenheiten berät, bei der Prävention, Erkennung, Handhabung, Eindämmung, Bewältigung und Erholung 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 erhebt, verwaltet und analysiert Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle betreffend nicht für Verschlusssachen genutzte IKT-Infrastrukturen und tauscht diese Informationen mit den Einrichtungen der Union aus. Es koordiniert die Reaktionen auf Sicherheitsvorfälle auf interinstitutioneller Ebene und auf der Ebene der Einrichtungen der Union, einschließlich durch die Bereitstellung oder Koordinierung der Bereitstellung spezifischer operativer Unterstützung.

(3) Das CERT-EU nimmt folgende Aufgaben zur Unterstützung der Einrichtungen der Union wahr:

a) Unterstützung der Einrichtungen der Union bei der Durchführung dieser Verordnung und Beitrag zur Koordinierung der Anwendung dieser Verordnung durch die in Artikel 14 Absatz 1 aufgeführten Maßnahmen oder durch vom IICB angeforderte Ad-hoc-Berichte,

b) Bereitstellung von Standard-CSIRT-Diensten für alle Einrichtungen der Union über ein Paket von Cybersicherheitsdiensten, die in seinem Leistungskatalog beschrieben sind (im Folgenden „Basisdienste“),

c) Pflege eines Netzes entsprechender Stellen und Partner zur Unterstützung der in den Artikeln 17 und 18 genannten Dienste,

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

e) auf der Grundlage der Informationen gemäß Absatz 2 Beitrag zur Erfassung der Cyberlage in der EU in enger Zusammenarbeit mit der ENISA,

f) Koordinierung der Bewältigung schwerwiegender Sicherheitsvorfälle,

g) Handeln im Namen der Einrichtungen der Union als Äquivalent des für die Zwecke einer koordinierten Offenlegung von Schwachstellen gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 benannten Koordinators,

h) auf Ersuchen einer Einrichtung der Union Durchführung eines proaktiven, nicht-intrusiven Scannens öffentlich zugänglicher Netz- und Informationssysteme dieser Einrichtung der Union.

Die in Unterabsatz 1 Buchstabe e genannten Informationen werden mit dem IICB, dem CSIRTs-Netz und dem Zentrum der Europäischen Union für Informationsgewinnung und Lageerfassung (EU INTCEN) ausgetauscht, soweit dies möglich und angemessen ist, und unterliegen adäquaten Vertraulichkeitsbestimmungen.

(4) Das CERT-EU kann gemäß Artikel 17 bzw. 18 mit einschlägigen Cybersicherheitsgemeinschaften in der Union und ihren Mitgliedstaaten zusammenarbeiten, unter anderem in folgenden Bereichen:

a) Abwehrbereitschaft, Koordinierung bei Sicherheitsvorfällen, Informationsaustausch und Krisenreaktion auf der technischen Ebene in Fällen in Verbindung mit Einrichtungen der Union,

b) operative Zusammenarbeit in Bezug auf das CSIRTs-Netz, auch zur gegenseitigen Unterstützung,

c) Informationen über Cyberbedrohungen, einschließlich Lageerfassung,

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

(5) Das CERT-EU kooperiert im Rahmen seiner Zuständigkeit in strukturierter Weise mit der ENISA in den Bereichen Kapazitätsaufbau, operative Zusammenarbeit und langfristige strategische Analysen von Cyberbedrohungen im Einklang mit der Verordnung (EU) 2019/881. Das CERT-EU kann mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität von Europol zusammenarbeiten und Informationen austauschen.

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

a) andere als die in Absatz 3 genannten Dienste, die die Cybersicherheit der IKT-Umgebung von Einrichtungen der Union unterstützen, auf der Grundlage von Leistungsvereinbarungen und vorbehaltlich verfügbarer Ressourcen, insbesondere die Überwachung eines breiten Spektrums von Netzen, darunter eine Rund-um-die-Uhr-Überwachung auf der ersten Ebene zur Erkennung hochgradig gefährlicher Cyberbedrohungen,

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

c) auf Anfrage eine proaktive Überprüfung der Netz- und Informationssysteme der betreffenden Einrichtung der Union, um Schwachstellen mit potenziell erheblichen Auswirkungen aufzudecken,

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

In Bezug auf Unterabsatz 1 Buchstabe d kann das CERT-EU in Ausnahmefällen mit vorheriger Zustimmung des IICB Leistungsvereinbarungen mit anderen Einrichtungen als den Einrichtungen der Union schließen.

(7) Das CERT-EU muss Cybersicherheitsübungen organisieren und kann an Cybersicherheitsübungen teilnehmen oder die Teilnahme an bestehenden Übungen empfehlen, gegebenenfalls in enger Zusammenarbeit mit der ENISA, um das Cybersicherheitsniveau der Einrichtungen der Union zu prüfen.

(8) Das CERT-EU kann Einrichtungen der Union in Bezug auf Sicherheitsvorfälle in Netz- und Informationssystemen, in denen EU-VS bearbeitet werden, unterstützen, wenn es von den betreffenden Einrichtungen der Union gemäß ihren jeweiligen Verfahren ausdrücklich dazu aufgefordert wird. Die Unterstützung durch das CERT-EU gemäß diesem Absatz lässt die geltenden Rechtsvorschriften über den Schutz von als Verschlusssachen eingestuften Informationen unberührt.

(9) Das CERT-EU unterrichtet die Einrichtungen der Union über seine Abläufe und Verfahren zur Handhabung von Sicherheitsvorfällen.

(10) Das CERT-EU stellt mit einem hohen Maß an Vertraulichkeit und Zuverlässigkeit über geeignete Kooperationsmechanismen und Meldewege sachdienliche und anonymisierte Informationen über schwerwiegende Sicherheitsvorfälle und die Art und Weise des Umgangs mit ihnen zur Verfügung. Diese Informationen werden in den in Artikel 10 Absatz 14 genannten Bericht aufgenommen.

(11) Das CERT-EU unterstützt in Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten die betroffenen Einrichtungen der Union bei der Bearbeitung von Sicherheitsvorfällen, die zu Verletzungen des Schutzes personenbezogener Daten führen, und zwar unbeschadet der Zuständigkeiten und Aufgaben des Europäischen Datenschutzbeauftragten als Aufsichtsbehörde gemäß der Verordnung (EU) 2018/1725.

(12) Das CERT-EU kann auf ausdrückliches Ersuchen der Fachabteilungen der Einrichtungen der Union technische Gutachten oder Beiträge zu wichtigen strategischen Aspekten liefern.

Artikel 14

Leitlinien, Empfehlungen und Aufrufe zum Tätigwerden

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

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

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

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

In Bezug auf Unterabsatz 1 Buchstabe a unterrichtet die betreffende Einrichtung der Union das CERT-EU unverzüglich nach Eingang des Aufrufs zum Tätigwerden darüber, wie die dringenden Sicherheitsmaßnahmen angewandt wurden.

(2) Die Leitlinien und Empfehlungen können Folgendes umfassen:

a) gemeinsame Methoden und ein Modell für die Bewertung der Cybersicherheitsreife der Einrichtungen der Union, einschließlich der entsprechenden Skalen oder wesentlichen Leistungsindikatoren, die als Referenz dienen, um die kontinuierliche Verbesserung der Cybersicherheit in allen Einrichtungen der Union zu unterstützen und die Priorisierung von Cybersicherheitsbereichen und -maßnahmen unter Berücksichtigung der Cybersicherheitslage der Einrichtungen zu erleichtern,

b) Vorkehrungen für das Management von Cybersicherheitsrisiken und die Maßnahmen zum Management von Cybersicherheitsrisiken oder diesbezügliche Verbesserungen,

c) Vorkehrungen für die Bewertungen des Cybersicherheitsreifegrads und die Cybersicherheitspläne;

d) gegebenenfalls den Einsatz gemeinsamer Technologie, Architektur, Open Source und dazugehöriger bewährter Verfahren mit dem Ziel, Interoperabilität und gemeinsame Normen, einschließlich eines koordinierten Ansatzes für die Sicherheit der Lieferkette, zu erreichen;

e) gegebenenfalls Informationen zur Erleichterung der Nutzung gemeinsamer Instrumente für die Auftragsvergabe zur Beschaffung einschlägiger Cybersicherheitsdienste und -produkte von Drittanbietern;

f) Vereinbarungen über den Informationsaustausch gemäß Artikel 20.

Artikel 15

Die Leitung des CERT-EU

(1) Die Kommission ernennt die Leiterin bzw. den Leiter des CERT-EU, nachdem sie die Zustimmung einer Zweidrittelmehrheit der Mitglieder des IICB erhalten hat. Der IICB wird in allen Phasen des Ernennungsverfahrens konsultiert, insbesondere zur Formulierung von Stellenausschreibungen, zur Prüfung von Bewerbungen und zur Ernennung von Auswahlausschüssen im Zusammenhang mit dem Posten. Das Auswahlverfahren, einschließlich der endgültigen Auswahlliste der Bewerberinnen und Bewerber, aus denen die Leiterin bzw. der Leiter des CERT-EU zu ernennen ist, gewährleistet eine ausgewogene Vertretung jedes Geschlechts unter Berücksichtigung der eingereichten Bewerbungen.

(2) Die Leitung des CERT-EU ist für das reibungslose Funktionieren des CERT-EU verantwortlich und handelt im Rahmen der Zuständigkeiten seiner Funktion unter der Leitung des IICB. Die Leitung des CERT-EU berichtet regelmäßig dem Vorsitzenden des IICB und legt dem IICB auf Anfrage Ad-hoc-Berichte vor.

(3) Die Leitung des CERT-EU unterstützt den zuständigen bevollmächtigten Anweisungsbefugten bei der Erstellung des in Artikel 74 Absatz 9 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates[1] vorgesehenen jährlichen Tätigkeitsberichts, der Finanz- und Verwaltungsinformationen, einschließlich der Ergebnisse von Kontrollen, enthält, und erstattet dem bevollmächtigten Anweisungsbefugten regelmäßig Bericht über die Durchführung von Maßnahmen, für die eine Weiterübertragung von Befugnissen an die Leitung des CERT-EU erfolgt ist.

(4) Die Leitung des CERT-EU erstellt alljährlich eine Finanzplanung für die Verwaltungseinnahmen und -ausgaben für dessen Tätigkeiten, ein vorgeschlagenes jährliches Arbeitsprogramm, einen vorgeschlagenen Leistungskatalog des CERT-EU, vorgeschlagene Überarbeitungen des Leistungskatalogs, vorgeschlagene Vorkehrungen für Leistungsvereinbarungen und vorgeschlagene wesentliche Leistungsindikatoren für das CERT-EU, die vom IICB gemäß Artikel 11 zu billigen sind. Bei der Überarbeitung der Liste der Dienste im Leistungskatalog des CERT-EU berücksichtigt die Leitung des CERT-EU die dem CERT-EU zugewiesenen Ressourcen.

---

[1] 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).

(5) Die Leitung des CERT-EU legt dem IICB und dem Vorsitzenden des IICB mindestens jährlich Berichte über die Tätigkeiten und die Leistung des CERT-EU während des Bezugszeitraums vor, unter anderem über die Ausführung des Haushaltsplans, Leistungsvereinbarungen und schriftliche Vereinbarungen, die Zusammenarbeit mit entsprechenden Stellen und Partnern und Dienstreisen des Personals, einschließlich der in Artikel 11 genannten Berichte. Diese Berichte enthalten ein Arbeitsprogramm für den folgenden Zeitraum, die Finanzplanung der Einnahmen und Ausgaben, einschließlich Personalkosten, geplante Aktualisierungen des Leistungskatalogs des CERT-EU und eine Bewertung der erwarteten Auswirkungen solcher Aktualisierungen auf die finanziellen und personellen Ressourcen.

Artikel 16

Finanzen und Personal

(1) Das CERT-EU wird in die Verwaltungsstruktur einer Generaldirektion der Kommission integriert, damit es die unterstützenden Strukturen der Kommission in den Bereichen Verwaltung, Finanzmanagement und Rechnungsführung nutzen kann, gleichzeitig aber sein Status als eigenständiger interinstitutioneller Dienstleister für alle Einrichtungen der Union erhalten bleibt. Die Kommission unterrichtet den IICB über die administrative Zuordnung des CERT-EU und diesbezügliche Änderungen. Die Kommission überprüft die Verwaltungsvereinbarungen im Zusammenhang mit dem CERT-EU regelmäßig, in jedem Fall jedoch vor der Festlegung eines mehrjährigen Finanzrahmens gemäß Artikel 312 AEUV, um geeignete Maßnahmen zu ermöglichen. Die Überprüfung umfasst die Möglichkeit, das CERT-EU als Amt der Union einzurichten.

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

(3) Aufgaben und Tätigkeiten des CERT-EU, einschließlich der Dienste, die vom CERT-EU gemäß Artikel 13 Absätze 3, 4, 5 und 7 sowie gemäß Artikel 14 Absatz 1 für aus der Rubrik „Europäische öffentliche Verwaltung“ des mehrjährigen Finanzrahmens finanzierte Einrichtungen 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 dieses Artikels genannten Einrichtungen der Union leisten einen jährlichen finanziellen Beitrag zum CERT-EU zur Deckung der vom CERT-EU gemäß dem genannten Absatz erbrachten Dienste. Die jeweiligen Beiträge beruhen auf Vorgaben des IICB und werden jeweils zwischen den einzelnen Einrichtungen der Union 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 als interne zweckgebundene Einnahmen in die in Absatz 3 dieses Artikels genannte gesonderte Haushaltslinie eingestellt.

(5) Die Kosten für die in Artikel 13 Absatz 6 festgelegten Leistungen werden bei den Einrichtungen der Union eingezogen, denen CERT-EU-Dienste erbracht werden. Die Einnahmen werden in die Haushaltslinien eingestellt, in denen die Kosten angesetzt wurden.

Artikel 17

Zusammenarbeit des CERT-EU mit den entsprechenden Stellen der Mitgliedstaaten

(1) Das CERT-EU arbeitet unverzüglich mit den entsprechenden Stellen der Mitgliedstaaten, insbesondere den gemäß Artikel 10 der Richtlinie (EU) 2022/2555 benannten oder eingerichteten CSIRTs oder, falls zutreffend, den gemäß Artikel 8 der genannten Richtlinie benannten oder eingerichteten zuständigen Behörden und zentralen Anlaufstellen zusammen und tauscht Informationen mit ihnen aus über Cyberbedrohungen, Schwachstellen, Beinahe-Vorfälle, mögliche Gegenmaßnahmen sowie bewährte Verfahren und über alle Angelegenheiten, die für die Verbesserung des Schutzes der IKT-Umgebungen der Einrichtungen der Union relevant sind, auch durch das gemäß Artikel 15 der Richtlinie (EU) 2022/2555 eingerichtete CSIRTs-Netzwerk. Das CERT-EU unterstützt die Kommission im Rahmen des gemäß Artikel 16 der Richtlinie (EU) 2022/2555 über die koordinierte Bewältigung von schwerwiegenden Vorfällen und Krisen eingerichteten EU-CyCLONe.

(2) Wenn das CERT-EU Kenntnis von einem erheblichen Sicherheitsvorfall in einem Mitgliedstaat erhält, unterrichtet es gemäß Absatz 1 unverzüglich alle einschlägigen entsprechenden Stellen dieses Mitgliedstaates.

(3) Sofern personenbezogene Daten im Einklang mit dem geltenden Datenschutzrecht der Union geschützt sind, gibt das CERT-EU relevante Informationen über spezifische Sicherheitsvorfälle ohne Genehmigung der betroffenen Einrichtung der Union unverzüglich an die entsprechenden Stellen der Mitgliedstaaten weiter, um die Aufdeckung ähnlicher Cyberbedrohungen oder Sicherheitsvorfälle zu erleichtern oder zur Analyse eines Sicherheitsvorfalls beizutragen. Das CERT-EU gibt spezifische Informationen über Sicherheitsvorfälle, aus denen die Identität der Zielgruppe des Cybersicherheitsvorfalls hervorgeht, nur in einem der folgenden Fälle weiter:

a) Die betroffene Einrichtung der Union erteilt ihre Zustimmung,

b) die betroffene Einrichtung der Union erteilt ihre Zustimmung gemäß Buchstabe a nicht, aber die Offenlegung der Identität der betroffenen Einrichtung der Union würde die Wahrscheinlichkeit erhöhen, dass anderswo Sicherheitsvorfälle vermieden oder abgeschwächt werden,

c) die betroffene Einrichtung der Union hat bereits öffentlich gemacht, dass sie betroffen war.

Beschlüsse über den Austausch spezifischer Informationen über Sicherheitsvorfälle, aus denen die Identität des Ziels des Sicherheitsvorfalls gemäß Unterabsatz 1 Buchstabe b hervorgeht, werden von der Leitung des CERT-EU gebilligt. Bevor ein solcher Beschluss gefasst wird, setzt sich das CERT-EU schriftlich mit der betroffenen Einrichtung der Union in Verbindung und erläutert klar, wie die Offenlegung ihrer Identität dazu beitragen würde, Sicherheitsvorfälle an anderer Stelle zu vermeiden oder abzuschwächen. Die Leitung des CERT-EU liefert die Erläuterung und fordert die Einrichtung der Union ausdrücklich auf, innerhalb einer bestimmten Frist mitzuteilen, ob sie einwilligt. Die Leitung des CERT-EU teilt der Einrichtung der Union ferner mit, dass sie sich aufgrund der vorgetragenen Erläuterung das Recht vorbehält, die Informationen auch dann offenzulegen, wenn keine Einwilligung vorliegt. Die betroffene Einrichtung der Union wird unterrichtet, bevor die Informationen offengelegt werden.

Artikel 18

Zusammenarbeit des CERT-EU mit anderen *entsprechenden Stellen*

(1) Das CERT-EU kann in Bezug auf Instrumente und Methoden wie Techniken, Taktiken, Verfahren und bewährte Verfahren sowie in Bezug auf Cyberbedrohungen und Schwachstellen mit anderen entsprechenden Stellen in der Europäischen Union als den in Artikel 17 genannten Stellen, die den Cybersicherheitsanforderungen der Union unterliegen, einschließlich branchenspezifischer entsprechender Stellen, zusammenarbeiten. Für jede Zusammenarbeit mit diesen entsprechenden Stellen holt das CERT-EU vorab im Einzelfall die Zustimmung des IICB ein. Nimmt das CERT-EU eine Zusammenarbeit mit diesen entsprechenden Stellen auf, so informiert es alle in Artikel 17 Absatz 1 genannten einschlägigen entsprechenden Stellen in dem Mitgliedstaat, in dem die entsprechende Stelle ansässig ist. Gegebenenfalls werden diese Zusammenarbeit und die Bedingungen hierfür, auch in Bezug auf Cybersicherheit, Datenschutz und den Umgang mit Informationen, in spezifischen Vertraulichkeitsvereinbarungen wie Verträgen oder Verwaltungsvereinbarungen festgelegt. Die Vertraulichkeitsvereinbarungen bedürfen keiner vorherigen Zustimmung des IICB, jedoch ist dessen Vorsitzender davon in Kenntnis zu setzen. Im Falle einer dringenden und unmittelbar bevorstehenden Notwendigkeit, Cybersicherheitsinformationen im Interesse von Einrichtungen der Union oder einer anderen Partei auszutauschen, kann das CERT-EU dies mit einer Einrichtung tun, deren spezifische Kompetenz, Kapazitäten und Fachkenntnisse berechtigterweise erforderlich sind, um bei einer solchen dringenden Notwendigkeit zu helfen, selbst wenn das CERT-EU mit dieser Einrichtung keine Vertraulichkeitsvereinbarung getroffen hat. In solchen Fällen unterrichtet das CERT-EU unverzüglich den Vorsitzenden des IICB und erstattet dem IICB in regelmäßigen Berichten oder Sitzungen Bericht.

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

(3) Das CERT-EU kann mit Zustimmung der von einem Sicherheitsvorfall betroffenen Einrichtung der Union und unter der Voraussetzung, dass eine Geheimhaltungsvereinbarung oder einen Nichoffenlegungsvertrag mit der betreffenden entsprechenden Stelle oder dem betreffenden Partner geschlossen wurde, den in den Absätzen 1 und 2 genannten entsprechenden Stellen oder Partnern Informationen über diesen konkreten Sicherheitsvorfall ausschließlich zu dem Zweck zur Verfügung stellen, zu seiner Analyse beizutragen.

Kapitel V
Zusammenarbeit und Berichterstattungspflichten

Artikel 19

Umgang mit Informationen

(1) Die Einrichtungen der Union und das CERT-EU kommen der Verpflichtung zur Wahrung des Berufsgeheimnisses gemäß Artikel 339 AEUV oder gleichwertigen geltenden Rahmenregelungen nach.

(2) Die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates[1] 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 Einrichtungen der Union oder gegebenenfalls der Mitgliedstaaten, wenn eine Anfrage deren Dokumente betrifft.

(3) Der Umgang der Einrichtungen der Union und des CERT-EU mit Informationen erfolgt im Einklang mit den geltenden Vorschriften über die Informationssicherheit.

Artikel 20

Vereinbarungen über den Austausch von Informationen zur Cybersicherheit

(1) Einrichtungen der Union können dem CERT-EU auf freiwilliger Basis sie betreffende Sicherheitsvorfälle, Cyberbedrohungen, Beinahe-Vorfälle und Schwachstellen melden und ihm Informationen darüber weitergeben. Das CERT-EU stellt sicher, dass effiziente Kommunikationsmittel mit einem hohen Maß an Rückverfolgbarkeit, Vertraulichkeit und Zuverlässigkeit zur Verfügung stehen, die den Informationsaustausch mit den Einrichtungen der Union erleichtern. Bei der Verarbeitung von Meldungen kann das CERT-EU der Bearbeitung von Pflichtmeldungen Vorrang vor freiwilligen Meldungen einräumen. Unbeschadet des Artikels 12 dürfen freiwillige Meldungen nicht dazu führen, dass der meldenden Einrichtung der Union zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

---

[1] 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).

(2) Zur Erfüllung seines Auftrags und seiner Aufgaben gemäß Artikel 13 kann das CERT-EU von den Einrichtungen der Union verlangen, ihm Informationen aus ihren jeweiligen IKT-Systemverzeichnissen zu übermitteln, einschließlich Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Kompromittierungsindikatoren (indicators of compromise), Cybersicherheitswarnungen und Empfehlungen zur Konfiguration von Cybersicherheitswerkzeugen zur Erkennung von Sicherheitsvorfällen. Die betreffende Einrichtung der Union übermittelt die verlangten Informationen und alle späteren Aktualisierungen unverzüglich.

(3) Das CERT-EU darf spezifische Informationen über Sicherheitsvorfälle, aus denen die Identität der von dem Sicherheitsvorfall betroffenen Einrichtung der Union hervorgeht an Einrichtungen der Union weitergeben, sofern die betroffene Einrichtung zustimmt. Verweigert eine Einrichtung der Union ihre Einwilligung, so legt sie dem CERT-EU Gründe für diese Entscheidung vor.

(4) Einrichtungen der Union geben dem Europäischen Parlament und dem Rat auf Anfrage Informationen über den Abschluss von Cybersicherheitsplänen weiter.

(5) Der IICB bzw. das CERT-EU geben dem Europäischen Parlament und dem Rat auf Anfrage Leitlinien, Empfehlungen und Aufforderungen zum Tätigwerden weiter.

(6) Die in diesem Artikel festgelegten Weitergabepflichten erstrecken sich nicht auf

a) EU-VS,

b) Informationen, deren Weiterverbreitung durch eine sichtbare Kennzeichnung ausgeschlossen wurde, es sei denn, ihre Weitergabe an das CERT-EU wurde ausdrücklich gestattet.

Artikel 21

Berichterstattungspflichten

(1) Ein Sicherheitsvorfall gilt als erheblich, wenn

a) er eine schwerwiegende Störung des Betriebs der betreffenden Einrichtung der Union oder einen finanziellen Verlust für sie verursacht hat oder verursachen kann;

b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

(2) Die Einrichtungen der Union übermitteln dem CERT-EU:

a) unverzüglich und in jedem Fall spätestens 24 Stunden, nachdem sie von dem erheblichen Sicherheitsvorfall Kenntnis erlangt haben, eine Frühwarnung, in der gegebenenfalls angegeben wird, dass der erhebliche Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist bzw. sich einrichtungs- oder auch grenzübergreifend auswirken könnte;

b) unverzüglich, in jedem Fall aber spätestens 72 Stunden, nachdem sie von dem erheblichen Sicherheitsvorfall Kenntnis erlangt haben, eine Meldung des Sicherheitsvorfall, in dem gegebenenfalls die unter Buchstabe a genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie, soweit verfügbar, die Kompromittierungssindikatoren angegeben werden;

c) auf Ersuchen des CERT-EU einen Zwischenbericht über relevante Statusaktualisierungen;

d) spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Buchstabe b einen Abschlussbericht, der Folgendes enthält:

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

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

   iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen,

   iv) gegebenenfalls die grenz- bzw. einrichtungsübergreifenden Auswirkungen des Sicherheitsvorfalls,

e) im Falle eines zum Zeitpunkt der Vorlage des Abschlussberichts gemäß Buchstabe d andauernden Sicherheitsvorfalls einen Fortschrittsbericht zu diesem Zeitpunkt und innerhalb eines Monats nach Behandlung des Vorfalls einen Abschlussbericht.

(3) Eine Einrichtung der Union unterrichtet unverzüglich, in jedem Fall aber innerhalb von 24 Stunden, nachdem sie Kenntnis von einem erheblichen Sicherheitsvorfall erlangt hat, alle in Artikel 17 Absatz 1 genannten einschlägigen entsprechenden mitgliedstaatlichen Stellen in dem Mitgliedstaat, in dem sie angesiedelt ist, darüber, dass ein erheblicher Sicherheitsvorfall aufgetreten ist.

(4) Die Einrichtungen der Union melden unter anderem sämtliche Informationen, die das CERT-EU in die Lage versetzen, die Auswirkungen eines erheblichen Sicherheitsvorfalls auf andere Einrichtungen und auf den Aufnahmemitgliedstaat bzw. seine grenzübergreifenden Auswirkungen zu ermitteln. Unbeschadet des Artikels 12 wird mit der bloßen Meldung keine höhere Haftung der Einrichtung der Union begründet.

(5) Gegebenenfalls teilen die Einrichtungen der Union den Nutzern der betroffenen Netz- und Informationssysteme oder anderer Komponenten des IKT-Umgebung, die potenziell von einem erheblichen Sicherheitsvorfall oder einer erheblichen Cyberbedrohung betroffen sind und gegebenenfalls Abhilfemaßnahmen treffen müssen, unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die sie als Reaktion auf diesen Sicherheitsvorfall bzw. diese Cyberbedrohung ergreifen können. Erforderlichenfalls informieren die Einrichtungen der Union diese Nutzer über die erhebliche Cyberbedrohung selbst.

(6) Betrifft ein erheblicher Sicherheitsvorfall oder eine erhebliche Cyberbedrohung ein Netz- und Informationssystem oder eine Komponente der IKT-Umgebung einer Einrichtung der Union, von der bekannt ist, dass sie mit der IKT-Umgebung einer anderen Einrichtung der Union verbunden ist, gibt das CERT-EU unverzüglich eine entsprechende Cybersicherheitswarnung aus.

(7) Die Einrichtungen der Union übermitteln dem CERT-EU auf dessen Anfrage unverzüglich die digitalen Informationen, die bei der Nutzung von den an den jeweiligen Sicherheitsvorfällen beteiligten Geräten erzeugt wurden. Das CERT-EU kann weitere Angaben zu den Arten von Informationen machen, die es für die Lageerfassung und die Reaktion auf den Sicherheitsvorfall benötigt.

(8) Das CERT-EU übermittelt dem IICB, der ENISA, dem EU INTCEN und dem CSIRTs-Netz alle drei Monate einen zusammenfassenden Bericht mit anonymisierten und aggregierten Daten zu erheblichen Sicherheitsvorfällen, Sicherheitsvorfällen, Cyberbedrohungen, Beinahe-Vorfällen und Schwachstellen gemäß Artikel 20 sowie zu erheblichen Sicherheitsvorfällen, die gemäß Absatz 2 dieses Artikels gemeldet wurden. Der zusammenfassende Bericht bildet einen Beitrag zum Zweijahresbericht über den Stand der Cybersicherheit in der Union, der gemäß Artikel 18 der Richtlinie (EU) 2022/2555 angenommen wird.

(9) Der IICB gibt bis zum … [sechs Monate nach dem Tag des Inkrafttretens dieser Verordnung] Leitlinien oder Empfehlungen heraus, in denen die Modalitäten, das Format und der Inhalt der Berichterstattung gemäß diesem Artikel näher festgelegt werden. Bei der Ausarbeitung solcher Leitlinien oder Empfehlungen berücksichtigt der IICB alle gemäß Artikel 23 Absatz 11 der Richtlinie (EU) 2022/2555 erlassenen Durchführungsrechtsakte, in denen die Art der Angaben, das Format und das Verfahren der Meldungen festgelegt werden. Das CERT-EU verbreitet die sachdienlichen technischen Einzelheiten, um eine proaktive Erkennung und Reaktion oder Abhilfemaßnahmen durch die Einrichtungen der Union zu ermöglichen.

(10) Die in diesem Artikel festgelegten Berichterstattungspflichten erstrecken sich nicht auf

a) EU-VS,

b) Informationen, deren Weiterverbreitung durch eine sichtbare Kennzeichnung ausgeschlossen wurde, es sei denn, ihre Weitergabe an das CERT-EU wurde ausdrücklich gestattet.

Artikel 22

Koordinierung der Reaktion auf Sicherheitsvorfälle und Zusammenarbeit

(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, Schwachstellen und Beinahe-Vorfälle zwischen:

a) Einrichtungen der Union,

b) den in den Artikeln 17 und 18 genannten entsprechenden Stellen.

(2) Das CERT-EU – gegebenenfalls in enger Zusammenarbeit mit der ENISA – erleichtert die Koordinierung zwischen den Einrichtungen der Union bei der Reaktion auf Sicherheitsvorfälle, unter anderem durch

a) einen Beitrag zur kontinuierlichen externen Kommunikation,

b) gegenseitige Unterstützung, z. B. durch die Weitergabe von Informationen, die für Einrichtungen der Union relevant sind, oder die Bereitstellung von Hilfe, gegebenenfalls direkt vor Ort,

c) optimale Nutzung der operativen Ressourcen,

d) die Koordinierung mit anderen Krisenreaktionsmechanismen auf Unionsebene.

(3) Das CERT-EU unterstützt in enger Zusammenarbeit mit der ENISA die Einrichtungen der Union bei der Lageerfassung im Falle von Sicherheitsvorfällen, Cyberbedrohungen, Schwachstellen und Beinahe-Vorfällen und beim Austausch über einschlägige Entwicklungen im Bereich der Cybersicherheit.

(4) Der IICB nimmt bis zum … [12 Monate nach dem Tag des Inkrafttretens dieser Verordnung] auf der Grundlage eines Vorschlags des CERT-EU Leitlinien oder Empfehlungen für die Koordinierung der Reaktion auf Sicherheitsvorfälle und die Zusammenarbeit bei erheblichen Sicherheitsvorfällen an. Wenn ein Sicherheitsvorfall mutmaßlich einen kriminellen Hintergrund hat, formuliert das CERT-EU unverzüglich Ratschläge für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

(5) Auf besonderes Ersuchen eines Mitgliedstaats und mit Zustimmung der betreffenden Einrichtungen der Union kann das CERT-EU Sachverständige aus der in Artikel 23 Absatz 4 genannten Liste hinzuziehen, um zur Reaktion auf einen schwerwiegenden Sicherheitsvorfall, der Auswirkungen in diesem Mitgliedstaat hat, oder einen Cybersicherheitsvorfall großen Ausmaßes gemäß Artikel 15 Absatz 3 Buchstabe g der Richtlinie (EU) 2022/2555 beizutragen. Besondere Vorschriften für den Zugang zu technischen Sachverständigen der Einrichtungen der Union und deren Nutzung werden vom IICB auf Vorschlag des CERT-EU gebilligt.

Artikel 23

Bewältigung schwerwiegender Sicherheitsvorfälle

(1) Um auf operativer Ebene die koordinierte Bewältigung schwerwiegender Sicherheitsvorfälle, von denen Einrichtungen der Union betroffen sind, zu unterstützen und zum regelmäßigen Austausch einschlägiger Informationen zwischen Einrichtungen der Union und mit Mitgliedstaaten beizutragen, entwickelt der IICB gemäß Artikel 11 Buchstabe q in enger Zusammenarbeit mit dem CERT-EU und der ENISA einen Cyberkrisenbewältigungsplan auf der Grundlage der in Artikel 22 Absatz 2 genannten Tätigkeiten. Der Cyberkrisenbewältigungsplan umfasst mindestens die folgenden Elemente:

a) Regelungen für die Koordinierung und den Informationsfluss zwischen Einrichtungen der Union zur Bewältigung schwerwiegender Sicherheitsvorfälle auf operativer Ebene,

b) gemeinsame Standardarbeitsverfahren,

c) eine gemeinsame Taxonomie des Schweregrads schwerwiegender Sicherheitsvorfälle und der Auslöser von Krisen,

d) regelmäßige Übungen,

e) zu verwendende sichere Kommunikationskanäle.

(2) Der Vertreter der Kommission im IICB ist vorbehaltlich des gemäß Absatz 1 dieses Artikels erstellten Cyberkrisenbewältigungsplans und unbeschadet des Artikels 16 Absatz 2 Unterabsatz 1 der Richtlinie (EU) 2022/2555 die Kontaktstelle für den Austausch einschlägiger Informationen über schwerwiegende Sicherheitsvorfälle mit dem EU-CyCLONe.

(3) Das CERT-EU koordiniert die Maßnahmen der Einrichtungen der Union zur Bewältigung schwerwiegender Sicherheitsvorfälle. Es führt ein Verzeichnis der verfügbaren technischen Fachkenntnisse, die für die Reaktion auf solche schwerwiegenden Sicherheitsvorfälle notwendig sind, und unterstützt den IICB bei der Koordinierung der Cyberkrisenmanagementpläne der Einrichtungen der Union für schwerwiegende Sicherheitsvorfälle gemäß Artikel 9 Absatz 2.

(4) Die Einrichtungen 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.

Kapitel VI
Schlussbestimmungen

Artikel 24

Erste Umschichtung von Haushaltsmitteln

Um ein ordnungsgemäßes und stabiles Funktionieren des CERT-EU sicherzustellen, kann die Kommission die Umschichtung personeller und finanzieller Ressourcen zum Haushaltsplan der Kommission zur Verwendung im Betrieb des CERT-EU vorschlagen. Die Umschichtung wird zum Zeitpunkt der Annahme des ersten nach dem Inkrafttreten dieser Verordnung angenommenen jährlichen Haushaltsplans der Union wirksam.

Artikel 25

Überprüfung

(1) Bis zum … [zwölf Monate nach dem Tag des Inkrafttretens dieser Verordnung] und danach jährlich erstattet der IICB der Kommission mit Unterstützung des CERT-EU über die Durchführung dieser Verordnung. Der IICB kann Empfehlungen an die Kommission richten, diese Verordnung zu überprüfen.

(2) Bis zum … [36 Monate nach dem Tag des Inkrafttretens dieser Verordnung] und danach alle zwei Jahre bewertet die Kommission die Durchführung dieser Verordnung und die auf strategischer und betrieblicher Ebene gemachten Erfahrungen und erstattet dem Europäischen Parlament und dem Rat darüber Bericht.

Der in Unterabsatz 1 dieses Absatzes genannte Bericht enthält die in Artikel 16 Absatz 1 genannte Überprüfung der Möglichkeit, das CERT-EU als Amt der Union einzurichten.

(3) Die Kommission bewertet bis zum … [fünf Jahre nach dem Tag des Inkrafttretens dieser Verordnung] die Funktionsweise dieser Verordnung und erstattet dem Europäischen Parlament, dem Rat, dem Europäischen Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen Bericht. Die Kommission bewertet ferner, ob es angemessen ist, Netz- und Informationssysteme, mit denen EU-VS bearbeitet werden, in den Anwendungsbereich dieser Verordnung aufzunehmen, wobei sie andere für diese Systeme geltende Gesetzgebungsakte der Union berücksichtigt. Dem Bericht ist erforderlichenfalls ein Gesetzgebungsvorschlag beizufügen.

Artikel 26

Inkrafttreten

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

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

Geschehen zu …,

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