Rat der
Europäischen Union

**Brüssel, den 31. Oktober 2022**
**(OR. en)**

**14128/22**

**Interinstitutionelles Dossier:**
**2022/0085(COD)**

**CYBER 343**
**TELECOM 428**
**INST 396**
**CSC 472**
**CSCI 157**
**INF 176**
**FIN 1158**
**BUDGET 22**
**DATAPROTECT 294**
**CODEC 1617**

**I/A-PUNKT-VERMERK**

| | |
|---|---|
| Absender: | Generalsekretariat des Rates |
| Empfänger: | Ausschuss der Ständigen Vertreter (2. Teil)/Rat |
| Nr. Vordok.: | 10097/5/22 REV 5 |
| Nr. Komm.dok.: | 7474/22 + ADD 1 |
| Betr.: | Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union<br>– Allgemeine Ausrichtung |

## EINLEITUNG

1. Am 22. März 2022 hat die Kommission den Vorschlag für eine Verordnung zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union angenommen. Der Vorschlag war eine der in der Cybersicherheitsstrategie der EU für die digitale Dekade[1] vorgesehenen Maßnahmen, mit der die gemeinsame Abwehrfähigkeit Europas gegenüber Cyberbedrohungen gestärkt werden soll.

[1] Dok. 14133/20.

In seinen Schlussfolgerungen zu dieser Strategie vom 22. März 2021[2] betonte der Rat, dass Cybersicherheit „für das Funktionieren der öffentlichen Verwaltung und der öffentlichen Institutionen sowohl auf nationaler als auch auf EU-Ebene sowie für unsere Gesellschaft und die Wirtschaft insgesamt von entscheidender Bedeutung“ ist.

2. Der Vorschlag der Kommission, der sich auf Artikel 298 des Vertrags über die Arbeitsweise der Europäischen Union stützt, zielt darauf ab, das Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union durch die Schaffung eines gemeinsamen Rahmens unter gebührender Berücksichtigung der Autonomie der einzelnen Einrichtungen der Union zu verbessern. Mit dem Vorschlag werden insbesondere folgende Ziele verfolgt:

   – Stärkung des Mandats und der Finanzierung des CERT-EU (autonomes interinstitutionelles IT-Notfallteam für die Einrichtungen der Union),

   – Einrichtung einer interinstitutionellen Struktur (Interinstitutioneller Cybersicherheitsbeirat – IICB), in dem Vertreter aller Einrichtungen der Union zusammenkommen, um die ordnungsgemäße Durchführung der Verordnung zu gewährleisten,

   – Einführung der Verpflichtung für die Einrichtungen der Union, (nicht als Verschlusssache eingestufte) Informationen über Sicherheitsvorfälle an das CERT-EU weiterzugeben und erhebliche Bedrohungen, Sicherheitslücken und Sicherheitsvorfälle zu melden, und

   – Förderung der Koordinierung und Zusammenarbeit bei der Reaktion auf erhebliche Sicherheitsvorfälle.

3. Das Europäische Parlament hat Frau Henna Virkkunen (EVP) zur Berichterstatterin des ITRE-Ausschusses ernannt, der für das Thema zuständig ist. Der Berichtsentwurf wurde am 7. Oktober 2022 veröffentlicht.

4. Der Europäische Datenschutzbeauftragte hat seine Stellungnahme am 17. Mai 2022 abgegeben.[3]

---

[2] Dok. 6722/21.
[3] Dok. 9252/22.

5. Im Rat begann die Prüfung des Vorschlags in der Horizontalen Gruppe „Fragen des Cyberraums“ (HWPCI) am 29. März 2022 unter französischem Vorsitz. Der französische Vorsitz arbeitete den ersten Kompromisstext aus, den die HWPCI im Juni 2022 erörterte, und legte dem Rat am 21. Juni 2022 einen Fortschrittsbericht[4] vor.

6. Während des tschechischen Vorsitzes widmete die HWPCI den Beratungen über den Vorschlag und über mehrere aufeinanderfolgende Kompromisstexte acht Sitzungen[5].

7. Am 23. Mai 2022 ersuchte der Vorsitz den Sicherheitsausschuss des Rates (CSC) um eine Stellungnahme zu den Aspekten des Vorschlags, die die Informationssicherheit und insbesondere Verschlusssachen betreffen. Der CSC hat seine Stellungnahme am 19. September 2022 abgegeben.[6] Wie vom CSC vorgeschlagen, wurden EU-Verschlusssachen ausdrücklich vom Anwendungsbereich der Verordnung ausgenommen. Die Bestimmungen über Ausnahmen von Weitergabe- und Meldepflichten in Bezug auf Informationen, die von außerhalb der Einrichtungen der Union stammen, wurden entsprechend geändert.

8. Am 28. Oktober 2022 hat die HWPCI Einvernehmen über den in der Anlage wiedergegebenen Kompromisstext des Vorsitzes erzielt.

---

4 Dok. 9719/22.
5 6. und 20. Juli, 13., 21. und 28. September, 5., 19. und 28. Oktober 2022.
6 Dok. 12603/22 + COR 1.

**WICHTIGSTE FRAGEN**

9. Die Mitgliedstaaten begrüßten den Vorschlag als zeitgerecht und Ergänzung zur künftigen Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union („NIS 2"-Richtlinie) und unterstützten seine allgemeinen Ziele. Die Mitgliedstaaten forderten jedoch weitere Angleichungen an die „NIS 2" sowie mehr Gegenseitigkeit beim Informationsaustausch zwischen den Einrichtungen der Union und den Mitgliedstaaten und verwiesen auf den allzu freiwilligen Charakter einiger der vorgeschlagenen Maßnahmen. Ferner sprachen sich die Mitgliedstaaten dafür aus, die Bezugnahmen auf die Gemeinsame Cyber-Einheit zu streichen, deren Mandat und Zusammensetzung noch nicht festgelegt sind.

10. Auf der Grundlage der Beratungen in der HWPCI wurden die folgenden Punkte als die wichtigsten politischen Fragen ermittelt:

a) **Angleichung an die künftige „NIS 2"-Richtlinie**

Wie von den Mitgliedstaaten gefordert, wurden weitere Angleichungen an die künftige „NIS 2"-Richtlinie vorgenommen, u. a. folgende:

– Eine Reihe von Begriffsbestimmungen (Artikel 3) wurde an diejenigen in der „NIS 2" angeglichen;

– es wurde ein neuer Artikel 7a über freiwillige Peer-Reviews eingefügt, der im Einklang mit der „NIS 2" steht und an die Bedürfnisse der Einrichtungen der Union angepasst ist;

– Meldepflichten in Artikel 20 wurden an diejenigen in der „NIS 2" angeglichen.

b) **Zusammensetzung des Interinstitutionellen Cybersicherheitsbeirats (IICB)** (Artikel 9)

Nach Beratungen über die angemessene Einbeziehung von Vertretern der Mitgliedstaaten in die Arbeit des IICB wurde ein Kompromiss in Form einer Protokollerklärung des Rates gefunden.

c) **Institutionelle Autonomie**

Es wurde ein ausgewogener Ansatz gefunden zwischen dem Willen der Mitgliedstaaten, die Einhaltungsmechanismen zu stärken, und der Notwendigkeit, den Grundsatz der institutionellen Autonomie zu achten, insbesondere in Bezug auf Prüfungen und Disziplinarmaßnahmen (Artikel 11).

Schließlich wurde die Bezugnahme auf einen bestimmten Prozentsatz des IT-Haushalts für Cybersicherheit in Erwägungsgrund 8 gestrichen.

**FAZIT**

11. Der Ausschuss der Ständigen Vertreter wird ersucht,

a) den in der Anlage wiedergegebenen Kompromisstext zu billigen, der anschließend das Mandat für Verhandlungen mit dem Europäischen Parlament bilden wird;

b) den Rat zu ersuchen, den in der Anlage wiedergegebenen Kompromisstext auf seiner Tagung am 18. November 2022 zu billigen und die im Addendum zu diesem Dokument enthaltene Erklärung des Rates in das Protokoll aufzunehmen.

**ANLAGE**

2022/0085 (COD)

Vorschlag für eine

**VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES**

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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

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

(2) Die Cyberbedrohungslandschaft, mit der die [...] 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 und Manipulation der öffentlichen Meinung bis hin zur Schwächung der digitalen Infrastruktur. Das Tempo, in dem die Verursacher ihre Cyberangriffe durchführen, nimmt weiter zu, während ihre Operationen zunehmend ausgefeilt und automatisiert und auf exponierte Angriffsflächen ausgerichtet sind, immer weiter expandieren und rasch Schwachstellen ausnutzen.

(3) Die IT-Umgebungen der [...] 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 Einrichtung [...] der Union beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die anderen [...] Einrichtungen [...] haben können. Darüber hinaus sind die IT-Umgebungen bestimmter [...] Einrichtungen **der Union** mit den IT-Umgebungen der Mitgliedstaaten verbunden, was dazu führt, dass ein Sicherheitsvorfall in einer Einrichtung der Union ein Risiko für die Cybersicherheit der IT-Umgebungen der Mitgliedstaaten darstellt, und umgekehrt. **Außerdem verarbeiten Einrichtungen der Union große Mengen oft sensibler Informationen aus Mitgliedstaaten, sodass sich Sicherheitsvorfälle auch auf Mitgliedstaaten negativ auswirken könnten. Aus diesem Grund ist die Cybersicherheit der Einrichtungen der Union auch für die Mitgliedstaaten von großer Bedeutung. Spezifische Informationen über Sicherheitsvorfälle können auch 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 europäischen Verwaltung ist es daher erforderlich, dass die [...] Einrichtungen [...] der Union **durch die Umsetzung von Cybersicherheitsmaßnahmen, Informationsaustausch und Zusammenarbeit** ein hohes gemeinsames Cybersicherheitsniveau erreichen [...].

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

(6) Um ein hohes gemeinsames Cybersicherheitsniveau zu erreichen, ist es erforderlich, dass [...] jede Einrichtung [...] der Union einen internen Rahmen für Risikomanagement, Governance und Kontrolle im Bereich der Cybersicherheit festlegt, der ein wirksames und umsichtiges Management aller Cybersicherheitsrisiken gewährleistet [...]. **In dem Rahmen sollten Cybersicherheitskonzepte festgelegt werden, einschließlich Verfahren zur Bewertung der Wirksamkeit durchgeführter Cybersicherheitsmaßnahmen. 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. Der Rahmen sollte die Ergebnisse der Risikoanalyse widerspiegeln, unter Berücksichtigung aller relevanten technischen, operativen und organisatorischen Risiken für die Cybersicherheit der betreffenden Einrichtung der Union.**

**(6a) Zur Bewältigung der in diesem Rahmen ermittelten Risiken sollte jede Einrichtung der Union sicherstellen, dass geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergriffen werden. Diese sollten sich auf die in dieser Verordnung festgelegten Bereiche, einschließlich Cybersicherheitsmaßnahmen, erstrecken, um die Cybersicherheit jeder Einrichtung der Union zu stärken.**

**(6b)** **Die im Rahmen ermittelten Anlagen und Risiken sowie die Schlussfolgerungen aus den regelmäßigen Bewertungen des Reifegrades sollten in den von jeder Einrichtung der Union erstellten Cybersicherheitsplan einfließen. Der Cybersicherheitsplan sollte die angenommenen Cybersicherheitsmaßnahmen enthalten, um die Cybersicherheit der betreffenden Einrichtung der Union insgesamt zu erhöhen.**

**(6c)** **Da es sich bei der Gewährleistung der Cybersicherheit um einen kontinuierlichen Prozess handelt, sollten die Eignung und Wirksamkeit aller Maßnahmen im Lichte der sich verändernden Risiken, Anlagen und Reifegrade der Einrichtungen der Union regelmäßig überprüft werden. Der Rahmen sollte regelmäßig und mindestens alle drei Jahre überprüft werden, während der Cybersicherheitsplan mindestens alle zwei Jahre oder nach jeder Reifegradbewertung oder jeder Überprüfung des Rahmens überarbeitet werden sollte.**

**(6d)** **Einrichtungen der Union sollten regelmäßig einschlägige Informationen austauschen, auch in Bezug auf relevante Sicherheitsvorfälle und Cyberbedrohungen, und dabei die Vertraulichkeit und den angemessenen Schutz der von der meldenden Einrichtung der Union bereitgestellten Informationen gewährleisten.**

**(6e)** **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. Die ausgetauschten Informationen sollten von der benannten Kontaktstelle für das EU-CyCLONe bei der Weitergabe einschlägiger Informationen an das EU-CyCLONe als Beitrag zur gemeinsamen Lageerfassung berücksichtigt werden.**

(7) Angesichts der Unterschiede zwischen den [...] Einrichtungen [...] der Union ist bei der Umsetzung Flexibilität erforderlich, da die Lösungen jeweils bedarfsgerecht zugeschnitten sein müssen. Die Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau sollten keine Verpflichtungen umfassen, die einen unmittelbaren Eingriff in die Wahrnehmung der Aufgaben der [...] Einrichtungen [...] der Union darstellen oder deren institutionelle Autonomie beeinträchtigen. Daher sollten diese [...] Einrichtungen **der Union** ihren eigenen Rahmen für das Risikomanagement, die Governance und die Kontrolle im Bereich der Cybersicherheit **sowie Cybersicherheitspläne** festlegen und **Cybersicherheitsmaßnahmen** annehmen. **Bei der Durchführung solcher Maßnahmen sollten bestehende Synergien zwischen Einrichtungen der Union gebührend berücksichtigt werden, mit dem Ziel einer ordnungsgemäßen Verwaltung der Ressourcen und einer Kostenoptimierung. Ferner sollte gebührend darauf geachtet werden, dass sich die Maßnahmen nicht negativ auf den effizienten Informationsaustausch und Betrieb der Einrichtungen der Union mit anderen Einrichtungen der Union und zuständigen nationalen Behörden auswirken.**

(8) Damit keine unverhältnismäßige finanzielle und administrative Belastung für die [...] Einrichtungen [...] der Union entsteht, sollten die Anforderungen an das Cybersicherheitsrisikomanagement in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei ist dem neuesten Stand solcher Maßnahmen Rechnung zu tragen. **Jede** Einrichtung [...] der Union sollte bestrebt sein, einen angemessenen Prozentsatz [...] ihres IT-Haushalts für die Verbesserung [...] ihres Cybersicherheitsniveaus zuzuweisen [...]. **Bei der Bewertungd des Reifegrads sollte auch bewertet werden, ob die Ausgaben für Cybersicherheit der Einrichtung der Union in einem angemessenen Verhältnis zu den Risiken stehen, denen sie ausgesetzt ist.**

(9) Ein hohes gemeinsames Cybersicherheitsniveau setzt voraus, dass die Cybersicherheit der Aufsicht der höchsten Managementebene [...] der jeweiligen Einrichtung [...] der Union unterstellt wird [...]. **Die höchste Managementebene sollte die Durchführung dieser Verordnung überwachen, einschließlich der Festlegung des Rahmens für Risikomanagement, Governance und Kontrolle und der Cybersicherheitspläne, die auch Cybersicherheitsmaßnahmen umfassen.** Die Pflege der Cybersicherheitskultur, d. h. die Cybersicherheit in der täglichen Praxis, ist Bestandteil **des Cybersicherheitsrahmens** in allen [...] Einrichtungen [...] der Union.

(10) **Cybersicherheitsmaßnahmen** sollten Teil **des Cybersicherheitsplans** sein und 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** die einschlägigen Rechtsvorschriften und Strategien der EU, einschließlich der Risikobewertungen und Empfehlungen der NIS-Kooperationsgruppe, wie etwa die koordinierte Risikobewertung der EU und das EU-Instrumentarium für die 5G-Cybersicherheit, gebührend berücksichtigt werden. Darüber hinaus könnte die Zertifizierung relevanter IKT-Produkte, -Dienste und -Prozesse im Rahmen spezifischer EU-Systeme für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, vorgeschrieben werden. **Gegebenenfalls sollte das CERT-EU mit der ENISA zusammenarbeiten.**

(11) Im Mai 2011 beschlossen die Generalsekretäre der Organe und Einrichtungen der Union die Einsetzung eines Vorbereitungsteams für ein Reaktionsteam für IT-Sicherheitsvorfälle für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) unter der Aufsicht eines interinstitutionellen Lenkungsausschusses. Im Juli 2012 bestätigten die Generalsekretäre die praktischen Vorkehrungen und vereinbarten, das CERT-EU als ständige Einrichtung beizubehalten; als Beispiel für eine sichtbare interinstitutionelle Zusammenarbeit auf dem Gebiet der Cybersicherheit sollte es weiterhin zur Verbesserung der allgemeinen Sicherheit der IT-Systeme der Organe, Einrichtungen und sonstigen Stellen der Union beitragen. Im September 2012 wurde das CERT-EU als Taskforce der Europäischen Kommission mit einem interinstitutionellen Mandat eingerichtet. Im Dezember 2017 schlossen die Organe und Einrichtungen der Union eine interinstitutionelle Vereinbarung über die Organisation und die Funktionsweise des CERT-EU[7]. Diese **Verordnung** sollte **ein umfassendes Regelwerk für die Organisation, den Betrieb und die Funktionsweise des CERT-EU bereitstellen. Die Bestimmungen dieser Verordnung haben Vorrang vor den Bestimmungen der im Dezember 2017 geschlossenen Interinstitutionellen Vereinbarung über die Organisation und die Funktionsweise des CERT-EU.**

[...]

**7** ABl. C 12 vom 13.1.2018, S. 1.

(13) Viele Cyberangriffe sind Teil umfassenderer Operationen, die auf Gruppen von [...] Einrichtungen [...] der Union oder Interessengemeinschaften, zu denen auch [...] Einrichtungen [...] der Union gehören, ausgerichtet sind. Um eine proaktive Erkennung von Sicherheitsvorfällen sowie Maßnahmen zu ihrer Bewältigung und Abschwächung zu ermöglichen, sollten die [...] Einrichtungen [...] der Union das CERT-EU über [...] Cyberbedrohungen, [...] Sicherheitslücken**, Beinahe-Vorfälle** und [...] Sicherheitsvorfälle informieren und geeignete technische Einzelheiten übermitteln, die die Erkennung bzw. Abschwächung sowie die Bewältigung ähnlicher Cyberbedrohungen, Sicherheitslücken**, Beinahe-Vorfälle** und Sicherheitsvorfälle in anderen Organen, [...] Einrichtungen [...] der Union ermöglichen. Nach demselben Ansatz, wie er in der Richtlinie [NIS-2-Vorschlag] vorgesehen ist, sollten Einrichtungen **der Union**, die von einem erheblichen Sicherheitsvorfall Kenntnis erhalten, verpflichtet sein, innerhalb von 24 Stunden 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 entsprechende Partner weiterzugeben, um dazu beizutragen, die IT-Umgebungen der Union und die IT-Umgebungen der Partner der Union vor ähnlichen Sicherheitsvorfällen [...] zu schützen.

**(13a)** **Mit dieser Verordnung wird ein mehrstufiger Ansatz für die Meldung von erheblichen Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von erheblichen Sicherheitsvorfällen entgegenwirkt und den Einrichtungen der Union die Möglichkeit gibt, 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. Diesbezüglich sollte diese Verordnung die Meldung von Sicherheitsvorfällen umfassen, die – entsprechend einer von der Einrichtung der Union durchgeführten ersten Bewertung – durch erheblichen materiellen oder immateriellen Schaden schwerwiegende Störungen des Betriebs der Einrichtung der Union oder finanzielle Verluste für die betreffende Einrichtung der Union oder andere natürliche oder juristische Personen verursachen könnten. Bei dieser ersten Bewertung sollten unter anderem die betroffenen Netz- und Informationssysteme – insbesondere ihre Bedeutung für das Funktionieren der Einrichtung der Union –, die Schwere und die technischen Merkmale einer Cyberbedrohung und alle zugrundeliegenden Sicherheitslücken, die ausgenutzt werden, sowie die Erfahrungen der Einrichtung der Union mit ähnlichen Sicherheitsvorfällen berücksichtigt werden. Indikatoren wie das Ausmaß, in dem die Funktionsweise 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.**

**(13b)** **Da die Infrastruktur und die Netze 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 ohne ungebührliche Verzögerung über einen erheblichen Sicherheitsvorfall innerhalb dieser Einrichtung der Union unterrichtet wird. Zu diesem Zweck sollte die betroffene Einrichtung der Union die entsprechende nationale Stelle des CERT-EU, die von dem Mitgliedstaat gemäß der Richtlinie [NIS-2-Vorschlag] benannt wurde, innerhalb derselben Frist unterrichten, innerhalb derer sie dem CERT-EU einen erheblichen Sicherheitsvorfall melden sollte. Das CERT-EU sollte diese nationale Stelle auch unterrichten, wenn es Kenntnis von einem schwerwiegenden Vorfall in dem Mitgliedstaat erhält, es sei denn, die betroffene Einrichtung der Union hat diesen bereits gemeldet.**

(14) Neben den zusätzlichen Aufgaben und der erweiterten Rolle, die für das CERT-EU vorgesehen werden, sollte auch ein Interinstitutioneller Cybersicherheitsbeirat (IICB) eingerichtet werden, der**, um** ein hohes gemeinsames Cybersicherheitsniveau der [...] Einrichtungen [...] der Union **zu** fördern [...], [...] **eine ausschließliche Rolle bei der Überwachung der** Umsetzung dieser Verordnung durch die [...] Einrichtungen [...] der Union **und bei der Beaufsichtigung der** Umsetzung der allgemeinen Prioritäten und Ziele durch das CERT-EU **sowie bei der Festlegung** strategische**r** Leitlinien für das CERT-EU **übernehmen sollte**. In dem IICB sollte **daher** die Vertretung der Organe gewährleistet sein, und dem Beirat sollten über das Netzwerk der Agenturen der Union auch Vertreter von Agenturen und Einrichtungen angehören. **Die Organisation und der Betrieb 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 Führungsebene jedes Mitglieds des IICB es dem IICB ermöglichen würden, strategische Diskussionen zu führen und strategische Leitlinien für das IICB vorzugeben. Darüber hinaus kann das IICB einen Exekutivausschuss einsetzen, der es bei seiner Arbeit unterstützt und ihm einige seiner Aufgaben und Befugnisse überträgt, insbesondere in Bezug auf Aufgaben, die spezifisches Fachwissen seiner Mitglieder erfordern, z. B. die Billigung des Dienstleistungskatalogs und etwaiger späterer Aktualisierungen desselben, Modalitäten 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 und die Amtszeit seiner Mitglieder festlegen.**

(15) Das CERT-EU sollte die Umsetzung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau durch Vorschläge für Leitfäden und Empfehlungen an den IICB oder durch Aufrufe zum Tätigwerden unterstützen. Diese Leitlinien und Empfehlungen sollten vom IICB genehmigt werden. Wenn erforderlich, sollte das CERT-EU Aufrufe zum Tätigwerden herausgeben, in denen dringende Sicherheitsmaßnahmen beschrieben werden, zu deren Ergreifung innerhalb einer vorgegebenen Frist die [...] Einrichtungen [...] der Union dringend aufgefordert werden. **Der IICB kann das CERT-EU anweisen, einen Vorschlag für Leitlinien oder Empfehlungen oder einen Aufruf zum Tätigwerden vorzulegen, zurückzuziehen oder zu ändern.**

(16) Der IICB sollte die Einhaltung dieser Verordnung sowie die Maßnahmen zur Befolgung von Leitlinien und Empfehlungen und der [...] Aufrufe zum Tätigwerden überwachen. Der IICB sollte in technischen Fragen von fachlichen Beratungsgruppen unterstützt werden, deren Zusammensetzung im Ermessen des IICB liegt und die bei Bedarf eng mit dem CERT-EU, den [...] Einrichtungen [...] der Union sowie mit anderen Interessenträgern zusammenarbeiten sollten. [...] **Stellt der IICB fest, dass Einrichtungen der Union diese Verordnung oder auf der Grundlage dieser Verordnung angenommene Leitlinien, Empfehlungen oder Aufrufe zum Tätigwerden nicht wirksam angewandt oder durchgeführt bzw. umgesetzt haben, so kann er unbeschadet der internen Verfahren der betreffenden Einrichtungen der Union Compliance-Maßnahmen treffen. Das System der Compliance-Maßnahmen sollte mit schrittweise zunehmender Strenge angewandt werden, d. h., wenn der IICB die Compliance-Maßnahmen beschließt, sollte er mit einer Verwarnung als der am wenigsten einschneidenden Maßnahme beginnen und erforderlichenfalls den Weg bis zur schwerwiegendsten Maßnahme beschreiten, die darin besteht, eine Benachrichtigung mit der Empfehlung einer vorübergehenden Aussetzung der Datenströme zu der betreffenden Einrichtung der Union zu übermitteln; dies würde in Ausnahmefällen erfolgen, wenn die betreffende Einrichtung der Union ihren Verpflichtungen aus dieser Verordnung langfristig, vorsätzlich und/oder in schwerwiegender Weise nicht nachkommt.**

**(16a)** **Die Verwarnung stellt die am wenigsten strenge Compliance-Maßnahme zur Behebung der festgestellten Mängel der Einrichtung der Union dar und umfasst Empfehlungen zur Änderung ihrer Cybersicherheitsdokumente innerhalb eines festgelegten Zeitrahmens. Die Verwarnung sollte allen Einrichtungen der Union zugänglich sein, sofern sie nicht im Einklang mit dieser Verordnung angemessen eingeschränkt wird.**

**(16b)** **Der IICB kann ferner die Durchführung eines Audits bei einer Einrichtung der Union empfehlen. Die Einrichtung der Union kann zu diesem Zweck ihre interne Auditfunktion nutzen. Der IICB könnte ferner verlangen, dass ein Audit von einem externen Prüfungsdienst – auch von einem gemeinsam vereinbarten privaten Dienstleister – durchgeführt wird.**

**(16c)** **Auf der Grundlage der Ergebnisse eines Audits, das auf Empfehlung oder Ersuchen des IICB durchgeführt wurde, kann der IICB die Einrichtung der Union ferner auffordern, das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken mit den Bestimmungen dieser Verordnung in Einklang zu bringen.**

**(16d)** **Da die Mitgliedstaaten Informationen, die möglicherweise sensibel sind, mit einschlägigen Einrichtungen der Union austauschen, ist die Cybersicherheit des Empfängers dieser Informationen für die Mitgliedstaaten von entscheidender Bedeutung. Daher kann der IICB in Ausnahmefällen bei einer langfristigen, vorsätzlichen, wiederholten und/oder schwerwiegenden Nichterfüllung der Verpflichtung der Einrichtung der Union als letztes Mittel eine Benachrichtigung an alle Mitgliedstaaten und Einrichtungen der Union richten und darin eine vorübergehende Aussetzung der Datenströme zu dieser Einrichtung der Union empfehlen, die so lange gilt, bis der Stand der Cybersicherheit dieser Einrichtung in Ordnung gebracht worden ist. Diese Benachrichtigung sollte allen Mitgliedstaaten und Einrichtungen der Union über geeignete sichere Kommunikationskanäle übermittelt werden.**

**(16e)** **Um die ordnungsgemäße Durchführung dieser Verordnung sicherzustellen, sollte der IICB, wenn er der Auffassung ist, dass ein anhaltender Verstoß gegen diese Verordnung durch eine Einrichtung der Union unmittelbar durch Handlungen oder Unterlassungen eines Mitglieds seines Personals – auch der obersten Führungsebene – verursacht wurde, die betreffende Einrichtung der Union auffordern, im Einklang mit dem Statut und anderen gleichwertigen Vorschriften, die in bestimmten Einrichtungen der Union gelten, angemessene Maßnahmen gegen das betreffende Mitglied des Personals zu ergreifen. Diese Maßnahmen können beispielsweise Disziplinarverfahren und gegebenenfalls – im speziellen Fall von Agenturen der Union – ein Ersuchen an die zuständige Behörde umfassen, die erforderlichen Schritte im Zusammenhang mit der möglichen Amtsenthebung der Person, die für den fortgesetzten Verstoß gegen diese Verordnung verantwortlich sein könnte, zu unternehmen.**

(17) Das CERT-EU sollte den Auftrag haben, zur Sicherheit der IT-Umgebung aller [...] Einrichtungen [...] der Union beizutragen. **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 seiner anderen in dieser Verordnung festgelegten Aufgaben nicht behindert.**

**(17a)** Das CERT-EU sollte für die Zwecke der koordinierten Offenlegung von Sicherheitslücken beim europäischen Schwachstellenregister gemäß Artikel 6 der Richtlinie [NIS-2-Vorschlag] als Äquivalent des benannten Koordinators für die [...] Einrichtungen [...] der Union fungieren **und eine Strategie für die Bewältigung von Sicherheitslücken entwickeln, die die Förderung und Erleichterung der freiwilligen koordinierten Offenlegung von Sicherheitslücken umfasst**.

[...]

(19) Das CERT-EU sollte zudem die Rolle übernehmen, die ihm nach der Richtlinie [NIS-2-Vorschlag] bei der Zusammenarbeit und beim Informationsaustausch mit dem Netzwerk der Computer-Notfallteams (CSIRT-Netzwerk) zukommt. Darüber hinaus sollte das CERT-EU im Einklang mit der Empfehlung (EU) 2017/1584 der Kommission[8] mit den einschlägigen Interessenträgern zusammenarbeiten und sich bezüglich der Reaktionsmaßnahmen mit diesen abstimmen. Um zu einem hohen Cybersicherheitsniveau in der gesamten Union beizutragen, sollte das CERT-EU Informationen zu den einzelnen Sicherheitsvorfällen an die nationalen Partner weiterleiten. Das CERT-EU sollte vorbehaltlich der vorherigen Genehmigung durch den IICB auch mit anderen öffentlichen und privaten Partnern, einschließlich der NATO, zusammenarbeiten.

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

(20) Bei der Unterstützung der operativen Cybersicherheit sollte das CERT-EU das verfügbare Fachwissen der Agentur der Europäischen Union für Cybersicherheit **(ENISA)** im Wege der strukturierten Zusammenarbeit gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[9] nutzen. Für die Festlegung der praktischen Aspekte einer solchen Kooperation und zur Vermeidung von Doppelarbeit sollten gegebenenfalls gesonderte Vereinbarungen zwischen den beiden Stellen getroffen werden. Das CERT-EU sollte mit der **ENISA** bei der Analyse der Bedrohungslage zusammenarbeiten und der Agentur seinen Bericht zur Bedrohungslage regelmäßig übermitteln.

[...]

(22) **Die Tätigkeiten und die Informationsverarbeitung des CERT-EU im Rahmen dieser Verordnung können die Verarbeitung personenbezogener Daten umfassen.** Alle im Rahmen dieser Verordnung verarbeiteten personenbezogenen Daten sollten im Einklang mit den Datenschutzvorschriften, einschließlich der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[10], verarbeitet werden. **Werden gemäß dieser Verordnung personenbezogene Daten an in der Union niedergelassene Empfänger, die keine Einrichtungen der Union sind, übermittelt, so sollte dies im Einklang mit Artikel 9 der Verordnung (EU) 2018/1725 erfolgen.**

---

**9** 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).

**10** 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).

(23) Der Umgang des CERT-EU und der [...] Einrichtungen [...] der Union mit Informationen sollte gemäß **den geltenden Vorschriften für** die Informationssicherheit erfolgen. [...]

**(23a) Für die Zwecke des Informationsaustauschs werden sichtbare Kennzeichnungen verwendet, um anzuzeigen, dass die Weitergabebeschränkungen von den Empfängern der Informationen insbesondere auf der Grundlage von 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, mit dem Informationen über etwaige Beschränkungen hinsichtlich der weiteren Verbreitung von Informationen bereitgestellt werden sollen. Es wird in fast allen IT-Notfallteams (CSIRT) und in einigen Informationsanalyse- und Informationsaustauschzentren eingesetzt.**

(24) **Diese Verordnung und die neuen Aufgaben, die dem CERT-EU übertragen werden, werden keine Auswirkungen auf die Gesamtausgaben im Rahmen des mehrjährigen Finanzrahmens haben.** Da die Dienste und Aufgaben des CERT-EU im Interesse aller [...] Einrichtungen [...] der Union erbracht werden bzw. liegen, sollte **jede** [...] Einrichtung [...] der Union, die über einen Etat für IT-Ausgaben verfüg**t**, einen angemessenen Beitrag für diese Dienste und Aufgaben leisten. Diese Beiträge lassen die Haushaltsautonomie der [...] Einrichtungen [...] der Union unberührt. **Alle Einrichtungen der Union und ihre Verwaltungen sollten die Optimierung ihrer Ressourcen auf dem derzeitigen Niveau sicherstellen und Effizienzgewinne verstärken, auch durch eine Vertiefung der interinstitutionellen Zusammenarbeit im Bereich der Cybersicherheit. Daher sollte ein gemeinsamer Ansatz für die Bündelung der Verwaltungsausgaben Vorrang vor individualisierten Ausgaben von Einrichtungen der Union erhalten.**

(25) Der IICB sollte die Durchführung dieser Verordnung mit Unterstützung des CERT-EU überprüfen und bewerten und der Kommission über seine Feststellungen Bericht erstatten. Die Kommission sollte dem Europäischen Parlament, dem Rat, dem Europäischen Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen regelmäßig Bericht erstatten. **Darüber hinaus wird der Europäische Rechnungshof ersucht, die Funktionsweise des CERT-EU regelmäßig zu bewerten —**

HABEN FOLGENDE VERORDNUNG ERLASSEN:

## Kapitel I
## ALLGEMEINE BESTIMMUNGEN

*Artikel 1*

***Gegenstand***

(1) Mit dieser Verordnung **werden Maßnahmen** festgelegt**, mit denen ein hohes gemeinsames Cybersicherheitsniveau in Einrichtungen der Union erreicht werden soll.**

**(2) Hierzu legt diese Verordnung Folgendes fest:**

c) Verpflichtungen für **jede Einrichtung** der Union zur Schaffung eines [...] Rahmens für das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken,

d) Cybersicherheitsrisikomanagements-**, Berichterstattungs- und Informationsaustauschpflichten** für die [...] Einrichtungen [...] der Union,

e) Vorschriften über die Organisation**, das Funktionieren** und **die** Arbeitsweise des **autonomen interinstitutionellen IT-Notfallteams** für die [...] Einrichtungen [...] der Union (CERT-EU) und über die Organisation**, das Funktionieren** und **die** Arbeitsweise des Interinstitutionellen Cybersicherheitsbeirats (IICB)**,**

f) **Vorschriften für die Überwachung der Durchführung dieser Verordnung.**

*Artikel 2*

***Anwendungsbereich***

(1) Diese Verordnung gilt für [...] alle [...] Einrichtungen [...] der Union und **das** CERT-EU und **den** IICB.

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

**(3) Mit Ausnahme von Artikel 12 Absatz 7 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 oder den Vertrag zur Gründung der Europäischen Atomgemeinschaft oder auf deren Grundlage geschaffen wurden;

2. „Netz- und Informationssystem“ ein Netz- und Informationssystem im Sinne des Artikels 4 Nummer 1 der Richtlinie [NIS-2-Vorschlag];

3. „Sicherheit von Netz- und Informationssystemen“ die Sicherheit von Netz- und Informationssystemen im Sinne des Artikels 4 Nummer 2 der Richtlinie [NIS-2-Vorschlag];

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

5. „höchste Managementebene“ eine Führungskraft, ein Management-, Koordinierungs- oder Aufsichtsgremium auf der höchsten Verwaltungsebene **mit Entscheidungsfähigkeit**, unter Berücksichtigung der Governance-Regelungen für die höchsten Ebenen in **jeder Einrichtung** der Union;

**5a. „Beinahe-Vorfall“ einen Beinahe-Vorfall im Sinne des Artikels 4 Nummer 4a der Richtlinie [NIS-2-Vorschlag];**

6. „Sicherheitsvorfall“ einen Sicherheitsvorfall im Sinne des Artikels 4 Nummer 5 der Richtlinie [NIS-2-Vorschlag];

[...]

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

9. „Bewältigung von Sicherheitsvorfällen“ die Bewältigung von Sicherheitsvorfällen im Sinne des Artikels 4 Nummer 6 der Richtlinie [NIS-2-Vorschlag];

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

[...]

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

[...]

14. „**Risiko**“ **ein Risiko im Sinne des Artikels 4 Nummer 7b der Richtlinie [NIS-2-Vorschlag].**

***Artikel 3a***

***Verarbeitung personenbezogener Daten***

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

**(2) Personenbezogene Daten werden von dem CERT-EU, dem IICB und Einrichtungen der Union nur im erforderlichen Umfang und zum alleinigen Zweck der Erfüllung ihrer jeweiligen Verpflichtungen aus der vorliegenden Verordnung verarbeitet und ausgetauscht.**

## Kapitel II

## MAßNAHMEN FÜR EIN HOHES GEMEINSAMES CYBERSICHERHEITSNIVEAU

*Artikel 4*

***Rahmen für Risikomanagement, Governance und Kontrolle***

(1) Alle [...] Einrichtungen [...] der Union legen in Unterstützung ihres jeweiligen Auftrags [...] ihren eigenen [...] Rahmen für Risikomanagement, Governance und Kontrolle im Bereich der Cybersicherheit (im Folgenden „Rahmen“) fest. **Dieser Rahmen wird von** der jeweiligen höchsten Managementebene **beaufsichtigt**, um ein wirksames und umsichtiges Management aller Cybersicherheitsrisiken zu gewährleisten. Der Rahmen ist bis spätestens ... [15 Monate nach dem Inkrafttreten dieser Verordnung] einzuführen.

(2) Der Rahmen deckt jeweils die gesamte **nichtvertrauliche** IKT-Umgebung der betreffenden **Einrichtung der Union** ab, insbesondere die IKT-Umgebung in den Räumlichkeiten der betreffenden Einrichtung, **das operative Technologienetz,** in Cloud-Computing-Umgebungen ausgelagerte oder von Dritten gehostete Anlagen und Dienste, mobile Geräte, Firmennetze, nicht mit dem Internet verbundene Geschäftsnetze und alle mit der IKT-Umgebung verbundenen Geräte. Der Rahmen **beruht auf einem gefahrenübergreifenden Ansatz und einer Bewertung des Reifegrads gemäß Artikel 6** und deckt **alle relevanten technischen, operativen und organisatorischen** Risiken ab, die Auswirkungen auf die Cybersicherheit [...] der betreffenden Einrichtung der Union haben könnten.

**(2a) In dem Rahmen werden Cybersicherheitskonzepte, einschließlich Ziele und Prioritäten für die Sicherheit von Netz- und Informationssystemen, sowie Konzepte und Verfahren zur Bewertung der Wirksamkeit durchgeführter Maßnahmen zum Cybersicherheitsrisikomanagement festgelegt sowie die Aufgaben und Zuständigkeiten der Mitarbeiter definiert.**

**(2b) Der Rahmen wird regelmäßig, mindestens jedoch alle drei Jahre, unter Berücksichtigung der sich verändernden Risiken, der Anlagen und des Reifegrads der Einrichtung der Union überprüft.**

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

**(3a) Gegebenenfalls und unbeschadet ihrer Zuständigkeit für die Durchführung dieser Verordnung kann die höchste Managementebene jeder Einrichtung der Union spezifische Verpflichtungen aus dieser Verordnung auf andere höhere Führungskräfte der betreffenden Einrichtung übertragen. Unabhängig von einer möglichen Übertragung ihrer spezifischen Verpflichtungen kann die höchste Managementebene für die Nichteinhaltung der Verpflichtungen aus dieser Verordnung durch die Einrichtungen haftbar gemacht werden.**

**(3b) Die höchste Managementebene jeder Einrichtung der Union stellt sicher, dass die Einrichtungen der Union den Cybersicherheitsplan, der Maßnahmen zum Cybersicherheitsrisikomanagement umfasst, entsprechend seiner Risikoanalyse billigen, damit der Rahmen im Einklang mit dieser Verordnung umgesetzt wird.**

(5) Alle [...] Einrichtungen [...] der Union ernennen einen lokalen Cybersicherheitsbeauftragten oder eine Kontaktperson mit gleichwertiger Funktion, der oder 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 im Zusammenhang mit der Durchführung dieser Verordnung auf der Grundlage einer Leistungsvereinbarung zwischen dieser Einrichtung der Union und dem CERT-EU auf das CERT-EU übertragen. Der IICB entscheidet unter Berücksichtigung der personellen und finanziellen Ressourcen der betreffenden Einrichtung der Union, ob die Bereitstellung dieses Dienstes Teil der Basisdienste des CERT-EU ist. Die ernannten lokalen Cybersicherheitsbeauftragten und etwaige spätere Änderungen an den Ernennungen werden dem CERT-EU von den einzelnen Einrichtungen der Union unverzüglich mitgeteilt. Das CERT-EU führt die regelmäßig aktualisierte Liste der ernannten lokalen Cybersicherheitsbeauftragten.**

**(6) Die höheren Führungskräfte im Sinne des Artikels 29 Absatz 2 des Statuts der Beamten[11] oder andere gleichrangige Beamte jeder Einrichtung der Union absolvieren regelmäßig spezifische Schulungen, um ausreichende Kenntnisse und Fähigkeiten zu erwerben, damit sie Cybersicherheitsrisiken und -managementverfahren und deren Auswirkungen auf den Betrieb der Organisation erfassen und bewerten können.**

---

**11** **Verordnung 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, ABl. L 56 vom 4.3.1968.**

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

*Artikel 5*

***Maßnahmen zum Cybersicherheitsrisikomanagement***

(1) **Alle Einrichtungen der Union stellen unter der Aufsicht der höchsten Managementebene sicher, dass geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergriffen werden, um die Risiken, die in dem in Artikel 4 Absatz 1 genannten Rahmen ermittelt werden, zu bewältigen und die Auswirkungen von Sicherheitsvorfällen zu verhindern bzw. zu minimieren. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Durchführungskosten bei den Netz- und Informationssystemen ein Sicherheitsniveau gewährleisten, das angesichts der bestehenden Risiken angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, ihre Größe und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schweregrad, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.**

**(3) Im Einklang mit den Leitlinien und Empfehlungen des IICB berücksichtigen die Einrichtungen der Union bei der Durchführung der Maßnahmen zum Cybersicherheitsrisikomanagement in ihren Cybersicherheitsplänen zumindest die folgenden besonderen Bereiche:**

**a) Cybersicherheitspolitik in Bezug auf die Festlegung der Instrumente und Maßnahmen, die zur Erreichung der in Artikel 4 und in Artikel 5 Absatz 4 genannten Ziele und Prioritäten erforderlich sind,**

**b) Risikoanalyse und Sicherheitskonzepte für Informationssysteme,**

**c) Organisation der Cybersicherheit, einschließlich Festlegung der Aufgaben und Zuständigkeiten,**

**d) Verwaltung der Anlagen, einschließlich IT-Bestandsverzeichnis und IT-Netzkartografie,**

**e) Sicherheit des Personals und Zugangskontrolle,**

**f) Betriebssicherheit,**

**g) Kommunikationssicherheit,**

**h) Beschaffung, Entwicklung und Wartung von Systemen, einschließlich Bewältigung und Offenlegung von Sicherheitslücken,**

**i) Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte im Zusammenhang mit den Beziehungen zwischen den einzelnen Einrichtungen der Union und ihren direkten Anbietern oder Diensteanbietern. Die Einrichtungen der Union berücksichtigen die spezifischen Sicherheitslücken der einzelnen direkten Anbieter und Diensteanbieter und die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse,**

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

**k) Betriebskontinuitätsmanagement, z. B. Datensicherungsmanagement, Wiederherstellung nach Katastrophen und Krisenmanagement, und**

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

**(4) Im Einklang mit den Leitlinien und Empfehlungen des IICB berücksichtigen die Einrichtungen der Union bei der Durchführung der Maßnahmen zum Cybersicherheitsrisikomanagement in ihren Cybersicherheitsplänen zumindest die folgenden besonderen Maßnahmen zum Cybersicherheitsrisikomanagement:**

**a) Ziele und Prioritäten hinsichtlich der Nutzung von Cloud-Computing-Diensten im Sinne des Artikels 4 Nummer 19 der Richtlinie [NIS-2-Vorschlag] und technischer Vorkehrungen zur Ermöglichung der Telearbeit;**

**b) konkrete Schritte für die künftige Anwendung von Zero-Trust-Grundsätzen, einschließlich eines Sicherheitsmodells, und eine koordinierte Cybersicherheits- und Systemmanagementstrategie, die auf der Anerkennung beruhen, dass sowohl innerhalb als auch außerhalb der herkömmlichen Netzgrenzen Bedrohungen bestehen;**

**c) Einführung der Multifaktor-Authentifizierung als Norm in allen Netz- und Informationssystemen;**

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

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

**i) die Beseitigung vertraglicher Hindernisse, die die Informationsweitergabe der IT-Dienstleister über Sicherheitsvorfälle, Sicherheitslücken und Cyberbedrohungen mit dem CERT-EU einschränken;**

**ii) die vertragliche Pflicht zur Meldung von Sicherheitsvorfällen, Sicherheitslücken und Cyberbedrohungen sowie zur angemessenen Bewältigung und Überwachung von Sicherheitsvorfällen;**

**f) Einsatz von Kryptografie und Verschlüsselung, insbesondere End-zu-End-Verschlüsselung;**

**g) gesicherte Kommunikationssysteme innerhalb der Organisation.**

*Artikel 6*

***Bewertung des Reifegrads***

(1) Alle [...] Einrichtungen [...] der Union führen **– gegebenenfalls mit Unterstützung eines spezialisierten Dritten –** mindestens alle drei Jahre eine Bewertung des **Reifegrads** durch, bei der alle in Artikel 4 genannten Elemente ihrer IT-Umgebung einbezogen und die gemäß Artikel 13 angenommenen einschlägigen Leitlinien und Empfehlungen berücksichtigt werden.

**(2) Der IICB nimmt auf Empfehlung des CERT-EU und nach Konsultation der Agentur der Europäischen Union für Cybersicherheit (ENISA) innerhalb von vier Monaten nach Inkrafttreten dieser Verordnung methodische Leitlinien für die Durchführung der Bewertung des Reifegrads an.**

**(3) Nach Abschluss der Bewertung des Reifegrads übermittelt die Einrichtung der Union diese dem IICB. Die erste Bewertung des Reifegrads wird spätestens [12 Monate nach Inkrafttreten dieser Verordnung] durchgeführt.**

*Artikel 7*

***Cybersicherheitspläne***

**(1)** Auf der Grundlage der Schlussfolgerungen aus der Bewertung des Reifegrads und unter Berücksichtigung der gemäß Artikel 4 ermittelten Anlagen und Risiken billigt die höchste Managementebene [...] jeder Einrichtung [...] der Union [...] nach der Festlegung des Rahmens**, der Annahme** der **Maßnahmen zum Cybersicherheitsrisikenmanagement und der Durchführung der Bewertung des Reifegrads unverzüglich, spätestens jedoch 21 Monate nach dem Inkrafttreten dieser Verordnung,** einen Cybersicherheitsplan. Der **Cybersicherheitsplan** zielt darauf ab, die Cybersicherheit [...] der betreffenden Einrichtung [...] der Union insgesamt zu erhöhen und trägt somit zur [...] Verbesserung eines hohen gemeinsamen Cybersicherheitsniveaus aller [...] Einrichtungen [...] der Union bei. **Der Cybersicherheitsplan enthält** mindestens die **Maßnahmen zum Cybersicherheitsrisikenmanagement gemäß Artikel 5**. Der **Cybersicherheitsplan** wird mindestens alle **zwei** Jahre **oder** im Anschluss an **jede** gemäß Artikel 6 **durchgeführte Bewertung** des Reifegrads **oder jede Überprüfung des Rahmens gemäß Artikel 4** überarbeitet.

**(2)**

**(3)** Der Cybersicherheitsplan trägt allen einschlägigen Leitlinien und Empfehlungen des CERT-EU **gemäß Artikel 13** Rechnung.

**(4)** **Nach Fertigstellung des Cybersicherheitsplans übermittelt die Einrichtung der Union diesen dem IICB.**

*Artikel 7a*

***Peer-Review***

**(1) Der IICB legt spätestens bis zum ... [24 Monate nach Inkrafttreten dieser Verordnung] auf Empfehlung des CERT-EU und nach Konsultation der ENISA unter Verwendung der Methodik für Peer-Reviews und der Methodik für die Eigenbewertung gemäß Artikel 16 der Richtlinie [NIS 2-Vorschlag], die erforderlichenfalls an die Erfordernisse der Einrichtungen der Union angepasst werden, die Methodik und die organisatorischen Aspekte einer Peer-Review fest, und zwar im Hinblick darauf, aus gemeinsamen Erfahrungen zu lernen, das gegenseitige Vertrauen zu erhöhen, ein hohes gemeinsames Cybersicherheitsniveau zu erreichen und die für die Durchführung dieser Verordnung erforderlichen Kapazitäten und Konzepte der Einrichtungen der Union im Bereich der Cybersicherheit zu verbessern. Die Teilnahme an den Peer-Reviews ist freiwillig. Vertreter der Mitgliedstaaten können als Beobachter an der Peer-Review teilnehmen. Die Peer-Reviews werden von Sachverständigen für Cybersicherheit durchgeführt, die von mindestens zwei anderen Einrichtungen der Union als den überprüften Einrichtungen der Union benannt wurden, und erstrecken sich auf mindestens einen der folgenden Aspekte:**

**i) den Stand der Umsetzung der Maßnahmen zum Cybersicherheitsrisikomanagement und der Meldepflichten gemäß den Artikeln 5 und 20;**

**ii) das Niveau der Kapazitäten, einschließlich der verfügbaren finanziellen, technischen und personellen Ressourcen;**

**iii) den Stand der Umsetzung des in Artikel 19 genannten Rahmens für den Informationsaustausch;**

**iv) spezifische sektorübergreifende Fragen.**

**(2) Einrichtungen der Union können spezifische in Absatz 1 Ziffer iv genannte Fragen herausstellen, die zu überprüfen sind. Der Umfang der Peer-Review, einschließlich der herausgestellten Fragen, wird den teilnehmenden Einrichtungen der Union vor Beginn der Peer-Review mitgeteilt.**

**(3) Vor Beginn der Peer-Review können Einrichtungen der Union eine Eigenbewertung der überprüften Aspekte durchführen und diese Eigenbewertung den benannten Sachverständigen zur Verfügung stellen.**

**(4) Die Peer-Reviews müssen physische oder virtuelle Besuche am Standort und einen Austausch außerhalb des Standorts umfassen. In Anbetracht des Grundsatzes der guten Zusammenarbeit stellen die der Peer-Review unterzogenen Einrichtungen der Union den benannten Sachverständigen die für die Bewertung erforderlichen Informationen zur Verfügung, vorbehaltlich der Rechtsvorschriften der Mitgliedstaaten oder der Union über den Schutz sensibler oder als Verschlusssachen eingestufter Informationen. Sämtliche durch das Peer-Review-Verfahren erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die an der Peer-Review beteiligten Sachverständigen geben keine sensiblen oder als Verschlusssachen eingestuften Informationen, die im Laufe der Peer-Review erlangt wurden, an Dritte weiter.**

**(5) Nach einer Peer-Review in Einrichtungen der Union dürfen in den zwei Jahren nach Abschluss der Peer-Review in diesen Einrichtungen der Union keine weiteren Peer-Reviews zu denselben Aspekten durchgeführt werden, es sei denn, die Einrichtungen der Union haben etwas anderes beantragt oder auf Vorschlag des IICB vereinbart.**

**(6) Die Einrichtungen der Union stellen sicher, dass jegliches Risiko eines Interessenkonflikts im Zusammenhang mit den benannten Sachverständigen den anderen Einrichtungen der Union und dem IICB vor Beginn der Peer-Review offengelegt wird. Die der Peer-Review unterzogenen Einrichtungen der Union können Einwände gegen die Benennung bestimmter Sachverständiger erheben, indem sie den benennenden Einrichtungen der Union eine hinreichende Begründung übermitteln.**

**(7)** **Die an Peer-Reviews beteiligten Sachverständigen erstellen Berichte über die Ergebnisse und Schlussfolgerungen der Peer-Reviews. Die Einrichtungen der Union können Bemerkungen zu dem sie jeweils betreffenden Berichtsentwurf übermitteln, die dem Bericht beigefügt werden. Die Berichte enthalten Empfehlungen für Verbesserungen in Bezug auf die von der Peer-Review abgedeckten Aspekte. Die Berichte werden gegebenenfalls dem IICB und dem CSIRT-Netzwerk vorgelegt. Die der Peer-Review unterzogenen Einrichtungen der Union können beschließen, dass der sie betreffende Bericht oder eine redigierte Fassung davon veröffentlicht wird.**

*Artikel 8*

***Durchführung***

**[...]**

**(2)** Gemäß Artikel 13 erstellte Leitlinien und Empfehlungen unterstützen die Durchführung der Bestimmungen dieses Kapitels.

**(3)** **Auf Verlangen des IICB erstatten die Einrichtungen der Union Bericht über spezifische Aspekte dieses Kapitels.**

## Kapitel III

## INTERINSTITUTIONELLER CYBERSICHERHEITSBEIRAT

*Artikel 9*

***Interinstitutioneller Cybersicherheitsbeirat***

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

(2) Der IICB ist zuständig für

a) die Überwachung der Durchführung dieser Verordnung durch die **Einrichtungen [...] der Union**;

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) Europäische Kommission;**

**v) Gerichtshof der Europäischen Union;**

**vi) Europäische Zentralbank;**

**vii) Europäischer Rechnungshof;**

**viii) Europäischer Auswärtiger Dienst;**

**ix) Europäischer Wirtschafts- und Sozialausschuss;**

**x) Europäischer Ausschuss der Regionen;**

**xi) Europäische Investitionsbank;**

**xii) Europäisches Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit; und**

**xiii) Agentur der Europäischen Union für Cybersicherheit;**

**b)** [...] drei Vertreter, die vom Netz der Agenturen der Union (EUAN) auf Vorschlag seines IKT-Beratungsausschusses benannt werden, um die Interessen der Agenturen und Einrichtungen zu vertreten, die ihre eigene IT-Umgebung betreiben [...]. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

**(3a)** Jedes Mitglied kann einen Stellvertreter haben. Der Vorsitzende kann weitere Vertreter der vorstehend genannten **Einrichtungen** [...] oder anderer **Einrichtungen** der Union zur Teilnahme an IICB-Sitzungen einladen, die kein Stimmrecht haben.

(4) Der IICB gibt sich eine Geschäftsordnung.

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

(6) Der IICB tritt auf Initiative seines Vorsitzes, **und/oder** auf Ersuchen des CERT-EU **und/**oder auf Antrag eines seiner Mitglieder **mindestens drei Mal jährlich** zusammen.

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

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

(9) Der Leiter des CERT-EU, **der Vorsitzende der NIS-Kooperationsgruppe, der Vorsitzende des EU-CyCLONe und der Vorsitzende des CSIRTs-Netzes** oder [...] **ihre** Stellvertreter [...] **können als Beobachter** an den IICB-Sitzungen teilnehmen, sofern der IICB nichts anderes beschließt.

(10) Die Sekretariatsgeschäfte des IICB werden von der **ENISA** [...] wahrgenommen; **für die Sekretariatsgeschäfte besteht Rechenschaftspflicht gegenüber dem Vorsitzenden des IICB.**

(11) Die vom EUAN auf Vorschlag des IKT-Beratungsausschusses benannten Vertreter und Vertreterinnen leiten die Beschlüsse des IICB an die **Mitglieder des EUAN** [...] weiter. Alle Agenturen und Stellen der Union haben das Recht, die 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 ihm einige seiner Aufgaben und Befugnisse übertragen, **insbesondere die in Artikel 10 Buchstaben c und e genannten Aufgaben und Befugnisse.** Der IICB legt die Geschäftsordnung sowie die Aufgaben und Befugnisse des Exekutivausschusses und die Amtszeit seiner Mitglieder fest.

(14) **Der IICB legt dem Rat alle zwölf Monate 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 seinen entsprechenden nationalen Stellen in jedem Mitgliedstaat dargelegt wird. Dieser Bericht ist ein Beitrag zum Zweijahresbericht über den Stand der Cybersicherheit in der Union im selben Zeitraum gemäß Artikel 15 der Richtlinie [NIS 2-Vorschlag].**

*Artikel 10*

*Aufgaben des IICB*

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

**a)** [...] **wirksame Überwachung und Beaufsichtigung der Anwendung** dieser Verordnung [...] **und Unterstützung der Einrichtungen der Union bei der Stärkung ihrer Cybersicherheit**; **zu diesem Zweck kann der IICB vom CERT-EU und von Einrichtungen der Union Ad-hoc-Berichte anfordern,**

**aa**) **im Anschluss an eine Strategiediskussion Annahme einer mehrjährigen Strategie zur Erhöhung des Cybersicherheitsniveaus in den Einrichtungen der Union und regelmäßige Bewertung, mindestens jedoch alle fünf Jahre, und erforderlichenfalls Änderung der Strategie,**

b) Genehmigung, auf der Grundlage eines [...] von der Leitung des CERT-EU **vorgelegten Vorschlags**, des jährlichen Arbeitsprogramms des CERT-EU und Überwachung seiner Umsetzung,

c) Genehmigung, auf der Grundlage eines Vorschlags der Leitung des CERT-EU, des Leistungskatalogs des CERT-EU **und etwaiger späterer Änderungen des Leistungskatalogs**,

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

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

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

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

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

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

j) **Annahme von Leitlinien und Empfehlungen auf der Grundlage eines Vorschlags des CERT-EU gemäß Artikel 13 und Anweisung des CERT-EU, einen Vorschlag für Leitlinien oder Empfehlungen oder einen Aufruf zum Tätigwerden vorzulegen, zurückzuziehen oder zu ändern,**

**k) Erhalt und Bewertung der von den Einrichtungen der Union im Rahmen dieser Verordnung vorgelegten Unterlagen und Berichte,**

**l) Unterstützung der Einsetzung einer informellen Gruppe, in der die lokalen Cybersicherheitsbeauftragten aller Einrichtungen zusammenkommen, und dadurch Erleichterung des Austauschs von bewährten Verfahren und Informationen im Zusammenhang mit der Durchführung dieser Verordnung,**

**m) Ausarbeitung eines Plans für das Cyberkrisenmanagement, um das koordinierte Management schwerwiegender Sicherheitsvorfälle auf operativer Ebene, die Einrichtungen der Union betreffen, zu unterstützen und zum regelmäßigen Austausch relevanter Informationen, insbesondere über die Auswirkungen und die Schwere schwerwiegender Sicherheitsvorfälle sowie über Möglichkeiten zur Abhilfe, beizutragen.**

*Artikel 11*

*Einhaltung*

**(1)** Der IICB überwacht **gemäß Artikel 9 Absatz 2 und Artikel 10 wirksam** die Durchführung dieser Verordnung und die Umsetzung der angenommenen Leitlinien, Empfehlungen und Aufrufe zum Tätigwerden durch die **Einrichtungen** [...] der Union. **Zu diesem Zweck kann der IICB Informationen oder Unterlagen anfordern, die erforderlich sind, um die ordnungsgemäße Anwendung der Bestimmungen der Verordnung durch die Einrichtungen der Union zu bewerten. Für die Zwecke der Annahme von Compliance-Maßnahmen nach diesem Artikel hat die betroffene Einrichtung der Union kein Stimmrecht.**

**(2)** Stellt der IICB fest, dass **Einrichtungen** [...] der Union diese Verordnung oder auf der Grundlage dieser Verordnung angenommene Leitlinien, Empfehlungen oder Aufrufe zum Tätigwerden nicht wirksam angewandt oder durchgeführt bzw. umgesetzt haben, so kann er – unbeschadet der internen Verfahren der betreffenden **Einrichtungen** [...] der Union **und nachdem er der betroffenen Einrichtung oder Person Gelegenheit gegeben hat, ihren Standpunkt darzulegen –**

a) eine Verwarnung aussprechen, **damit festgestellte Mängel innerhalb eines bestimmten Zeitrahmens behoben werden, einschließlich Empfehlungen zur Änderung von Cybersicherheitsdokumenten, die von den Einrichtungen der Union auf der Grundlage dieser Verordnung angenommen wurden;** sofern angesichts eines zwingenden Cybersicherheitsrisikos notwendig wird der Empfängerkreis der Verwarnung in geeigneter Weise eingeschränkt,

**aa) eine mit Gründen versehene Mitteilung an eine Einrichtung der Union richten, falls die in der zuvor ausgesprochenen Verwarnung festgestellten Mängel innerhalb eines bestimmten Zeitrahmens nicht ausreichend behoben wurden, und diese Stellungnahme dem Rat, dem Europäischen Parlament und der Kommission förmlich übermitteln;**

b) **insbesondere:** [...]

**i) die Durchführung eines Audits bei einer Einrichtung der Union empfehlen;**

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

**c) die Einrichtung der Union auffordern, das Management, die Governance und die Kontrolle von Cybersicherheitsrisiken mit den Bestimmungen dieser Verordnung in Einklang zu bringen, und zwar gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums;**

**d) eine Empfehlung an alle Mitgliedstaaten und Einrichtungen der Union für eine vorübergehende Aussetzung der Datenströme zu der betreffenden Einrichtung der Union abgeben.**

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

**(4) Ist der IICB der Auffassung, dass ein dauerhafter Verstoß einer Einrichtung der Union gegen die Bestimmungen dieser Verordnung vorliegt, der unmittelbar auf Handlungen oder Unterlassungen eines Beamten oder sonstigen Bediensteten der Union, auch auf der höchsten Führungsebene, zurückzuführen ist, so fordert der IIZB die betreffende Einrichtung auf, die geeigneten Maßnahmen, einschließlich disziplinarischer Art, zu ergreifen, insbesondere im Einklang mit den Bestimmungen des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union. Zu diesem Zweck übermittelt der IICB der betreffenden Einrichtung die erforderlichen Informationen.**

## KAPITEL IV
## CERT-EU

*Artikel 12*

***Auftrag und Aufgaben des CERT-EU***

(1) Der Auftrag des CERT-EU [...] besteht darin, zur Sicherheit der nichtvertraulichen IT-Umgebung aller [...] **Einrichtungen** der Union beizutragen, indem es diese in Cybersicherheitsangelegenheiten berät, bei der Prävention, Erkennung, Abschwächung und Bewältigung von Sicherheitsvorfällen unterstützt und als zentrale Stelle für den Austausch von Informationen zur Cybersicherheit und die Koordinierung der Reaktion auf Sicherheitsvorfälle fungiert.

**(1a) Das CERT-EU erhebt, verwaltet und analysiert Informationen über Bedrohungen, Sicherheitslücken und Sicherheitsvorfälle betreffend nicht für Verschlusssachen genutzte IKT-Infrastrukturen und tauscht diese Informationen mit den Einrichtungen der Union aus. Es koordiniert die Reaktionen auf Vorfälle auf interinstitutioneller Ebene und auf Ebene der Einrichtungen der Union, einschließlich durch die Bereitstellung oder Koordinierung der Bereitstellung spezifischer operativer Unterstützung.**

(2) Das CERT-EU nimmt folgende Aufgaben für die **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 13 Absatz 1 aufgeführten **Bestimmungen** [...] 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 16 und 17 genannten Dienste,

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

e) **auf der Grundlage der Informationen gemäß Absatz 1a** [...] Beitrag zur Erfassung der Cyberlage in der EU **in enger Zusammenarbeit mit der ENISA**. **Derartige Informationen werden an den IICB sowie das CSIRTs-Netz und das EU-INTCEN weitergegeben;**

**f) Handeln als Äquivalent des benannten Koordinators für die Einrichtungen der Union gemäß Artikel 6 der Richtlinie [NIS 2-Vorschlag].**

[...]

[...]

[...]

[...]

[...]

(4) Das CERT-EU kooperiert **im Rahmen seiner Zuständigkeiten** 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 des Europäischen Parlaments und des Rates.

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

a) andere als die in Absatz 2 genannten Dienste, die die Cybersicherheit der IT-Umgebung von **Einrichtungen** [...] der Union unterstützen, auf der Grundlage von Leistungsvereinbarungen und vorbehaltlich verfügbarer Ressourcen,

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

c) Dienste, die die Sicherheit der jeweiligen IT-Umgebung unterstützen, für andere Organisationen als die **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 Genehmigung des IICB.

(6) Das CERT-EU kann Cybersicherheitsübungen organisieren **oder 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.

(7) Das CERT-EU kann **Einrichtungen** [...] der Union in Bezug auf Sicherheitsvorfälle in nicht frei zugänglichen IT-Umgebungen unterstützen, wenn es von den betreffenden **Einrichtungen der Union gemäß ihren jeweiligen Verfahren** ausdrücklich dazu aufgefordert wird. **In diesem Fall finden die Bestimmungen der Artikel 19 bis 21 dieser Verordnung keine Anwendung. Die Unterstützung durch das CERT-EU gemäß diesem Absatz lässt die anzuwendenden Rechtsvorschriften der Mitgliedstaaten oder der Union über den Schutz von sensiblen oder als Verschlusssachen eingestuften Informationen unberührt.**

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

**(9) Das CERT-EU kann mit Zustimmung der betreffenden Einrichtung der Union deren Netzverkehr überwachen.**

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

**(11) Das CERT-EU unterstützt die betroffenen Einrichtungen der Union in Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten bei der Bewältigung von Sicherheitsvorfällen, die zu Verletzungen des Schutzes personenbezogener Daten führen.**

*Artikel 13*

***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 Einrichtungen [...] der Union aufgefordert werden. Die betreffende Einrichtung der Union unterrichtet das CERT-EU unverzüglich nach Eingang der Aufforderung zum Tätigwerden darüber, wie diese Maßnahmen angewandt wurden;

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 einzelne **Einrichtungen** [...] der Union gerichtet sind.

(2) Die Leitlinien und Empfehlungen können Folgendes umfassen:

a) Modalitäten für das Cybersicherheitsrisikomanagement und die **Maßnahmen zum Cybersicherheitsrisikomanagement** [...] oder diesbezügliche Verbesserungen;

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

c) gegebenenfalls den Einsatz gemeinsamer Technologie, Architektur und dazugehöriger bewährter Verfahren mit dem Ziel, Interoperabilität und gemeinsame Normen **einschließlich eines koordinierten Ansatzes für die Sicherheit der Lieferkette** [...] zu erreichen.

[...]

[...]

*Artikel 14*

***Der Leiter des CERT-EU***

**(1) Die Kommission ernennt nach Billigung von zwei Dritteln der Mitglieder des IICB den Leiter des CERT-EU. Der IICB wird in allen Phasen des Verfahrens vor der Ernennung des Leiters des CERT-EU konsultiert, insbesondere bei der Ausarbeitung von Stellenausschreibungen, der Prüfung von Bewerbungen und der Ernennung von Auswahlausschüssen im Zusammenhang mit diesem Posten.**

**(2) Der Leiter des CERT-EU ist für das reibungslose Funktionieren des CERT-EU verantwortlich und handelt im Rahmen seiner Zuständigkeiten unter der Leitung des IICB. Er ist verantwortlich für die Umsetzung der strategischen Leitlinien, der Orientierungshilfen, der Ziele und Prioritäten, die vom IICB festgelegt werden, und für die Verwaltung des CERT-EU, einschließlich derjenigen seiner finanziellen und personellen Ressourcen. Er erstattet dem Vorsitzenden des IICB regelmäßig Bericht.**

**(3) Der Leiter des CERT-EU unterstützt den zuständigen bevollmächtigten Anweisungsbefugten bei der Erstellung des in Artikel 66 Absatz 9 der Haushaltsordnung vorgesehenen jährlichen Tätigkeitsberichts, der Finanz- und Verwaltungsinformationen sowie Kontrollergebnisse enthält, und erstattet ihm regelmäßig Bericht über die Umsetzung von Maßnahmen, für die eine Weiterübertragung von Befugnissen erfolgt ist.**

**(4) Der Leiter des CERT-EU erstellt alljährlich eine Finanzplanung für die Verwaltungseinnahmen und -ausgaben für dessen Tätigkeiten, den Vorschlag für das jährliche Arbeitsprogramm, den Vorschlag für den Leistungskatalog des CERT-EU und dessen Überarbeitung, den Vorschlag für die Modalitäten für Leistungsvereinbarungen und den Vorschlag für wesentliche Leistungsindikatoren für das CERT-EU, die vom IICB gemäß Artikel 10 zu billigen sind.**

**Bei der Überarbeitung der Liste der Dienste im Leistungskatalog des CERT-EU berücksichtigt der Leiter des CERT-EU die dem CERT-EU zugewiesenen Ressourcen.**

(5) **Der Leiter** [...] des CERT-EU legt dem IICB **jährliche** Berichte über die Leistung des CERT-EU, die Finanzplanung, die Einnahmen, die Ausführung des Haushaltsplans, Leistungsvereinbarungen und schriftliche Vereinbarungen, die Zusammenarbeit mit entsprechenden Stellen und Partnern und Dienstreisen des Personals vor, einschließlich der in Artikel 10 Buchstabe a [...] genannten Berichte.

*Artikel 15*

***Finanzen und Personal***

[...]

**(1a) Das CERT-EU wird als eigenständiger interinstitutioneller Dienstleister geschaffen, der allen Einrichtungen der Union dient, und wird zugleich in die Verwaltungsstruktur einer Generaldirektion der Kommission integriert, um die Unterstützungsstrukturen der Kommission für Verwaltung, Finanzmanagement und Rechnungsführung nutzen zu können. Die Kommission unterrichtet den IICB über die administrative Zuordnung des CERT-EU und diesbezügliche Änderungen. Dieser Ansatz wird regelmäßig, spätestens vor Ablauf eines gemäß Artikel 312 AEUV festgelegten mehrjährigen Finanzrahmens, bewertet, damit geeignete Maßnahmen ergriffen werden können.**

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

(3) Aufgaben und Tätigkeiten des CERT-EU, einschließlich der Dienste, die vom CERT-EU gemäß Artikel 12 Absätze 2, [...] 4 und 6 sowie gemäß Artikel 13 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 genannten **Einrichtungen** [...] der Union leisten einen jährlichen finanziellen Beitrag zum CERT-EU zur Deckung der vom CERT-EU gemäß Absatz 3 erbrachten Dienste. Die jeweiligen Beiträge beruhen auf Vorgaben des IICB und werden jeweils zwischen den einzelnen Organen, Einrichtungen oder sonstigen Stellen und dem CERT-EU in Leistungsvereinbarungen festgelegt. Die Beiträge entsprechen einem angemessenen und verhältnismäßigen Anteil an den Gesamtkosten der erbrachten Dienste. Sie werden gemäß Artikel 21 Absatz 3 Buchstabe c der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates als zweckgebundene Einnahmen in die in Absatz 3 genannte gesonderte Haushaltslinie eingestellt[12].

(5) Die Kosten für die in Artikel 12 Absatz 5 festgelegten Aufgaben werden bei den **Einrichtungen** [...] der Union eingezogen, denen die CERT-EU-Dienste erbracht werden. Die Einnahmen werden in die Haushaltslinien eingestellt, in denen die Kosten angesetzt wurden.

---

**12** 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).

*Artikel 16*

***Zusammenarbeit des CERT-EU mit den entsprechenden Stellen der Mitgliedstaaten***

(1) Das CERT-EU arbeitet **unverzüglich** mit den entsprechenden nationalen Stellen der Mitgliedstaaten, [...] **insbesondere CSIRTs gemäß Artikel 9 der Richtlinie [NIS-2-Vorschlag] und/oder gegebenenfalls nationalen zuständigen Behörden** und den in Artikel 8 der Richtlinie [NIS-2-Vorschlag] genannten zentralen Anlaufstellen zusammen und tauscht Informationen mit ihnen aus über Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfälle sowie über alle Angelegenheiten, die für die Verbesserung des Schutzes der IT-Umgebungen der **Einrichtungen** [...] der Union relevant sind, auch durch das in Artikel 13 der Richtlinie [NIS-2-Vorschlag] genannte CSIRTs-Netz.

**(1a) Das CERT-EU unterrichtet unverzüglich alle in Absatz 1 genannten entsprechenden nationalen Stellen in einem Mitgliedstaat, wenn es Kenntnis von erheblichen Sicherheitsvorfällen erhält, die sich im Hoheitsgebiet dieses Mitgliedstaats ereignet haben, es sei denn, dem CERT-EU liegt die Information vor, dass die betroffene Einrichtung der Union einen solchen Sicherheitsvorfall bereits gemäß Artikel 20 Absatz 2a gemeldet hat.**

(2) Das CERT-EU **gibt ohne unnötige Verzögerung** [...] spezifische Informationen über Sicherheitsvorfälle an die entsprechenden nationalen Stellen weiter, **ohne dass es** der Einwilligung der betroffenen **Einrichtung** [...] der Union **bedarf**, 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, **nicht weiter** [...], es sei denn

**a) es liegt die Zustimmung der betroffenen Einrichtung der Union vor;**

**b) die betroffene Einrichtung der Union hat bereits veröffentlicht, dass sie betroffen war;**

**c) es gibt keine Zustimmung der betroffenen Einrichtung der Union, aber die Veröffentlichung der Identität der betroffenen Einrichtung der Union würde die Wahrscheinlichkeit erhöhen, dass Sicherheitsvorfälle anderswo vermieden oder abgeschwächt werden. Solche Beschlüsse bedürfen der Zustimmung des Leiters des CERT-EU. Die betroffene Einrichtung der Union wird vor der Veröffentlichung unterrichtet.**

*Artikel 17*

***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 Sicherheitslücken **mit anderen entsprechenden Stellen in der Europäischen Union als den in Artikel 16 genannten Stellen**, einschließlich branchenspezifischer Stellen, zusammenarbeiten. Für jede Zusammenarbeit mit diesen Stellen [...] holt das CERT-EU vorab **im Einzelfall** die Zustimmung des IICB ein. **Das CERT-EU informiert alle einschlägigen entsprechenden nationalen Stellen gemäß Artikel 16 Absatz 1 in einem Mitgliedstaat, in dem die entsprechende Stelle ansässig ist, wenn das CERT-EU mit diesen Stellen zusammenarbeitet.**

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

(3) Das CERT-EU kann, mit Einwilligung der von einem Sicherheitsvorfall betroffenen **Einrichtung der Union** [...], Informationen über diesen **spezifischen** Sicherheitsvorfall an Partner **gemäß den Absätzen 1 und 2 ausschließlich für die Zwecke eines Beitrags** zu seiner Analyse weitergeben, **sofern eine Geheimhaltungsvereinbarung oder ein Geheimhaltungsvertrag mit dem entsprechenden Partner besteht. Solche Geheimhaltungsvereinbarungen oder -verträge sind einer rechtlichen Prüfung im Einklang mit den einschlägigen internen Verfahren der Kommission zu unterziehen. Geheimhaltungsvereinbarungen oder -verträge bedürfen keiner vorherigen Genehmigung durch den IICB, doch dessen Vorsitz ist davon in Kenntnis zu setzen.**

(4) **Das CERT-EU kann in Ausnahmefällen mit vorheriger Zustimmung des IICB Leistungsvereinbarungen mit anderen Einrichtungen als den Einrichtungen der Union schließen.**

## Kapitel V
## ZUSAMMENARBEIT UND BERICHTERSTATTUNGSPFLICHTEN

*Artikel 18*

***Umgang mit Informationen***

(1) Das CERT-EU und die [...] Einrichtungen [...] der Union kommen der Verpflichtung zur Wahrung des Berufsgeheimnisses gemäß Artikel 339 des Vertrags über die Arbeitsweise der Europäischen Union oder gleichwertigen geltenden Rahmenregelungen nach.

(2) Die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates[13] 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 **und gegebenenfalls der Mitgliedstaaten**, wenn eine Anfrage deren Dokumente betrifft.

[...]

(4) Der Umgang des CERT-EU und der [...] Einrichtungen [...] der Union mit Informationen erfolgt im Einklang mit **den geltenden Vorschriften für** die Informationssicherheit [...].

[...]

*Artikel 19*

***Austausch von Informationen zur Cybersicherheit***

**(-1) Einrichtungen der Union können dem CERT-EU freiwillig Informationen über sie betreffende Cyberbedrohungen, Sicherheitsvorfälle, Beinahe-Vorfälle und Sicherheitslücken weitergeben. Das CERT-EU stellt sicher, dass effiziente Kommunikationsmittel zur Verfügung stehen, um den Informationsaustausch mit den Einrichtungen der Union zu erleichtern. Das CERT-EU kann Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten.**

[13] 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).

(1) **Zur Erfüllung seines Auftrags und seiner Aufgaben gemäß Artikel 12 kann** das CERT-EU [...] von [...] Einrichtungen [...] der Union verlangen, ihm Informationen aus ihren jeweiligen IT-Systemverzeichnissen zu übermitteln, **einschließlich Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Sicherheitslücken, Gefährdungsindikatoren, Cybersicherheitswarnungen und Empfehlungen zur Konfiguration von Cybersicherheitsinstrumenten zur Erkennung von Cybersicherheitsvorfällen**. Die **betreffende Einrichtung der Union übermittelt** die verlangten Informationen und alle späteren Aktualisierungen unverzüglich.

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

(3) Das CERT-EU darf spezifische Informationen über Sicherheitsvorfälle, aus denen die Identität der von dem Sicherheitsvorfall betroffenen **Einrichtung** der Union hervorgeht, nur mit Einwilligung der betroffenen **Einrichtung an die Einrichtungen der Union** weitergeben. **Wird die Einwilligung verweigert, so legt die betreffende Einrichtung dem CERT-EU eine hinreichende Begründung vor.**

(4) Die Weitergabepflichten erstrecken sich nicht auf EU-Verschlusssachen (EU-VS) und nicht auf Informationen, **deren Verbreitung über die empfangende Einrichtung der Union hinaus von der Informationsquelle durch eine sichtbare Kennzeichnung ausgeschlossen wurde, es sei denn, die Informationsquelle gestattet ausdrücklich die Weitergabe dieser Informationen an das CERT-EU**.

*Artikel 20*

***Meldepflichten***

**(-1) Ein Sicherheitsvorfall gilt als erheblich, wenn**

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

**b) er andere natürliche oder juristische Personen durch Verursachung eines erheblichen materiellen oder immateriellen Schadens beeinträchtigt hat oder beeinträchtigen kann.**

(1) Alle [...] 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, ob der erhebliche Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist und grenzüberschreitende Auswirkungen hat oder haben könnte;**

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

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

**d) spätestens einen Monat nach Übermittlung der Meldung über den erheblichen Sicherheitsvorfall gemäß Buchstabe b einen Abschlussbericht, der mindestens Folgendes enthält:**

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

**ii) Angaben zur Art der Bedrohung bzw. zugrundeliegenden Ursache, die den erheblichen Sicherheitsvorfall wahrscheinlich ausgelöst hat;**

**iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;**

**iv) gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls;**

**e) in Fällen, in denen erhebliche Sicherheitsvorfälle zum Zeitpunkt der Übermittlung des unter Buchstabe d genannten Abschlussberichts noch andauern, einen Fortschrittsbericht zu diesem Zeitpunkt und einen Abschlussbericht innerhalb eines Monats nach Bewältigung des Sicherheitsvorfalls.**

[...]

[...]

[...]

[...]

**(2a) Alle Einrichtungen der Union geben die gemäß Absatz 1 gemeldeten Informationen innerhalb desselben Zeitrahmens an etwaige einschlägige entsprechende nationale Stellen nach Artikel 16 Absatz 1 an ihrem Standort weiter.**

(3) Das CERT-EU legt **dem IICB, dem EU-INTCEN und dem CSIRT-Netzwerk alle drei Monate** einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu [...] Cyberbedrohungen, [...] Sicherheitslücken **gemäß Artikel 19, Antworten von Einrichtungen der Union auf Aufrufe zum Tätigwerden gemäß Artikel 13 Absatz 1 Buchstabe a** und erheblichen Sicherheitsvorfällen enthält, die gemäß Absatz 1 gemeldet wurden. **Dieser Bericht ist ein Beitrag zum Zweijahresbericht über den Stand der Cybersicherheit in der Union gemäß Artikel 15 der Richtlinie [NIS-2-Vorschlag].**

(4) Das IICB **gibt bis zum [6 Monate nach Inkrafttreten dieser Verordnung]** Leitlinien oder Empfehlungen **heraus, in denen die** Modalitäten**, das Format und der** Inhalt der **Berichterstattung näher festgelegt werden**. **In den Leitlinien oder Empfehlungen werden die Bestimmungen, die durch etwaige Durchführungsrechtsakte gemäß Artikel 20 Absatz 11 der Richtlinie [NIS-2-Vorschlag] durchgeführt werden, gebührend berücksichtigt.** Das CERT-EU verbreitet die sachdienlichen technischen Einzelheiten, um eine proaktive Erkennung und Reaktion oder Abhilfemaßnahmen durch die [...] Einrichtungen [...] der Union zu ermöglichen.

(5) Die **Meldepflichten** erstrecken sich nicht auf EU-Verschlusssachen (EU-VS) und nicht auf Informationen, **deren Verbreitung über die empfangende Einrichtung der Union hinaus von der Informationsquelle durch eine sichtbare Kennzeichnung ausgeschlossen wurde, es sei denn, die Informationsquelle gestattet ausdrücklich die Weitergabe dieser Informationen an das CERT-EU**.

*Artikel 21*

***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, Sicherheitslücken und Sicherheitsvorfälle zwischen

a) [...] Einrichtungen [...] der Union,

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

(2) Das CERT-EU – **gegebenenfalls in enger Zusammenarbeit mit der ENISA gemäß Artikel 7 Absatz 7 Buchstabe d des Rechtsakts zur Cybersicherheit[14] –** erleichtert die Koordinierung zwischen den [...] Einrichtungen [...] der Union bei der Reaktion auf Sicherheitsvorfälle, unter anderem durch

a) einen Beitrag zur kontinuierlichen externen Kommunikation;

[...]

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 Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfällen.

---

**14** 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).

(4) Der IICB **nimmt bis zum [12 Monate nach Inkrafttreten 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 Ratschläge für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

*Artikel 22*

***Bewältigung schwerwiegender Sicherheitsvorfälle***

**(-1) Zur Unterstützung der koordinierten Bewältigung schwerwiegender Sicherheitsvorfälle auf operativer Ebene, von denen Einrichtungen der Union betroffen sind, und als Beitrag zum regelmäßigen Austausch einschlägiger Informationen zwischen Einrichtungen der Union und mit Mitgliedstaaten entwickelt der IICB in enger Zusammenarbeit mit dem CERT-EU und der ENISA einen Cyberkrisenbewältigungsplan auf der Grundlage der in Artikel 21 Absatz 2 beschriebenen Tätigkeiten, der mindestens folgende Elemente enthält:**

a) **Modalitäten für die Koordinierung und den Informationsfluss zwischen Einrichtungen der Union für die 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;**

f) **eine Kontaktstelle für das EU-CyCLONe, die einschlägige Informationen als Beiträge zu einer gemeinsamen Lageerfassung an das EU-CyCLONe weitergibt.**

(1) Das CERT-EU koordiniert die Maßnahmen der [...] Einrichtungen [...] der Union zur Bewältigung schwerwiegender **Sicherheitsvorfälle**. Es führt ein Verzeichnis der technischen Fachkenntnisse, die für die Reaktion auf **schwerwiegende Sicherheitsvorfälle** notwendig sind.

(2) 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.

**(3) Auf ausdrückliches Ersuchen eines Mitgliedstaats, in dem die betroffene Einrichtung der Union ansässig ist, und mit** Zustimmung der betroffenen **Einrichtung** der Union kann das CERT-EU [...] auch Sachverständige aus der in Absatz 2 genannten Liste für einen Beitrag zu der Reaktion auf einen schwerwiegenden **Sicherheitsvorfall in dieser Einrichtung der Union** hinzuziehen.

## Kapitel VI
## SCHLUSSBESTIMMUNGEN

*Artikel 23*

***Erste Umschichtung von Haushaltsmitteln***

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

*Artikel 24*

***Überprüfung***

(1) Der IICB erstattet der Kommission mit Unterstützung des CERT-EU regelmäßig Bericht über die Durchführung dieser Verordnung. Der IICB kann auch Empfehlungen **zur Überprüfung dieser Verordnung** an die Kommission richten [...].

(2) Die Kommission erstattet dem Europäischen Parlament und dem Rat spätestens **36** Monate nach dem Inkrafttreten dieser Verordnung und danach alle drei Jahre Bericht über die Durchführung dieser Verordnung.

(3) Die Kommission evaluiert die Funktionsweise dieser Verordnung und erstattet dem Europäischen Parlament, dem Rat, dem Wirtschafts- und Sozialausschuss und dem Ausschuss der Regionen **spätestens** fünf Jahre nach dem Inkrafttreten Bericht. **Dem Bericht wird erforderlichenfalls ein Gesetzgebungsvorschlag beigefügt.**

*Artikel 25*

***Inkrafttreten***

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

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

Geschehen zu Brüssel am

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

[...]

**ANHANG II**

[...]