STELLUNGNAHME

DER REGIERUNG

AN DEN

LANDTAG DES FÜRSTENTUMS LIECHTENSTEIN

ZU DEN ANLÄSSLICH DER ERSTEN LESUNG BETREFFEND DIE SCHAFFUNG EINES GESETZES ÜBER CYBERSICHERHEIT (CYBER-SICHERHEITSGESETZ; CSG) SOWIE ABÄNDERUNG DES BESCHWERDEKOMMISSIONSGESETZES AUFGEWORFENEN FRAGEN

Behandlung im Landtag	
	Datum
1. Lesung	**03.03.2023**
2. Lesung	
Schlussabstimmung	

Nr. 35 /2023

INHALTSVERZEICHNIS

Seite

Beilage:

- Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1);
- Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls (ABl. L 26 vom 31.1.2018, S. 48);
- Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1);

ZUSAMMENFASSUNG

Der Landtag hat an seiner Sitzung vom 3. März 2023 die Regierungsvorlage betreffend die Schaffung eines Gesetzes über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG) sowie die Abänderung des Beschwerdekommissionsgesetzes in erster Lesung behandelt. Die Regierungsvorlage wurde begrüsst, das Eintreten auf die Vorlage war unbestritten.

Die vorliegende Stellungnahme beantwortet die anlässlich der ersten Lesung aufgeworfenen Fragen, soweit sie seitens der Regierung nicht bereits während der Landtagsdebatte abschliessend beantwortet wurden.

Die offenen Fragen betrafen schwerpunktmässig die Verordnung (EU) 2019/817, bei welcher es sich um eine Weiterentwicklung des Schengen-Besitzstandes handelt, sowie den Geltungsbereich des Cyber-Sicherheitsgesetzes, beispielsweise ob dieser auf den Bereich Polizei und Feuerwehr anwendbar sei sowie allfällige Einschränkungen in Bezug auf den Geltungsbereich, etwa in Bezug auf die Ausnahmen für Klein- und Kleinstgesellschaften. Die übrigen Fragen betrafen die Unterrichtung der Öffentlichkeit nach Sicherheitsvorfällen, den fehlenden Lex specialis-Vorbehalt für Anbieter digitaler Dienste, die NIS-Strategie sowie die Zusammenarbeit mit Dritten zwecks der Erfüllung ihrer Aufgaben durch die Stabsstelle Cyber-Sicherheit.

Im Nachgang zur ersten Lesung im Landtag wurden Anpassungen im Gesetzesentwurf vorgenommen. Neu eingefügt wurde ein Lex specialis-Vorbehalt für Anbieter digitaler Dienste im Zusammenhang mit den Sicherheitsanforderungen und der Meldepflicht. Die nicht abschliessende Liste jener Stellen, mit welchen die Stabsstelle Cyber-Sicherheit zusammenarbeitet, wurde erweitert. Überdies wurde vorgesehen, dass die NIS-Strategie nach der Genehmigung durch die Regierung auf der Internetseite der Stabsstelle Cyber-Sicherheit veröffentlicht werden soll.

Abschliessend hat sich gezeigt, dass es im Hinblick auf die Übernahme der Richtlinie (EU) 2016/1148 (NIS-Richtlinie) voraussichtlich zu Verzögerungen kommen wird. Das Inkrafttreten des EWR-Übernahmebeschlusses ist damit noch nicht absehbar. Aus diesem Grund erscheint es notwendig, eine Vorabumsetzung vorzusehen. Die diesbezüglichen Artikel wurden in den Schlussbestimmungen angepasst.

ZUSTÄNDIGES MINISTERIUM

Ministerium für Präsidiales und Finanzen

BETROFFENE STELLEN

Stabsstelle Cyber-Sicherheit
Amt für Informatik
Amt für Kommunikation
Datenschutzstelle
Finanzmarktaufsicht Liechtenstein
Landespolizei
Staatsanwaltschaft
Stabsstelle FIU
Gemeinden
Öffentlich-rechtliche Stiftungen und Anstalten
Andere juristische Personen des öffentlichen und privaten Rechts, die überwiegend vom Staat, den Gemeinden oder von anderen Einrichtungen des öffentlichen Rechts finanziert werden oder deren Aufsicht unterliegen.

Vaduz, 03. April 2023

LNR 2023-503

P

Sehr geehrter Herr Landtagspräsident,
Sehr geehrte Frauen und Herren Abgeordnete

Die Regierung gestattet sich, dem Hohen Landtag nachstehende Stellungnahme zu den anlässlich der ersten Lesung betreffend die Schaffung eines Gesetzes über Cybersicherheit sowie die Abänderung des Beschwerdekommissionsgesetzes (BuA Nr. 9/2023) aufgeworfenen Fragen zu unterbreiten.

I. STELLUNGNAHME DER REGIERUNG

1. ALLGEMEINES

Anlässlich der ersten Lesung des Bericht und Antrags betreffend die Schaffung eines Gesetzes über Cybersicherheit (Cyber-Sicherheitsgesetz; CSG) sowie Abänderung des Beschwerdekommissionsgesetzes am 3. März 2023 hat der Landtag die Vorlage begrüsst. Das Eintreten auf die Gesetzesvorlagen war unbestritten.

In der Eintretensdebatte wurden verschiedene Fragen zu den Ausführungen im Bericht und Antrag Nr. 9/2023 aufgeworfen. Diese Fragen werden mit der gegenständlichen Stellungnahme beantwortet, soweit diese vom zuständigen Regierungsmitglied im Rahmen der ersten Lesung nicht abschliessend beantwortet wurden.

2. GRUNDSÄTZLICHE FRAGEN

Im Rahmen der Eintretensdebatte wurde von einem Abgeordneten mehrfach die Frage aufgeworfen, ob in der vorliegenden Gesetzesvorlage zum Cyber-Sicherheitsgesetz allenfalls die Schengen Verordnung (EU) 2019/817 zu berücksichtigen gewesen wäre.

Einleitend ist festgehalten, dass die Verordnung (EU) 2019/817[1] nicht EWR-relevant ist, sondern es sich um eine Weiterentwicklung des Schengen-Besitzstandes handelt. Die Übernahme der Verordnung (EU) 2019/817 war bereits im Jahr 2020 Gegenstand von Beratungen im Landtag (BuA Nr. 66/2020). Daraufhin wurde auch das Ausländergesetz (vgl. Art. 76a ff.) entsprechend angepasst.

Die Zuständigkeiten in Bezug auf die Informationssysteme der EU, sprich das Einreise-/Ausreisesystem («EES»), das Visa-Informationssystem («VIS»), das Europäische Reiseinformations- und Reisegenehmigungssystem («ETIAS»), Eurodac, das Schengener Informationssystem («SIS») und das Europäische Strafregisterinformationssystem für Drittstaatsangehörige («ECRIS-TCN»), liegen bei der Landespolizei und beim Ausländer- und Passamt. Dort sind die Zuständigkeiten auch richtig verortet.

Der sichere Betrieb von IT- oder auch OT-Systemen obliegt dem jeweiligen Betreiber der Systeme oder, wie im Falle von Informationssystemen der EU, der jeweils zuständigen nationalen Stelle. Die Stabsstelle Cyber-Sicherheit kann keine – auch

[1] Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27-84).

nicht für die Liechtensteinische Landesverwaltung oder das Amt für Informatik – Zuständigkeit für bestimmte Netz- und Informationssysteme übernehmen.

Dies ist alleine deswegen nicht möglich, weil der Stabsstelle Cyber-Sicherheit als nationale Behörde nach Art. 8 Abs. 1 der Richtlinie (EU) 2016/1148 die Aufsicht und der Vollzug dieses Gesetzes obliegen. Eine Zuständigkeit für ein bestimmtes Netz- und Informationssystem würde unweigerlich zu einem unüberwindbaren Interessenskonflikt führen. Denn mit der Übernahme von Zuständigkeiten für ein Netz- und Informationssystem wären der Betrieb und die Weiterentwicklung der Systeme im weitesten Sinn, und dadurch die Einhaltung der Sicherheitsanforderungen sowie der Meldepflichten nach diesem Gesetz gleichzeitig mit der Aufsicht bei der Stabsstelle vereint.

Ungeachtet dessen wird die Stabsstelle Cyber-Sicherheit eng mit der Landespolizei sowie dem Ausländer- und Passamt zusammenarbeiten. Bereits jetzt findet ein regelmässiger Informationsaustausch auf strategischer Ebene zwischen der Landespolizei und der Stabsstelle Cyber-Sicherheit statt. Aus diesem Grund wurde die Zusammenarbeit mit der Landespolizei auch explizit als Aufgabe der Stabsstelle Cyber-Sicherheit in die ohnehin bloss demonstrative Aufzählung in Art. 13 Abs. 1 Bst. i dieser Vorlage mitaufgenommen.

Der Abgeordnete verwies auf den Anhang der Verordnung (EU) 2019/817, wonach in jedem Land ein sogenanntes Reaktionsteam für Sicherheitsvorfälle (Security Incident Response Capability Team, SIRC) als auch weitere Organisationsstrukturen unter der Verantwortung eines Inzident-Managers im Rahmen einer 365/24/7-Verfügbarkeit aufgebaut werden müssen. Anschliessend wurde seitens des Landtagsabgeordneten die Struktur des nationalen Koordinierungszentrums, der Kooperationsgruppe und des CSIRT-Teams erwähnt, wobei letzteres bei der Stabsstelle Cyber-Sicherheit «erstellt» werde. Der Abgeordnete sieht Parallelen und befürchtet, dass mit dieser Vorlage ohne Berücksichtigung der Verordnung (EU)

2019/817 allenfalls sogar Parallelstrukturen ohne eine definierte Zuständigkeit aufgebaut würden.

Gemäss Art. 13 Abs. 1 Bst. b CSG wird das CSIRT nach Art. 19 bei der Stabsstelle Cyber-Sicherheit eingerichtet und von dieser koordiniert. Wie weiter unten zu Art. 9 ausgeführt, wird von der Stabsstelle Cyber-Sicherheit derzeit evaluiert, inwiefern die Anforderungen an ein CSIRT selbst erfüllt werden können und welche Aufgaben allenfalls an Dritte ausgelagert werden müssen.

Die Vernetzung und der Informationsaustausch mit den «Reaktionsteams» der einzelnen Betreiber wesentlicher Dienste ist eine zentrale Aufgabe der Stabsstelle Cyber-Sicherheit, weshalb die Regierung der Auffassung ist, dass die Stabsstelle dafür die korrekte Stelle ist.

Betreffend die nationale Koordinierungsstelle (NCC) im Sinne der Verordnung (EU) 2021/887[2] wird auf die Ausführungen zu Art. 13 Abs. 1 Bst. g im Bericht und Antrag zum Cyber-Sicherheitsgesetz (BuA Nr. 9/2023) verwiesen. Die Stabsstelle Cyber-Sicherheit wird hier insbesondere eine koordinierende Rolle innehaben.

Die Kooperationsgruppe nach Art. 11 der Richtlinie (EU) 2016/1148 (sogenannte «NIS Cooperation Group») setzt sich aus Vertretern der EU-Mitgliedstaaten, der Europäischen Kommission und der EU-Agentur für Cybersicherheit (ENISA) zusammen. Der Vorsitz wird von jenem Mitgliedstaat besetzt, der den Vorsitz im Rat der Europäischen Union innehat. Die Kooperationsgruppe soll die strategische Zusammenarbeit und den Informationsaustausch zwischen den EWR-Mitgliedstaaten gewährleisten.

---

[2] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. 202 vom 8.6.2021, S. 1).

Jeder EWR-Mitgliedstaat hat eine zentrale Anlaufstelle für die Sicherheit von Netz- und Informationssystemen zu benennen, die für die Gewährleistung der grenzüberschreitenden Zusammenarbeit mit anderen Mitgliedstaaten und mit der Kooperationsgruppe zuständig ist. In Liechtenstein wird diese Aufgabe die Stabsstelle Cyber-Sicherheit übernehmen.

Aufgrund der Tatsache, dass die Kooperationsgruppe bereits unter dem Vorsitz der EU-Mitgliedstaaten eingerichtet wurde und ein regelmässiger Austausch der EWR-Mitgliedstaaten im Rahmen der Kooperationsgruppe bereits stattfindet, erachtet es die Regierung nicht für erforderlich, dass hier Strukturen bei der Stabsstelle Cyber-Sicherheit aufgebaut werden.

Die Regierung ist daher überzeugt, dass die Zuständigkeiten im Bereich der Cyber-Sicherheit in Liechtenstein bereits korrekt definiert sind und insbesondere keine Parallelstrukturen aufgebaut werden. Vielmehr wird durch die Vernetzung und Zusammenarbeit der jeweils zuständigen Stellen insgesamt ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen gewährleistet und die Ressourcen in Liechtenstein optimal genutzt.

3. FRAGEN ZU EINZELNEN ARTIKELN

Zu Art. 1

Ein Abgeordneter fragte, ob der Geltungsbereich die Polizei und die Feuerwehr miteinschliesse, denn diese würden in Krisensituationen für die Sicherheit im Land sorgen. In diesem Zusammenhang wird das bei der Feuerwehr verwendete System «POLYCOM» erwähnt.

Mit dem zu erlassenden Gesetz werden den Betreibern wesentlicher Dienste in den Sektoren gemäss Abs. 1 Bst. a entsprechende Pflichten, wie beispielsweise die Einhaltung von bestimmten Sicherheitsanforderungen nach Art. 4 und Meldepflichten

nach Art. 5, auferlegt. Die gegenständlichen Regelungen zielen vor allem darauf ab, die Verfügbarkeit der wesentlichen Dienste sicherzustellen.

Die Landespolizei und die Feuerwehren sind per se nicht als wesentlicher Dienst im Sinne der NIS-Richtlinie bzw. des Gesetzes zu qualifizieren. Um ihren Aufgaben nachzukommen, greifen aber sowohl die Landespolizei als auch die Feuerwehren auf Dienste zurück, die in den Geltungsbereich dieses Gesetzes fallen. Wesentlich für die Landespolizei und die Feuerwehren sind unter anderem die (öffentlichen) Informations- und Kommunikationstechnologien, welche für die Alarmierung sowie die Kommunikation und Koordination von Einsätzen unabdingbar sind.

Der Sektor «Digitale Infrastruktur» in Art. 1 Abs. 1 Bst. a umfasst unter anderem die Anbieter öffentlicher elektronischer Kommunikationsnetze sowie elektronischer Kommunikationsdienste, wodurch für die Betreiber dieser Dienste die Anforderungen dieses Gesetzes gelten. Zur Klarstellung wird dies in die Verordnung zum Cyber-Sicherheitsgesetz auch mit aufgenommen werden. Zu berücksichtigen ist jedoch, dass das gegenständliche Gesetz gemäss Art. 3 Abs. 1 Bst. e lediglich für Betreiber wesentlicher Dienste mit Sitz in Liechtenstein gilt.

Zur Frage, ob das POLYCOM System in den Geltungsbereich des Gesetzes fällt, weist die Regierung darauf hin, dass das POLYCOM ein flächendeckendes Sicherheitsfunknetz der Schweizer Behörden und Organisationen für Rettung und Sicherheit ist. Liechtenstein nimmt basierend auf einer Vereinbarung zwischen der Regierung und dem Schweizerischen Bundesrat an POLYCOM teil.[3] Die zuständigen Behörden und Stellen für den Vollzug dieser Vereinbarung in Liechtenstein sind

[3] Vereinbarung zwischen der Regierung des Fürstentums Liechtenstein und dem Schweizerischen Bundesrat über die Teilnahme des Fürstentums Liechtenstein am Sicherheitsnetz Funk «POLYCOM», abgeschlossen in Vaduz am 18. Oktober 2003; LGBl-Nr. 2014.339, LR-Nr.: 0.141.310.112.

gemäss Art. 2 Bst. b der erwähnten Vereinbarung die Landespolizei als auch das Amt für Kommunikation.

POLYCOM ist als geschlossenes und abgesichertes Kommunikationsmittel auf Mobilfunkbasis konzipiert, welches in Krisen und ausserordentlichen Lagen, auch bei Ausfall des Stromnetzes, den Einsatzkräften zur Verfügung steht. Das System besteht aus einer festen Funkinfrastruktur mit entsprechenden Basisstationen sowie mobilen Funkgeräten. Betrieben wird POLYCOM – ebenso unter Berücksichtigung der Cyber-Sicherheit – vom Bund in der Schweiz.

Zu Art. 3

Betreffend Art. 3 Abs. 1 Bst. g erwähnte ein Abgeordneter die Ausnahme für Klein- und Kleinstgesellschaften. Diese habe er in Art. 4 Ziff. 6 der Richtlinie (EU) 2016/1148 so nicht gefunden. Er stelle sich deshalb die Frage, woher diese Ausnahme komme.

Diese Einschränkung ist nicht in den Begriffsbestimmungen in Art. 4 der Richtlinie (EU) 2016/1148 zu finden, sondern in Art. 16 Abs. 11 der Richtlinie (EU) 2016/1148. Darin wird geregelt, dass Kapitel V, das unter anderem die Sicherheitsanforderungen und Meldepflichten für Anbieter digitaler Dienste enthält, nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission gilt.

Diese Ausnahme wird ebenso in Erwägungsgrund 53 der Richtlinie (EU) 2016/1148 aufgeführt. Demnach sollen die Verpflichtungen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist. Im Fall von Anbietern digitaler Dienste sollen diese Bestimmungen nicht für Kleinst- und Kleinunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission gelten.

Die Empfehlung 2003/361/EG der Kommission ist nicht EWR-relevant. Sie wurde daher nicht in das EWR-Abkommen übernommen. Folglich entfaltet die Empfehlung 2003/361/EG der Kommission in Liechtenstein keine rechtliche Wirkung.

Welche Unternehmen als kleine Gesellschaft oder Kleinstgesellschaften gelten, ist in Liechtenstein in Art. 1064 Abs. 1 und 1a des Personen- und Gesellschaftsrechts (PGR) geregelt. Daher wird in Art. 3 Abs. 1 Bst. g auf Art. 1064 Abs. 1 und 1a PGR und nicht auf besagte Empfehlung der Kommission verwiesen.

Ein Abgeordneter möchte ebenso zu Art. 3 Abs. 1 Bst. g wissen, warum die Definition zu den Anbietern digitaler Dienste nur juristische Personen und nicht auch natürliche Personen umfasse.

In Art. 4 Ziff. 6 der Richtlinie (EU) 2016/1148 ist eine entsprechende Einschränkung auf juristische Personen vorgesehen, weshalb diese im Sinne einer richtlinienkonformen Umsetzung in die Vorlage übernommen wurde.

Weiters stellte ein Abgeordneter unter Berücksichtigung der Definition gemäss Art. 3 Abs. 1 Bst. g Ziff. 1 und 2 die Frage, inwiefern Anbieter digitaler Dienste in anderen EWR Ländern – ausser Liechtenstein – hier von der Legaldefinition umfasst seien.

Die Anbieter digitaler Dienste unterliegen jeweils den nationalen Gesetzen jenes Staates, in dem sie ihren Sitz haben. Die Richtlinie (EU) 2016/1148 ist von sämtlichen EWR-Mitgliedstaaten umzusetzen, weshalb davon ausgegangen werden kann, dass sämtliche Mitgliedstaaten des EWR im Bereich der Cyber-Sicherheit dasselbe Sicherheitsniveau haben.

Somit besteht hier keine etwaige Regelungslücke. Die Stabsstelle Cyber-Sicherheit ist für sämtliche Anbieter digitaler Dienste mit Sitz in Liechtenstein (Art. 3 Abs. 1 Bst. g) oder Anbieter digitaler Dienste mit Sitz in einem Drittstaat zuständig, sofern

letztere einen Vertreter nach Bst. h im Inland benannt haben. Anbieter digitaler Dienste mit Sitz in einem anderen EWR-Mitgliedstaat unterliegen deren nationalem Recht und der Aufsicht der dortigen Behörden.

Ein Abgeordneter möchte zu Bst. m wissen, wie hoch die Aufwendungen für die Teilnahme an der Kooperationsgruppe nach Art. 11 der Richtlinie (EU) 2016/1148 seien?

Die Kooperationsgruppe trifft sich an vier Tagen im Jahr in Brüssel und tauscht in diesen Sitzungen insbesondere Erfahrungen und Informationen zu aktuellen Themen betreffend Cyber-Sicherheit aus. Die Sitzungen finden in hybrider Form statt und eine virtuelle Teilnahme ist ebenfalls möglich. Seit November 2022 wird die Stabsstelle Cyber-Sicherheit zu den Sitzungen eingeladen und nahm bisher an zwei Sitzungstagen teil.

Ein Abgeordneter stellt eine Frage zu den Begriffsbestimmungen. Künstliche Intelligenzen (KI) seien auf dem Vormarsch und es wäre daher sinnvoll, wenn diese in irgendeiner Form in den Definitionen aufgenommen werden würden. Am ehesten in Art. 1 Abs. 1 Bst. p, den «Online-Suchmaschinen», was aber auch nicht wirklich treffend sei. Dort würde von Links und nicht von Ergebnissen gesprochen.

Die Definition der Online-Suchmaschinen in Bst. p entspricht – mit Ausnahme des Begriffs Internetseite anstelle von Website – wortwörtlich jener in Art. 3 Ziff. 18 der Richtlinie (EU) 2016/1148.

Wie seitens der Regierung im Zuge der ersten Lesung im Landtag am 3. März 2023 bereits ausgeführt wurde, hat die EU-Kommission im April 2021 einen Vorschlag für eine Verordnung zur Regulierung von Künstlicher Intelligenz in der EU

veröffentlicht (KI-Verordnung).[4] Darin findet sich in den Begriffsbestimmungen in Art. 3 Ziff. 1 auch eine Definition für ein «System der künstlichen Intelligenz».

Die Verordnung ist EWR-relevant und wird nach Abschluss des Gesetzgebungsverfahrens in der EU in das EWR-Abkommen zu übernehmen sein.

Wie von einer Abgeordneten erwähnt, finden sich in der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) zwei Hinweise auf künstliche Intelligenz. So soll gemäss Erwägungsgrund 51 der NIS-2-Richtlinie der Einsatz innovativer Technologien, einschliesslich künstlicher Intelligenz, gefördert werden, deren Einsatz die Aufdeckung und Verhütung von Cyberangriffen verbessern können. Ausserdem sollten gemäss Erwägungsgrund 89 die wesentlichen und wichtigen Einrichtungen ihre eigenen Cybersicherheitskapazitäten bewerten und gegebenenfalls die Integration von Technologien zur Verbesserung der Cybersicherheit anstreben, etwa künstliche Intelligenz oder Systeme des maschinellen Lernens, um ihre Kapazitäten und die Sicherheit von Netz- und Informationssystemen zu erhöhen. Doch auch hier wird die KI nicht näher definiert.

Die Regierung möchte der erwähnten KI-Verordnung sowie anderer einschlägiger Rechtsakte aus der EU weder mit einer Definition noch mit anderweitigen Regelungen zu KI vorgreifen und die jeweiligen EU-Regelungen bzw. deren Übernahme in das EWR-Abkommen abwarten.

Wie seitens der Regierung bereits in der ersten Lesung ausgeführt, macht es für die Anwendung dieses Gesetzes auch keinen Unterschied, ob ein Mensch oder eine künstliche Intelligenz den Ausgangspunkt einer Cyberbedrohung darstellen.

---

[4] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final vom 21. April 2021.

Zu Art. 5

Ein Abgeordneter möchte wissen, in welchen Fällen die Stabsstelle Cyber-Sicherheit die Öffentlichkeit informiert und in welchen nicht.

Gemäss Abs. 5 kann die Stabsstelle Cyber-Sicherheit nach Anhörung des meldenden Betreibers wesentlicher Dienste die Öffentlichkeit über konkrete Sicherheitsvorfälle unterrichten, wenn die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist.

So wird die Stabsstelle Cyber-Sicherheit nach Meldungen nach Art. 5 beispielsweise die Öffentlichkeit über die Vorgehensweise eines Angreifers informieren oder falls vorhanden und zweckmässig sogenannte IOCs (Indicators of compromise) zur Verfügung stellen, damit weitere Sicherheitsvorfälle verhindert werden können. Solche IOCs können vor allem für die Früherkennung von zukünftigen Angriffen genutzt werden. Diese Informationen stammen jedoch in der Regel von der meldenden Stelle, die aus diesem Grund vor der Veröffentlichung von Informationen auch anzuhören ist.

Eine Unterrichtung der Öffentlichkeit ist nicht für Sicherheitsvorfälle vorgesehen, die sich beispielsweise lediglich auf den Betreiber wesentlicher Dienste selbst begrenzen und aufgrund der Art des Sicherheitsvorfalls eine Sensibilisierung der Öffentlichkeit unterbleiben kann.

Zu Art. 6

Eine Abgeordnete stellt fest, dass es für Betreiber wesentlicher Dienste, u.a. für das Bankwesen, einen Lex specialis Vorbehalt gibt. Hier stelle sich die Frage, ob es eine solche nicht auch für digitale Dienste gemäss Art. 3 Abs. 1 Bst. f, beispielsweise für den Krypto-Markt, geben sollte?

Der Lex specialis Vorbehalt für Anbieter digitaler Dienste wurde in der bisherigen Gesetzesvorlage nicht berücksichtigt, da dieser derzeit nach Auffassung der Regierung in Liechtenstein keinen Anwendungsbereich hätte. Die Regierung nimmt den Hinweis der Landtagsabgeordneten jedoch zur Kenntnis und teilt die Auffassung, dass die Aufnahme eines Lex specialis Vorbehalts auch für Anbieter digitaler Dienste im Hinblick auf zukünftige Entwicklungen sinnvoll ist. Schliesslich ist derzeit nicht auszuschliessen, dass künftig ein Anwendungsbereich dafür entstehen könnte. Da die Richtlinie (EU) 2016/1148 einen solchen gemäss Art. 1 Abs. 7 ebenso vorsieht, wurde dieser in der überarbeiteten Vorlage in Abs. 3 neu eingefügt.

Zu Art. 7

Neben dem Lex specialis Vorbehalt für die Sicherheitsanforderungen gemäss Art. 6 wurde der Vorbehalt ebenso für die Meldepflicht von Anbietern digitaler Dienste mit Abs. 3 neu eingefügt.

Zu Art. 9

Ein Abgeordneter bittet die Regierung in Bezug auf Abs. 1 die erwähnte Verordnung (EU) 2019/817 zu beachten.

In Bezug auf die Verordnung (EU) 2019/817 wird auf die detaillierten Ausführungen in Abschnitt 2 (Grundsätzliche Fragen) verwiesen.

Ein Abgeordneter möchte wissen, welche Aufgaben nach Abs. 2 ausgelagert werden sollen?

Die Aufgaben der Stabsstelle Cyber-Sicherheit sind in Art. 13 Abs. 1 sowie des Computer-Notfallteams in Art. 19 Abs. 1 geregelt. Inwiefern bestimmte Aufgaben ständig ausgelagert werden, wird im Einzelfall zu prüfen sein und soll eher die Ausnahme als die Regel darstellen. Wo möglich und zweckmässig soll das erforderliche Know-how intern in der Stabsstelle Cyber-Sicherheit auf- bzw. wo bereits vorhanden, noch ausgebaut werden.

Die Stabsstelle Cyber-Sicherheit wird sich jedoch insbesondere bei Kontrollen nach Art. 13 Abs. 1 Bst. a i.V.m. Art. 18 Abs. 1 qualifizierten Dritten bedienen müssen, wie beispielsweise bei der Kontrolle der Sicherheitsmassnahmen von Systemen eines Energie- oder Wasserversorgers. Die IT- und OT-Systeme in den Sektoren Energie- und Trinkwasserversorgung, aber auch in anderen Sektoren wie Gesundheit, sind weitgehend branchenspezifisch, sodass hier auf externe Experten zurückgegriffen werden muss.

Das Computer-Notfallteam (CSIRT) wird am ehesten in Bezug auf die allgemeine Unterstützung bei der Reaktion auf einen Sicherheitsvorfall gemäss Art. 19 Abs. 1 Bst. c auf externe Experten zurückgreifen. Aktuell wird von der Stabsstelle Cyber-Sicherheit evaluiert, inwiefern die Anforderungen an ein CSIRT selbst erfüllt werden können und welche Aufgaben allenfalls an Dritte ausgelagert werden müssen.

Zu Art. 13

Ein Abgeordneter merkt an, dass in Abs. 1 Bst. i das Amt für Informatik fehlen würde.

Bei Art. 13 Abs. 1 Bst. i handelt es sich um eine demonstrative und nicht abschliessende Aufzählung. Ungeachtet dessen wird dem Anliegen entsprochen und das Amt für Informatik der Liechtensteinischen Landesverwaltung in die Liste unter Art. 13 Abs. 1 Bst. i aufgenommen.

Es wird jedoch unterstrichen, dass es sich bei der Aufzählung in Art. 13 Abs. 1 um eine demonstrative und damit nicht abschliessende Aufzählung handelt. Es ist daher eine Aufgabe der Stabsstelle Cyber-Sicherheit, auch mit anderen nicht in Bst. i aufgeführten inländischen Behörden und Stellen zusammenzuarbeiten.

Zu Art. 16

Seitens eines Abgeordneten wird um nähere Ausführungen zum Begriff «formlos» in Abs. 1 erbeten.

Zu den bereits in der ersten Lesung gemachten Ausführungen wird ergänzt, dass der Begriff «formlos» in Abs. 1 so zu verstehen ist, dass es sich um keine rechtsmittelfähige Verfügung handelt, wie sie beispielsweise in Abs. 5 erwähnt wird.

Jedenfalls wird die Stabsstelle Cyber-Sicherheit aber stets eine solche Form wählen, die der Situation angemessen ist. So wird die Mitteilung grundsätzlich schriftlich (Brief oder auch elektronisch über einen gesicherten Kanal) erfolgen. In dieser Mitteilung hat die Stabsstelle Cyber-Sicherheit auch die Anhaltspunkte entsprechend darzulegen, aufgrund welcher sie davon ausgeht, dass ein Betreiber wesentlicher Dienste oder ein Anbieter digitaler Dienste gegen das Cyber-Sicherheitsgesetz verstösst.

Zusammengefasst kann ausgeführt werden, dass der Begriff «formlos» ein Rechtsbegriff ist, der regelmässig Verwendung findet, um darzulegen, dass es sich bei einer Mitteilung um keine rechtsmittelfähige Verfügung handelt.

Für die Verhängung von Bussen nach Art. 22 ist in jedem Fall eine rechtsmittelfähige Verfügung erforderlich.

Zu Art. 20

Eine Abgeordnete schlägt vor, Art. 20 Abs. 3 dahingehend zu ändern, dass die NIS-Strategie nach der Genehmigung veröffentlicht werden soll.

Dem Vorschlag wird entsprochen, weshalb Art. 20 Abs. 3 entsprechend ergänzt wurde. So wird die NIS-Strategie im Anschluss an die Genehmigung der Regierung auf der Internetseite der Stabsstelle Cyber-Sicherheit veröffentlicht.

Zu Art. 21

Ein Abgeordneter möchte die Gründe für die Beschränkung der Überprüfungsbefugnis der Beschwerdekommission für Verwaltungsangelegenheiten sowie des Verwaltungsgerichtshofes auf Rechts- und Sachfragen gemäss Abs. 3 wissen.

Die Beschwerdekommission für Verwaltungsangelegenheiten sowie der Verwaltungsgerichtshof dürfen nach Abs. 3 nur jene Punkte der Beschwerde aufgreifen, die in der Beschwerde vorgebracht wurden. D.h., der Prüfungsumfang beschränkt sich auf den Inhalt der Beschwerde im Sinne von Rechts- und Sachfragen, beispielsweise Rechtsverletzungen, unvollständiger Sachverhalt oder unrichtige Feststellung des Sachverhalts. Es können aber keine neuen Behauptungen oder Beweise vorgebracht werden und die Beschwerdekommission für Verwaltungsangelegenheiten bzw. der Verwaltungsgerichtshof sind nicht gehalten, alle sich stellenden rechtlichen Fragen zu untersuchen.

Die ausschliesslich rechtliche Überprüfung der Ausübung des Ermessens heisst, dass es grundsätzlich die Möglichkeit der gerichtlichen Überprüfung einer Ermessensentscheidung gibt. Diese muss aber in einem engen Rahmen stattfinden. Sie konzentriert sich allein darauf, ob der Behörde bei ihrer Entscheidung Fehler unterlaufen sind, sie also vom Ermessen im Sinne des Gesetzes Gebrauch gemacht hat. Eine weitergehende Überprüfung hätte andernfalls zur Folge, dass ein Gericht über einen individuellen Sachverhalt entschiede. Dessen Hintergründe sind ihm aber ebenso wenig bekannt wie ihm vergleichbare Fälle vertraut sind. Insofern steht es dem Gericht nicht zu, die Richtig- oder Unrichtigkeit der verwaltungsrechtlichen Entscheidung an sich zu überprüfen. Es darf vielmehr nur kontrollieren, ob die Verwaltung die Gesetze eingehalten oder Fehler bei der Entscheidung gemacht hat. Eine solche Nachprüfung der Ermessensbetätigung ist aber nur möglich, wenn seitens der Behörde eine nachvollziehbare Begründung erfolgt ist (vgl. VGH 2009/129). Nach der Rechtsprechung des Staatsgerichtshofes gilt, dass die Anforderungen an die Begründungsdichte u.a. umso höher sind, je grösser der Handlungsspielraum einer Behörde ist (vgl. StGH 2005/67).

Zu Art. 24 (neu)

Mit Art. 24 erhält die Regierung die Möglichkeit, die zur Durchführung dieses Gesetzes notwendigen Verordnungen zu erlassen.

Zu Art. 25 (neu)

Im Bericht und Antrag an den Landtag zur ersten Lesung war noch das gemeinsame Inkrafttreten mit dem EWR-Übernahmebeschluss betreffend die Richtlinie (EU) 2016/1148 sowie der Verordnung (EU) 2021/887 vorgesehen. Dabei wurde in den Erläuterungen bereits darauf hingewiesen, dass sich dieses Inkrafttreten im Hinblick auf die zweite Lesung, je nach Entwicklung des EWR-Übernahmeverfahrens, noch ändern könne.

Ein kürzlich erfolgter Austausch mit den EWR/EFTA-Staaten Island und Norwegen hat ergeben, dass es in einem der beiden Staaten zu nicht abschätzbaren zeitlichen Verzögerungen kommen wird.

Aus Sicht der Regierung ist es jedoch unbedingt erforderlich, dass die gegenständliche Gesetzesvorlage möglichst rasch in Kraft treten kann. Nur so kann sichergestellt werden, dass Liechtenstein im Bereich der Cyber-Sicherheit denselben Rechtsbestand aufweist wie die EU-Mitgliedstaaten. Zudem werden durch die gegenständliche Gesetzesvorlage die rechtlichen Grundlagen für die Tätigkeit der Stabsstelle Cyber-Sicherheit geschaffen und sichergestellt, dass der Zugang zu allen relevanten EU-Arbeitsgruppen und -gremien erhalten bleibt.

Im Weiteren wird auf die Ausführungen in Abschnitt 4.2.1 des Berichts und Antrags aus der ersten Lesung verwiesen.

Aus den ausgeführten Gründen wurde Art. 25 neu in die Gesetzesvorlage eingefügt.

Zu Art. 26

Mit der Einführung des Art. 25 musste Art. 26 (vormals Art. 24) entsprechend angepasst werden. Das Cyber-Sicherheitsgesetz soll somit am 1. Juli 2023 in Kraft treten.

II. ANTRAG DER REGIERUNG

Aufgrund der vorstehenden Ausführungen unterbreitet die Regierung dem Landtag den

A n t r a g ,

der Hohe Landtag wolle diese Stellungnahme zur Kenntnis nehmen und die beiliegende Gesetzesvorlage in Behandlung ziehen.

Genehmigen Sie, sehr geehrter Herr Landtagspräsident, sehr geehrte Frauen und Herren Abgeordnete, den Ausdruck der vorzüglichen Hochachtung.

REGIERUNG DES
FÜRSTENTUMS LIECHTENSTEIN

gez. Dr. Daniel Risch

III. REGIERUNGSVORLAGEN

Abänderungen in der überarbeiteten Vorlage mit Unterstreichungen versehen.

Cyber-Sicherheitsgesetz (CSG)

vom …

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I. Allgemeine Bestimmungen

Art. 1

Gegenstand und Geltungsbereich

1) Dieses Gesetz legt die Massnahmen fest, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll von:

a) Betreibern wesentlicher Dienste in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung sowie Digitale Infrastruktur; und

b) Anbietern digitaler Dienste.

2) Die in diesem Gesetz vorgesehenen Sicherheitsanforderungen und Meldepflichten gelten nicht für:

a) Unternehmen, die den Anforderungen nach Art. 40 und 41 der Richtlinie (EU) 2018/1972[5] unterliegen; und

b) Vertrauensdiensteanbieter, die den Anforderungen nach Art. 19 der Verordnung (EU) Nr. 910/2014[6] unterliegen.

Art. 2

Umsetzung und Durchführung von EWR-Rechtsvorschriften

1) Dieses Gesetz dient der Umsetzung bzw. Durchführung folgender EWR-Rechtsvorschriften:

a) Richtlinie (EU) 2016/1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union[7];

b) Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren[8].

2) Die gültige Fassung der EWR-Rechtsvorschriften, auf die in diesem Gesetz Bezug genommen wird, ergibt sich aus der Kundmachung der Beschlüsse des

---

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

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

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

[8] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1)

Gemeinsamen EWR-Ausschusses im Liechtensteinischen Landesgesetzblatt nach Art. 3 Bst. k des Kundmachungsgesetzes.

Art. 3

Begriffsbestimmungen und Bezeichnungen

1) Im Sinne dieses Gesetzes gelten als:

a) "Netz- und Informationssystem":

1. ein elektronisches Kommunikationsnetz im Sinne von Art. 3 Abs. 1 Ziff. 5 des Kommunikationsgesetzes;

2. eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen; oder

3. digitale Daten, die von den in Ziff. 1 und 2 genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

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

c) "NIS-Strategie" (Nationale Strategie für die Sicherheit von Netz- und Informationssystemen): ein Rahmen mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen auf nationaler Ebene;

d) "wesentlicher Dienst": ein Dienst:

1. der in einem der in Art. 1 Abs. 1 Bst. a genannten Sektoren erbracht wird;

2. der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung ist, insbesondere für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologien;

3. dessen Bereitstellung abhängig von Netz- und Informationssystemen ist; und

4. bei dem ein Sicherheitsvorfall mit tatsächlichen Auswirkungen auf die Sicherheit von Netz- und Informationssystemen eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken würde;

e) "Betreiber wesentlicher Dienste": eine öffentliche oder private Einrichtung mit Sitz in Liechtenstein, die einen wesentlichen Dienst erbringt;

f) "digitaler Dienst": ein Dienst im Sinne des Art. 3 Abs. 1 Bst. e des EWR-Notifikationsgesetzes, bei dem es sich um einen Online-Marktplatz, eine Online-Suchmaschine oder einen Cloud-Computing-Dienst handelt;

g) "Anbieter digitaler Dienste": eine juristische Person, die einen digitalen Dienst anbietet und die keine kleine Gesellschaft oder Kleinstgesellschaft im Sinne des Art. 1064 Abs. 1 und 1a des Personen- und Gesellschaftsrechts ist:

1. mit Sitz in Liechtenstein; oder

2. mit Sitz ausserhalb des Europäischen Wirtschaftsraums (EWR), die einen Vertreter nach Bst. h namhaft gemacht hat;

h) "Vertreter": eine natürliche oder juristische Person mit Wohnsitz oder Sitz in Liechtenstein, die ausdrücklich benannt wurde, um im Auftrag eines

Anbieters digitaler Dienste mit Sitz ausserhalb des EWR zu handeln, und an die sich die Stabsstelle Cyber-Sicherheit – statt an den Anbieter digitaler Dienste – hinsichtlich der Pflichten dieses Anbieters digitaler Dienste gemäss diesem Gesetz wenden kann;

i) "Sicherheitsvorfall": jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigen;

k) "Bewältigung von Sicherheitsvorfällen": alle Verfahren zur Unterstützung der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf;

l) "Risiko": alle mit vernünftigem Aufwand feststellbaren Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben;

m) "Kooperationsgruppe": ein nach Art. 11 der Richtlinie (EU) 2016/1148 eingerichtetes Gremium, das sich aus Vertretern der EWR-Mitgliedstaaten, der Europäischen Kommission und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zusammensetzt und der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den EWR-Mitgliedstaaten zum Aufbau von Vertrauen und zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen im EWR dient;

n) "CSIRTs-Netzwerk": ein nach Art. 12 der Richtlinie (EU) 2016/1148 eingerichtetes Gremium, das sich aus Vertretern der Computer-Notfallteams der EWR-Mitgliedstaaten und des europäischen Computer-Notfallteams zusammensetzt und zum Aufbau von Vertrauen zwischen den EWR-

Mitgliedstaaten beitragen und eine rasche und wirksame operative Zusammenarbeit fördern soll;

o) "Online-Marktplatz": ein digitaler Dienst, der es Verbrauchern oder Unternehmern ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern entweder auf der Internetseite des Online-Marktplatzes oder auf der Internetseite eines Unternehmers, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschliessen;

p) "Online-Suchmaschine": ein digitaler Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Internetseiten oder auf Internetseiten in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, und der daraufhin Links anzeigt, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können;

q) "Cloud-Computing-Dienst": ein digitaler Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht.

2) Unter den in diesem Gesetz verwendeten Personenbezeichnungen sind alle Personen unabhängig ihres Geschlechts zu verstehen, sofern sich die Personenbezeichnungen nicht ausdrücklich auf ein bestimmtes Geschlecht beziehen.

II. Sicherheitsanforderungen und Meldepflichten

A. Betreiber wesentlicher Dienste

Art. 4

Sicherheitsanforderungen

1) Betreiber wesentlicher Dienste ergreifen geeignete und verhältnismässige technische und organisatorische Massnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen.

2) Die Massnahmen nach Abs. 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist.

3) Betreiber wesentlicher Dienste ergreifen geeignete Massnahmen, um den Auswirkungen von Sicherheitsvorfällen, welche die Sicherheit der von ihnen für die Bereitstellung von Diensten genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit ihrer Dienste gewährleistet wird.

4) Die Pflichten nach Abs. 1 bis 3 finden keine Anwendung, wenn spezialgesetzliche Bestimmungen über Sicherheitsanforderungen bestehen, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme vorsehen.

5) Die Regierung kann das Nähere über die Sicherheitsanforderungen für Betreiber wesentlicher Dienste mit Verordnung regeln.

Art. 5

Meldepflicht

1) Betreiber wesentlicher Dienste haben einen Sicherheitsvorfall, der erhebliche Auswirkungen auf die Verfügbarkeit eines von ihnen bereitgestellten Dienstes hat oder der geeignet ist, sich erheblich auf die Verfügbarkeit eines von ihnen bereitgestellten Dienstes auszuwirken, unverzüglich der Stabsstelle Cyber-Sicherheit zu melden.

2) Die Meldung muss sämtliche relevante Angaben zum Sicherheitsvorfall und zu den technischen Rahmenbedingungen, die im Zeitpunkt der Erstmeldung bekannt sind, enthalten, insbesondere die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder Anlage. Angaben über später bekanntgewordene Umstände zum Sicherheitsvorfall sind in Nachmeldungen und letztendlich in einer Abschlussmeldung unverzüglich nach Feststellung der Umstände mitzuteilen.

3) Meldungen sind in einem gesicherten und soweit möglich standardisierten elektronischen Format zu übermitteln.

4) Nimmt ein Betreiber wesentlicher Dienste für die Bereitstellung eines wesentlichen Dienstes die Dienste eines Dritten als Anbieter digitaler Dienste in Anspruch, so ist jede Auswirkung auf die Verfügbarkeit dieser Dienste im Sinne des Abs. 1, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, vom Betreiber wesentlicher Dienste unverzüglich der Stabsstelle Cyber-Sicherheit zu melden.

5) Nach Anhörung des meldenden Betreibers wesentlicher Dienste kann die Stabsstelle Cyber-Sicherheit die Öffentlichkeit über konkrete Sicherheitsvorfälle

unterrichten, wenn die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist.

6) Die Pflichten nach Abs. 1 bis 5 finden keine Anwendung, wenn spezialgesetzliche Bestimmungen über die Meldepflicht bestehen und die Kriterien für die Meldepflicht mindestens gleichwertig sind. In diesen Fällen haben die Meldungsempfänger die bei ihnen eingegangenen Meldungen unverzüglich an die Stabsstelle Cyber-Sicherheit weiterzuleiten.

7) Die Regierung kann das Nähere über die Meldepflicht für Betreiber wesentlicher Dienste mit Verordnung regeln.

B. Anbieter digitaler Dienste

Art. 6
Sicherheitsanforderungen

1) Anbieter digitaler Dienste ergreifen geeignete und verhältnismässige technische und organisatorische Massnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung des digitalen Dienstes nutzen, zu bewältigen.

2) Die Massnahmen nach Abs. 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

a) der Sicherheit der Systeme und Anlagen;

b) der Bewältigung von Sicherheitsvorfällen;

c) dem Betriebskontinuitätsmanagement;

d) der Überwachung, Überprüfung und Erprobung;

e) der Einhaltung internationaler Normen.

3) Art. 4 Abs. 4 findet sinngemäss Anwendung.

Art. 7

Meldepflicht

1) Anbieter digitaler Dienste haben jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen im EWR erbrachten Dienstes hat, unverzüglich der Stabsstelle Cyber-Sicherheit zu melden.

2) Nach Anhörung des betreffenden Anbieters digitaler Dienste kann die Stabsstelle Cyber-Sicherheit die Öffentlichkeit über konkrete Sicherheitsvorfälle unterrichten oder verlangen, dass der Anbieter digitaler Dienste dies unternimmt, wenn:

a) die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist; oder

b) die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

3) Art. 5 Abs. 6 findet sinngemäss Anwendung.

C. Andere Einrichtungen

Art. 8

Freiwillige Meldung

1) Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und keine Anbieter digitaler Dienste sind, können Risiken und Sicherheitsvorfälle der Stabsstelle Cyber-Sicherheit melden.

2) Die freiwillige Meldung muss weder die Identität der Einrichtung noch Informationen, die auf diese schliessen lassen, enthalten.

III. Organisation und Durchführung

A. Allgemeines

Art. 9

Zuständigkeit

1) Mit der Durchführung dieses Gesetzes sind betraut:

a) die Stabsstelle Cyber-Sicherheit;

b) das Computer-Notfallteam (CSIRT).

2) Die Stabsstelle Cyber-Sicherheit und das CSIRT können zur Erfüllung ihrer Aufgaben qualifizierte Dritte beauftragen.

3) Die Regierung kann das Nähere über die Anforderungen an qualifizierte Dritte nach Abs. 2 mit Verordnung regeln.

Art. 10

Amtsgeheimnis

Die mit der Durchführung dieses Gesetzes betrauten Organe sowie allfällig durch diese beauftragte qualifizierte Dritte unterliegen dem Amtsgeheimnis und haben gegenüber anderen Amtsstellen und Personen über die in Ausübung dieser Tätigkeit gemachten Wahrnehmungen Stillschweigen zu bewahren und Einsicht in verarbeitete Daten und amtliche Akten zu verweigern. Art. 14 bleibt vorbehalten.

Art. 11

Verarbeitung und Offenlegung personenbezogener Daten

1) Die Stabsstelle Cyber-Sicherheit ist berechtigt, zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen bei der Wahrnehmung ihrer Aufgaben nach diesem Gesetz die erforderlichen personenbezogenen Daten nach Art. 4 Ziff. 1 der Verordnung (EU) 2016/679[9] zu verarbeiten.

2) Sie kann Daten nach Abs. 1, die ihr aufgrund der Wahrnehmung ihrer Aufgaben nach diesem Gesetz bekannt sind, in- und ausländischen Behörden und Stellen offenlegen, wenn:

a) dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz oder der Richtlinie (EU) 2016/1148 erforderlich ist;

b) die Vertraulichkeit der Daten gewährleistet ist; sowie

c) die Sicherheit und die geschäftlichen Interessen der Betreiber wesentlicher Dienste und der Anbieter digitaler Dienste geschützt sind.

---

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

B. Stabsstelle Cyber-Sicherheit

Art. 12

Zuständigkeit

1) Die Stabsstelle Cyber-Sicherheit ist die für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörde nach Art. 8 Abs. 1 der Richtlinie (EU) 2016/1148. Ihr obliegt die Aufsicht und der Vollzug dieses Gesetzes.

2) Die Stabsstelle Cyber-Sicherheit ist zudem die für die Sicherheit von Netz- und Informationssystemen zuständige zentrale Anlaufstelle nach Art. 8 Abs. 3 der Richtlinie (EU) 2016/1148. Sie ist die Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit internationalen Gremien und Gruppen, wie insbesondere den zuständigen Stellen in anderen EWR-Mitgliedstaaten, der Kooperationsgruppe und dem CSIRTs-Netzwerk.

Art. 13

Aufgaben

1) Die Stabsstelle Cyber-Sicherheit trifft die im Rahmen ihrer Zuständigkeit erforderlichen Massnahmen, um die Einhaltung dieses Gesetzes sicherzustellen. Ihr obliegen insbesondere:

a) die Überprüfung der Sicherheitsanforderungen nach Art. 4 und 6 sowie die Einhaltung der Meldepflichten nach Art. 5 und 7;

b) die Einrichtung und Koordination des CSIRT nach Art. 19;

c) die Entgegennahme und Analyse von Meldungen über Risiken oder Sicherheitsvorfälle, die Erstellung eines diesbezüglichen Lagebildes und Weiterleitung der Meldungen sowie des Lagebildes und zusätzlicher relevanter

Informationen an inländische Behörden oder andere betroffene Stellen bei Bedarf;

d) die Erstellung und Weitergabe von relevanten Informationen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen oder zur Vorbeugung von Sicherheitsvorfällen;

e) die Ermittlung der Betreiber wesentlicher Dienste sowie die Erstellung und regelmässige, mindestens jedoch einmal alle zwei Jahre, Überprüfung und Aktualisierung einer Liste mit wesentlichen Diensten;

f) die Unterrichtung und Weiterleitung von durch den Betreiber wesentlicher Dienste bereitgestellten Informationen an die zentrale Anlaufstelle der betroffenen EWR-Mitgliedstaaten, wenn ein Sicherheitsvorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in diesen EWR-Mitgliedsstaaten hat;

g) die Koordination der öffentlich-privaten Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen;

h) die Unterrichtung der Öffentlichkeit über Sicherheitsvorfälle, die Sensibilisierung der Öffentlichkeit zur Verhütung oder Bewältigung von Sicherheitsvorfällen sowie die Veröffentlichung allgemeiner Informationen im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen;

i) die Zusammenarbeit und der Informationsaustausch mit anderen inländischen Behörden und Stellen, insbesondere der Landespolizei, der Staatsanwaltschaft, der Datenschutzstelle, dem Amt für Informatik, dem Amt für Kommunikation, der Stabsstelle FIU und der Finanzmarktaufsicht Liechtenstein;

k) die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch mit den zuständigen Behörden und Stellen in

anderen EWR-Mitgliedstaaten, der ENISA, der Kooperationsgruppe und dem CSIRTs-Netzwerk;

l) die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch im Bereich der Sicherheit von Netz- und Informationssystemen mit den zuständigen Behörden und Stellen in Drittstaaten;

m) die Koordination der Erstellung einer NIS-Strategie nach Art. 20;

n) die Vertretung Liechtensteins in der Kooperationsgruppe, dem CSIRTs-Netzwerk sowie in anderen grenzüberschreitenden Gremien im EWR und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen.

2) Die Stabsstelle Cyber-Sicherheit kann nach Rücksprache mit dem zuständigen Regierungsmitglied mit anderen in- und ausländischen Behörden Vereinbarungen über die Modalitäten der Zusammenarbeit abschliessen sowie zur Aufgabenerfüllung mit Privaten im Rahmen von öffentlich-privaten Partnerschaften zusammenarbeiten.

3) Die Regierung kann das Nähere über die Aufgaben der Stabsstelle Cyber-Sicherheit mit Verordnung regeln.

Art. 14

Befugnisse gegenüber Betreibern wesentlicher Dienste

1) Die Stabsstelle Cyber-Sicherheit kann bei der Wahrnehmung ihrer Aufgaben nach diesem Gesetz von den Betreibern wesentlicher Dienste verlangen, dass sie ihr:

a) die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschliesslich der dokumentierten Sicherheitsmassnahmen, zur Verfügung stellen;

b) Nachweise für die wirksame Umsetzung der Sicherheitsmassnahmen erbringen;

c) Informationen, insbesondere technische und statistische Daten, zu statistischen Zwecken oder für die Erstellung konkreter Lagebilder unentgeltlich offenlegen.

2) Betreiber wesentlicher Dienste können die Offenlegung von Informationen nach Abs. 1 Bst. c nicht wegen Berufs-, Geschäfts- oder Betriebsgeheimnissen verweigern.

Art. 15

Befugnisse gegenüber Anbietern digitaler Dienste

Die Stabsstelle Cyber-Sicherheit kann, wenn ihr Nachweise vorliegen, dass Anbieter digitaler Dienste die Anforderungen nach diesem Gesetz nicht einhalten, von den Anbietern verlangen, dass sie ihr die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen nach Art. 2 Abs. 2 der Durchführungsverordnung (EU) 2018/151[10], einschliesslich der nachweislichen Sicherheitsmassahmen, unverzüglich zur Verfügung stellen.

Art. 16

Befugnisse bei Verstössen

1) Hat die Stabstelle Cyber-Sicherheit Anhaltspunkte dafür, dass ein Betreiber wesentlicher Dienste oder ein Anbieter digitaler Dienste gegen Vorschriften

[10] Durchführungsverordnung (EU) 2018/151 der Kommission vom 30. Januar 2018 über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls (ABl. L 26 vom 31.1.2018, S. 48)

dieses Gesetzes, der dazu erlassenen Verordnungen oder gegen darauf gestützte Entscheidungen oder Verfügungen verstösst, teilt sie dies dem Betreiber wesentlicher Dienste oder dem Anbieter digitaler Dienste vorbehaltlich Abs. 5 formlos mit und setzt ihm eine angemessene Frist, um:

a) zur Mitteilung Stellung zu nehmen; oder

b) den rechtmässigen Zustand herzustellen.

2) Die Stabsstelle Cyber-Sicherheit kann die Frist nach Abs. 1 Bst. b in begründeten Fällen auf Antrag angemessen verlängern, wenn der Betreiber wesentlicher Dienste oder der Anbieter digitaler Dienste dadurch voraussichtlich den rechtmässigen Zustand herstellt.

3) Handelt es sich beim Betreiber wesentlicher Dienste oder beim Anbieter digitaler Dienste um eine öffentliche Stelle oder eine Stelle, welche mit öffentlichen Aufgaben betraut ist, informiert die Stabsstelle Cyber-Sicherheit zusätzlich die Regierung über die Aufforderung nach Abs. 1.

4) Die Stabsstelle Cyber-Sicherheit informiert bei Anhaltspunkten zu Verstössen gegen Vorschriften dieses Gesetzes oder dazu erlassenen Verordnungen durch Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste die zuständige Aufsichtsbehörde und gibt dieser vor einer Aufforderung nach Abs. 1 Gelegenheit zur Stellungnahme.

5) Kommt ein Betreiber wesentlicher Dienste oder ein Anbieter digitaler Dienste der Aufforderung nach Abs. 1 nicht nach, so erlässt die Stabsstelle Cyber-Sicherheit eine entsprechende Verfügung; in dringenden Fällen kann auch ohne Aufforderung eine Verfügung erfolgen. Die Stabsstelle Cyber-Sicherheit informiert die zuständige Aufsichtsbehörde des Betreibers wesentlicher Dienste oder des Anbieters digitaler Dienste über die Entscheidung.

6) Die Verhängung von Bussen nach Art. 22 bleibt vorbehalten.

Art. 17

Betrieb von Informations- und Kommunikationstechnik-Lösungen (IKT-Lösungen)

Die Stabsstelle Cyber-Sicherheit ist zur Erfüllung ihrer Aufgaben berechtigt:

a) IKT-Lösungen zu betreiben oder durch Dritte betreiben zu lassen, die Risiken oder Sicherheitsvorfälle von Netz- und Informationssystemen frühzeitig erkennen;

b) IKT-Lösungen zu betreiben oder nach Einwilligung der betroffenen Einrichtung zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen.

Art. 18

Kontrolle

1) Die Stabsstelle Cyber-Sicherheit kann Kontrollen zur Einhaltung der Anforderungen nach diesem Gesetz durchführen oder durch von ihr beauftragte qualifizierte Dritte durchführen lassen.

2) Zur Durchführung von Kontrollen können die Stabsstelle Cyber-Sicherheit oder von ihr beauftragte qualifizierte Dritte Einsicht in die Netz- und Informationssysteme, die für die Bereitstellung wesentlicher Dienste und Anbieter digitaler Dienste genutzt werden, und diesbezügliche Unterlagen nehmen. Dabei sind sie berechtigt, Örtlichkeiten, in welchen Netz- und Informationssysteme gelegen sind, zu betreten. Die Ausübung der Einsicht hat verhältnismässig zu erfolgen und ist unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter sowie des Betriebs auszuüben.

3) Die Regierung kann das Nähere über die Durchführung von Kontrollen mit Verordnung regeln.

C. Computer-Notfallteam (CSIRT)

Art. 19

Zweck und Aufgaben

1) Zur Gewährleistung der Sicherheit von Netz- und Informationssystemen wird bei der Stabsstelle Cyber-Sicherheit ein CSIRT eingerichtet. Ihm obliegen insbesondere:

a) gegebenenfalls das zur Verfügung stellen von zur Bewältigung eines Sicherheitsvorfalls nützlichen Informationen nach Eingang von Meldungen über Risiken oder Sicherheitsvorfälle nach Art. 5, 7 und 8;

b) die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und Verbreitung von Informationen über Risiken und Sicherheitsvorfälle unter den einschlägigen Interessenträgern;

c) die erste allgemeine Unterstützung bei der Reaktion auf einen Sicherheitsvorfall;

d) die Beobachtung und Analyse von Risiken und Sicherheitsvorfällen sowie die Lagebeurteilung;

e) die Beteiligung am CSIRTs-Netzwerk.

2) Das CSIRT kann die Aufgaben nach Abs. 1 Bst. a bis d auch gegenüber sonstigen Einrichtungen oder Personen wahrnehmen, wenn diese von einem Risiko oder einem Sicherheitsvorfall ihrer Netz- und Informationssysteme betroffen sind.

3) Die Regierung kann das Nähere über den Zweck und die Aufgaben des CSIRT mit Verordnung regeln.

D. NIS-Strategie

Art. 20

Grundsatz

1) Die NIS-Strategie bestimmt insbesondere die strategischen Ziele und angemessenen Politik- und Regulierungsmassnahmen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll.

2) Die Stabsstelle Cyber-Sicherheit teilt die NIS-Strategie der EFTA-Überwachungsbehörde innerhalb von drei Monaten nach ihrer Festlegung mit. Elemente der Strategie, die die nationale Sicherheit berühren, sind nicht mitzuteilen.

3) Die NIS-Strategie ist von der Regierung zu genehmigen. Sie wird nach der Genehmigung auf der Internetseite der Stabsstelle Cyber-Sicherheit veröffentlicht.

IV. Rechtsmittel

Art. 21

Beschwerde

1) Gegen Entscheidungen und Verfügungen der Stabsstelle Cyber-Sicherheit kann binnen 14 Tagen ab Zustellung Beschwerde bei der Beschwerdekommission für Verwaltungsangelegenheiten erhoben werden.

2) Gegen Entscheidungen und Verfügungen der Beschwerdekommission für Verwaltungsangelegenheiten kann binnen 14 Tagen ab Zustellung Beschwerde an den Verwaltungsgerichtshof erhoben werden.

3) Die Überprüfungsbefugnis der Beschwerdekommission für Verwaltungsangelegenheiten sowie des Verwaltungsgerichtshofes beschränkt sich auf Rechts- und Sachfragen. Die Ausübung des Ermessens wird ausschliesslich rechtlich überprüft.

4) Im Übrigen finden auf das Verfahren die Bestimmungen des Gesetzes über die allgemeine Landesverwaltungspflege Anwendung.

V. Strafbestimmungen

Art. 22

Verwaltungsübertretungen

1) Von der Stabsstelle Cyber-Sicherheit wird, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, wegen Übertretung mit Busse bis zu 100 000 Franken bestraft, wer:

a) als Betreiber wesentlicher Dienste nicht die vorgeschriebenen Massnahmen nach Art. 4 Abs. 1 bis 3 ergreift;

b) als Betreiber wesentlicher Dienste die Meldepflicht nach Art. 5 Abs. 1 bis 4 verletzt;

c) als Anbieter digitaler Dienste nicht die vorgeschriebenen Massnahmen nach Art. 6 Abs. 1 und 2 ergreift;

d) als Anbieter digitaler Dienste die Meldepflicht nach Art. 7 Abs. 1 verletzt;

e) als Betreiber wesentlicher Dienste die nach Art. 14 Abs. 1 Bst. a erforderlichen Informationen, einschliesslich der dokumentierten Sicherheitsmassnahmen, nicht zur Verfügung stellt;

f) als Betreiber wesentlicher Dienste Nachweise nach Art. 14 Abs. 1 Bst. b nicht erbringt;

g) als Betreiber wesentlicher Dienste Informationen nach Art. 14 Abs. 1 Bst. c gegenüber der Stabsstelle Cyber-Sicherheit nicht offenlegt;

h) als Anbieter digitaler Dienste die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme nach Art. 15 erforderlichen Informationen, einschliesslich der nachweislichen Sicherheitsmassahmen, nicht unverzüglich zur Verfügung stellt;

i) als Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste die ordnungsgemässe Durchführung einer Kontrolle nach Art. 18 erschwert, behindert oder verunmöglicht;

k) als Betreiber wesentlicher Dienste oder als Anbieter digitaler Dienste gegen eine rechtskräftige Verfügung oder Entscheidung der Stabsstelle Cyber-Sicherheit verstösst.

2) Bei fahrlässiger Begehung wird die Strafobergrenze nach Abs. 1 auf die Hälfte herabgesetzt. Im Wiederholungsfall verdoppelt sich die Strafobergrenze.

Art. 23

Verantwortlichkeit

Werden strafbare Handlungen im Geschäftsbetrieb einer juristischen Person, einer Personengesellschaft oder einer Einzelfirma begangen, so finden die Strafbestimmungen auf die Personen Anwendung, die für sie gehandelt haben oder hätten handeln sollen, jedoch unter solidarischer Mithaftung der juristischen Person, der Personengesellschaft oder der Einzelfirma für die Bussen und Kosten.

VI. Schlussbestimmungen

Art. 24

Durchführungsverordnungen

Die Regierung erlässt die zur Durchführung dieses Gesetzes notwendigen Verordnungen.

Art. 25

Anwendbarkeit von EU-Rechtsvorschriften

1) Bis zu ihrer Übernahme in das EWR-Abkommen gelten als nationale Rechtsvorschriften:

a) die Richtlinie (EU) 2016/1148 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union;

b) die Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenz-zentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren;

c) die Durchführungsrechtsakte zu den EU-Rechtsvorschriften nach Bst. a und b.

2) Der vollständige Wortlaut der in Abs. 1 genannten Rechtsvorschriften ist im Amtsblatt der Europäischen Union unter https://eur-lex.europa.eu veröffentlicht; er kann auf der Internetseite der Stabsstelle Cyber-Sicherheit unter https://scs.llv.li abgerufen werden.

Art. 26

Inkrafttreten

1) Dieses Gesetz tritt unter Vorbehalt des ungenutzten Ablaufs der Referendumsfrist am 1. Juli 2023 in Kraft, andernfalls am Tag nach der Kundmachung.

2) Art. 2 Abs. 1 Bst. a tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses Nr. 21/2023 vom 3. Februar 2023 zur Änderung von Anhang XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) des EWR-Abkommens in Kraft.

3) Art. 2 Abs. 1 Bst. b tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses Nr. 27/2023 vom 3. Februar 2023 zur Änderung von Protokoll 31 (Zusammenarbeit in bestimmten Bereichen ausserhalb der vier Freiheiten) des EWR-Abkommens in Kraft.

Gesetz

vom …

über die Abänderung des Beschwerdekommissionsgesetzes

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I.

Abänderung bisherigen Rechts

Das Beschwerdekommissionsgesetz vom 25. Oktober 2000, LGBl. 2000 Nr. 248, wird wie folgt abgeändert:

Art. 4 Abs. 1 Bst. w

1) Die Beschwerdekommission ist zuständig für Beschwerden gegen Verfügungen und Entscheidungen im Bereich:

w) Cyber-Sicherheit:

der Stabsstelle Cyber-Sicherheit aufgrund des Cyber-Sicherheitsgesetzes sowie der darauf gestützten Verordnungen.

II.

Inkrafttreten

Dieses Gesetz tritt gleichzeitig mit dem Cyber-Sicherheitsgesetz vom … in Kraft.

I

(Gesetzgebungsakte)

RICHTLINIEN

RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 6. Juli 2016

über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten und insbesondere für das Funktionieren des Binnenmarkts ist es von entscheidender Bedeutung, dass sie verlässlich und sicher sind.

(2) Die Tragweite, Häufigkeit und Auswirkungen von Sicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Diese Systeme können auch zu einem Angriffsziel vorsätzlich schädigender Handlungen werden, die auf die Störung oder den Ausfall des Betriebs der Systeme gerichtet sind. Solche Sicherheitsvorfälle können die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, beträchtliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft der Union großen Schaden zufügen.

(3) Netz- und Informationssysteme, allen voran das Internet, spielen eine tragende Rolle bei der Erleichterung des grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehrs. Aufgrund dieses transnationalen Charakters können schwere Störungen solcher Systeme — unabhängig davon, ob sie beabsichtigt oder unbeabsichtigt sind und wo sie auftreten — einzelne Mitgliedstaaten und die Union insgesamt in Mitleidenschaft ziehen. Sichere Netz- und Informationssysteme sind daher unerlässlich für das reibungslose Funktionieren des Binnenmarkts.

(4) Auf der Grundlage der beträchtlichen Fortschritte, die im Rahmen des Europäischen Forums der Mitgliedstaaten zur Förderung von Gesprächen und des Austauschs bewährter Vorgehensweisen, unter anderem zur Entwicklung von Grundsätzen für die europäische Zusammenarbeit bei Cyberkrisen, erzielt worden sind, sollte eine Kooperationsgruppe aus Vertretern der Mitgliedstaaten, der Kommission und der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) eingesetzt werden, um die strategische Zusammenarbeit

([1]) ABl. C 271vom 19.9.2013, S. 133.
([2]) Standpunkt des Europäischen Parlaments vom 13. März 2014 (noch nicht im Amtsblatt veröffentlicht)] und Standpunkt des Rates in erster Lesung vom 17. Mai 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 6. Juli 2016 (noch nicht im Amtsblatt veröffentlicht).

zwischen den Mitgliedstaaten im Bereich der Sicherheit von Netz- und Informationssystemen zu unterstützen und zu erleichtern. Damit eine solche Gruppe wirksam sein kann und alle Beteiligten einbezogen werden, muss jeder Mitgliedstaat über Minimalfähigkeiten und eine Strategie verfügen, die in seinem Hoheitsgebiet ein hohes Sicherheitsniveau von Netz- und Informationssystemen gewährleisten. Außerdem sollten für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste Sicherheitsanforderungen und Meldepflichten gelten, damit eine Kultur des Risikomanagements gefördert wird und sichergestellt ist, dass die gravierendsten Sicherheitsvorfälle gemeldet werden.

(5) Die bestehenden Fähigkeiten reichen nicht aus, um ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der Union zu gewährleisten. Aufgrund des sehr unterschiedlichen Niveaus der Abwehrbereitschaft verfolgen die Mitgliedstaaten uneinheitliche Ansätze innerhalb der Union. Dies führt dazu, dass Verbraucher und Unternehmen ein unterschiedliches Schutzniveau genießen und die Sicherheit von Netz- und Informationssystemen in der Union generell untergraben wird. Wegen fehlender gemeinsamer Anforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste kann wiederum kein umfassender, wirksamer Mechanismus für die Zusammenarbeit auf Unionsebene geschaffen werden. Universitäten und Forschungszentren müssen eine entscheidende Rolle spielen, wenn es darum geht, Forschung, Entwicklung und Innovationen in diesen Bereichen voranzutreiben.

(6) Um wirksam auf die Herausforderungen im Bereich der Sicherheit von Netz- und Informationssystemen reagieren zu können, ist deshalb ein umfassender Ansatz auf Unionsebene erforderlich, der gemeinsame Mindestanforderungen für Kapazitätsaufbau und -planung, Informationsaustausch, Zusammenarbeit sowie gemeinsame Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beinhaltet. Jedoch sind Betreiber wesentlicher Dienste und Anbieter digitaler Dienste nicht daran gehindert, strengere Sicherheitsmaßnahmen anzuwenden, als sie in dieser Richtlinie vorgesehen sind.

(7) Um alle einschlägigen Vorfälle und Risiken abdecken zu können, sollte diese Richtlinie sowohl für Betreiber wesentlicher Dienste als auch für Anbieter digitaler Dienste gelten. Die den Betreibern wesentlicher Dienste und den Anbietern digitaler Dienste auferlegten Verpflichtungen sollten hingegen nicht für Unternehmen gelten, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates ([1]) bereitstellen und die den besonderen Sicherheits- und Integritätsanforderungen jener Richtlinie unterliegen; die Verpflichtungen sollten auch nicht für Vertrauensdiensteanbieter im Sinne der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([2]) gelten, die den Sicherheitsanforderungen jener Verordnung unterliegen.

(8) Die Möglichkeit der Mitgliedstaaten, die für die Wahrung seiner wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, sollte von dieser Richtlinie unberührt bleiben. Nach Artikel 346 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht. In diesem Zusammenhang sind der Beschluss 2013/488/EU des Rates ([3]) sowie Geheimhaltungsvereinbarungen oder informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol (TLP) von Bedeutung.

(9) Für bestimmte Wirtschaftssektoren gelten bereits sektorspezifische Rechtsakte der Union, die Vorschriften im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen beinhalten; für weitere Wirtschaftssektoren kann dies künftig der Fall sein. Wann immer solche Unionsrechtsakte Bestimmungen enthalten, mit denen Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen oder die Meldung von Sicherheitsvorfällen auferlegt werden, sollten diese Bestimmungen gelten, wenn sie Anforderungen vorsehen, die hinsichtlich ihrer Wirkung den in dieser Richtlinie enthaltenen Verpflichtungen mindestens gleichwertig sind. Die Mitgliedstaaten sollten dann die Bestimmungen des betreffenden sektorspezifischen Unionsrechtsakts anwenden, einschließlich der Bestimmungen über die gerichtliche Zuständigkeit, und nicht das in dieser Richtlinie festgelegte Verfahren zur Ermittlung der Betreiber wesentlicher Dienste durchführen. In diesem Zusammenhang sollten die Mitgliedstaaten die Kommission über die Anwendung solcher Lex-specialis-Bestimmungen unterrichten. Bei der Feststellung, ob die in sektorspezifischen Unionsrechtsakten enthaltenen Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen und die Meldung von Sicherheitsvorfällen den in dieser Richtlinie enthaltenen Anforderungen gleichwertig sind, sollten ausschließlich die Bestimmungen der einschlägigen Unionsrechtsakte und ihre Anwendung in den Mitgliedstaaten berücksichtigt werden.

(10) Im Bereich der Schifffahrt umfassen die Sicherheitsanforderungen für Unternehmen, Schiffe, Hafeneinrichtungen, Häfen und Schiffsverkehrsdienste nach Rechtsakten der Union sämtliche Tätigkeiten einschließlich der Funk- und Telekommunikationssysteme, Computersysteme und Netze. Ein Teil der verbindlichen Verfahren beinhaltet das Melden sämtlicher Vorfälle und sollte daher insoweit als Lex specialis betrachtet werden, als diese Anforderungen den entsprechenden Bestimmungen dieser Richtlinie mindestens gleichwertig sind.

([1]) Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) (ABl. L 108 vom 24.4.2002, S. 33).

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

([3]) Beschluss 2013/488/EU des Rates vom 23. September 2013 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 274 vom 15.10.2013, S. 1).

(11) Bei der Ermittlung von Betreibern im Schifffahrtsektor sollten die Mitgliedstaaten den geltenden und künftigen internationalen Codes und Leitlinien Rechnung tragen, insbesondere den von der Internationalen Seeschifffahrtsorganisation ausgearbeiteten, um einzelnen Betreibern gegenüber ein kohärentes Vorgehen zu gewährleisten.

(12) Die Regulierung und die Aufsicht in den Sektoren der Banken- und Finanzmarktinfrastrukturen sind auf Unionsebene durch die Verwendung des Primär- und Sekundärrechts der Union sowie der Normen, die gemeinsam mit den Europäischen Aufsichtsbehörden ausgearbeitet wurden, in hohem Maße harmonisiert. Innerhalb der Bankenunion werden die Anwendung und die Beaufsichtigung dieser Anforderungen durch den Einheitlichen Aufsichtsmechanismus sichergestellt. In Mitgliedstaaten, die nicht Teil der Bankenunion sind, gewährleisten dies die einschlägigen Bankenaufsichtsbehörden der Mitgliedstaaten. Darüber hinaus sorgt in anderen Bereichen der Regulierung des Finanzsektors das Europäische Finanzaufsichtssystem für ein hohes Maß an Gemeinsamkeit und Annäherung bei der Aufsichtspraxis. Die Europäische Wertpapier- und Marktaufsichtsbehörde übt außerdem die direkte Aufsicht über bestimmte Einrichtungen, d. h. über Kreditratingagenturen und Transaktionsregister aus.

(13) Das operationelle Risiko macht einen großen Teil der Aufsichtsvorschriften und der Kontrolle in den Sektoren Banken- und Finanzmarktinfrastrukturen aus. Davon erfasst sind sämtliche Tätigkeiten einschließlich der Sicherheit, Integrität und Robustheit von Netz- und Informationssystemen. Die Anforderungen für diese Systeme, die oft über die Anforderungen aus dieser Richtlinie hinausgehen, sind in einer Reihe von Unionsrechtsakten festgelegt; hierzu zählen unter anderem: Vorschriften über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen und Vorschriften über die Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen, die Anforderungen zum operationellen Risiko enthalten, Vorschriften über Märkte für Finanzinstrumente, die Anforderungen zur Risikobewertung für Wertpapierfirmen und für geregelte Märkte enthalten, Vorschriften über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, die Anforderungen zum operationellen Risiko für zentrale Gegenparteien und Transaktionsregister enthalten, sowie Vorschriften zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Union und über Zentralverwahrer, die ebenfalls Anforderungen zum operationellen Risiko enthalten. Darüber hinaus sind Anforderungen in Bezug auf die Meldung von Sicherheitsvorfällen Teil der üblichen Aufsichtspraxis im Finanzsektor und sind oft in den Handbüchern über die Aufsicht enthalten. Die Mitgliedstaaten sollten bei ihrer Anwendung der Lex specialis diesen Regeln und Anforderungen Rechnung tragen.

(14) Wie die Europäische Zentralbank in ihrer Stellungnahme vom 25. Juli 2014 [1] festgestellt hat, berührt die Richtlinie nicht die bestehenden unionsrechtlichen Bestimmungen zur Überwachung von Zahlungsverkehrs- und Abwicklungssystemen durch das Eurosystem. Die für eine derartige Überwachung verantwortlichen Behörden sollten ihre Erfahrungen in Angelegenheiten der Sicherheit von Netz- und Informationssystemen mit den nach dieser Richtlinie zuständigen Behörden austauschen. Gleiches gilt für die Mitgliedstaaten, die zwar nicht Mitglied des Euroraums, wohl aber des Europäischen Systems der Zentralbanken sind, und die eine Überwachung der Zahlungsverkehrs- und Abwicklungssysteme auf der Grundlage nationaler Gesetze und Vorschriften vornehmen.

(15) Ein Online-Marktplatz ermöglicht es Verbrauchern und Unternehmern, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern abzuschließen, und ist der endgültige Bestimmungsort für den Abschluss dieser Verträge. Er sollte sich nicht auf Online-Dienste erstrecken, die lediglich als Vermittler für Drittdienste fungieren, durch die letztlich ein Vertrag geschlossen werden kann. Er sollte sich deshalb nicht auf Online-Dienste erstrecken, die die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern miteinander vergleichen und den Nutzer anschließend an den bevorzugten Unternehmer weiterleiten, damit er das Produkt dort kauft. Die von dem Online-Marktplatz bereitgestellten IT-Dienste können die Verarbeitung von Transaktionen, die Aggregation von Daten oder die Erstellung von Nutzerprofilen einschließen. Als Online Stores tätige Application Stores, die den digitalen Vertrieb von Anwendungen oder Software-Programmen von Dritten ermöglichen, sollten als eine Art Online-Marktplatz betrachtet werden.

(16) Eine Online-Suchmaschine ermöglicht es dem Nutzer, Suchen grundsätzlich auf allen Websites anhand einer Abfrage zu einem beliebigen Thema vorzunehmen. Sie kann alternativ dazu auf Websites in einer bestimmten Sprache beschränkt sein. Die Definition des Begriffs „Online-Suchmaschine" in dieser Richtlinie sollte sich nicht auf Suchfunktionen erstrecken, die auf den Inhalt einer bestimmten Website beschränkt sind, unabhängig davon, ob die Suchfunktion durch eine externe Suchmaschine bereitgestellt wird. Sie sollte sich auch nicht auf Online-Dienste erstrecken, die die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern miteinander vergleichen und den Nutzer anschließend an den bevorzugten Unternehmer weiterleiten, damit er das Produkt dort kauft.

(17) Cloud-Computing-Dienste umfassen eine breite Palette von Tätigkeiten, die auf unterschiedliche Weise erbracht werden können. Für die Zwecke dieser Richtlinie sind unter dem Begriff „Cloud-Computing-Dienste" Dienste zu verstehen, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Speicher, Anwendungen und Dienste. Der Begriff „skalierbar" bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastischer Pool" wird verwendet, um die Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die verfügbaren

[1] ABl. C 352 vom 7.10.2014, S. 4.

Ressourcen je nach Arbeitsaufkommen rasch auf- bzw. abgebaut werden können. Der Begriff „gemeinsam nutzbar" wird verwendet, um die Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst von derselben elektronischen Einrichtung erbracht wird.

(18) Die Funktion eines Internet-Knotens (IXP) besteht in der Zusammenschaltung von Netzen. Ein IXP ermöglicht keinen Netzzugang und fungiert weder als Transit-Anbieter noch als Carrier. Ein IXP erbringt auch keine anderen Dienste, die in keinem Zusammenhang mit der Zusammenschaltung stehen, was einen IXP-Betreiber jedoch nicht daran hindert, Dienste anzubieten, bei denen dieser Zusammenhang nicht gegeben ist. Ein IXP dient zur Zusammenschaltung von Netzen, die technisch und organisatorisch getrennt sind. Der Begriff „autonomes System" wird verwendet, um ein in technischer Hinsicht eigenständiges Netz zu beschreiben.

(19) Die Mitgliedstaaten sollten dafür zuständig sein, zu ermitteln, welche Einrichtungen die Kriterien der Definition des Begriffs „Betreiber wesentlicher Dienste" erfüllen. Damit ein einheitlicher Ansatz gewährleistet ist, sollte die Definition des Begriffs „Betreiber wesentlicher Dienste" in allen Mitgliedstaaten kohärent angewendet werden. Hierzu sieht diese Richtlinie Folgendes vor: Bewertung der Einrichtungen, die in spezifischen Sektoren und Teilsektoren tätig sind; Festlegung einer Liste wesentlicher Dienste; Prüfung einer gemeinsamen Liste sektorübergreifender Faktoren, um zu bestimmen, ob ein potenzieller Sicherheitsvorfall eine erhebliche Störung bewirken würde; Konsultationsprozess unter Einbeziehung der betreffenden Mitgliedstaaten im Falle von Einrichtungen, die in mehr als einem Mitgliedstaat Dienste erbringen, sowie Unterstützung der Kooperationsgruppe im Rahmen des Verfahrens der Ermittlung. Damit dafür gesorgt ist, dass etwaige Marktveränderungen genau berücksichtigt werden, sollte die Liste der ermittelten Betreiber von den Mitgliedstaaten regelmäßig überprüft und bei Bedarf aktualisiert werden. Ferner sollten die Mitgliedstaaten der Kommission die Informationen vorlegen, die erforderlich sind, um zu bewerten, inwieweit diese gemeinsame Methodik eine einheitliche Anwendung der Begriffsbestimmung durch die Mitgliedstaaten ermöglicht hat.

(20) Während des Verfahrens zur Ermittlung von Betreibern wesentlicher Dienste sollten die Mitgliedstaaten zumindest für jeden in dieser Richtlinie genannten Teilsektor beurteilen, welche Dienste als für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten wesentlich zu betrachten sind, und beurteilen, ob die Einrichtungen, die in den Sektoren und Teilsektoren im Rahmen dieser Richtlinie aufgeführt sind und diese Dienste erbringen, die Kriterien zur Ermittlung der Betreiber erfüllen. Bei der Beurteilung, ob eine Einrichtung einen Dienst erbringt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten wesentlich ist, sollte ausreichen, dass geprüft wird, ob die betreffende Einrichtung einen Dienst erbringt, der in der Liste der wesentlichen Dienste aufgeführt ist. Außerdem sollte dargelegt werden, dass die Erbringung des wesentlichen Dienstes von Netz- und Informationssystemen abhängt. Ferner sollten die Mitgliedstaaten bei der Beurteilung, ob ein Sicherheitsvorfall erhebliche Störungen der Bereitstellung des Dienstes bewirken würde, eine Reihe von sektorübergreifenden Faktoren und gegebenenfalls auch sektorspezifische Faktoren berücksichtigen.

(21) Für die Zwecke der Ermittlung von Betreibern wesentlicher Dienste setzt eine Niederlassung in einem Mitgliedstaat die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich.

(22) Es ist möglich, dass Einrichtungen in den in dieser Richtlinie aufgeführten Sektoren und Teilsektoren sowohl wesentliche als auch nicht wesentliche Dienste erbringen. Beispielsweise erbringen im Luftverkehrssektor die Flughäfen Dienste, die von einem Mitgliedstaat als wesentlich betrachtet werden könnten, wie etwa das Start-und Landebahn-Management, jedoch auch eine Reihe von Diensten, die als nicht wesentlich betrachtet werden könnten, wie die Bereitstellung von Einkaufsbereichen. Betreiber wesentlicher Dienste sollten den spezifischen Sicherheitsanforderungen nur in Bezug auf die als wesentlich geltenden Dienste unterworfen sein. Zum Zwecke der Ermittlung von Betreibern sollten die Mitgliedstaaten deshalb eine Liste der Dienste erstellen, die als wesentlich betrachtet werden.

(23) Die Liste der Dienste sollte alle im Hoheitsgebiet eines Mitgliedstaats erbrachten Dienste enthalten, die die Anforderungen nach dieser Richtlinie erfüllen. Der betreffende Mitgliedstaat sollte die Möglichkeit haben, das bestehende Verzeichnis zu ändern, indem er neue Dienste aufnimmt. Die Liste der Dienste sollte den Mitgliedstaaten als Bezugspunkt für die Ermittlung von Betreibern wesentlicher Dienste dienen. Zweck der Liste ist es, die in einem bestimmten in dieser Richtlinie genannten Sektor als wesentlich geltenden Arten von Diensten auszuweisen und sie damit von den nicht wesentlichen Tätigkeiten abzugrenzen, für die eine in einem beliebigen Sektor tätige Einrichtung zuständig sein könnte. Die von jedem Mitgliedstaat erstellte Liste der Dienste wäre ein weiterer Beitrag zur Beurteilung der Regelungspraxis der einzelnen Mitgliedstaaten im Hinblick auf das Ziel, ein insgesamt kohärentes Verfahren der Ermittlung auf der Ebene der Mitgliedstaaten zu gewährleisten.

(24) Bietet eine Einrichtung einen wesentlichen Dienst in zwei oder mehr Mitgliedstaaten an, sollten diese Mitgliedstaaten zur Ermittlung des Betreibers untereinander bilaterale oder multilaterale Beratungen aufnehmen. Dieser Konsultationsprozess soll ihnen dabei helfen, die kritische Rolle des Betreibers im Hinblick auf grenzüberschreitende Auswirkungen zu beurteilen, und soll somit jedem beteiligten Mitgliedstaat ermöglichen, sich zu den Risiken zu äußern, die seiner Ansicht nach mit den angebotenen Diensten verbunden sind. Die betroffenen Mitgliedstaaten sollten den Ansichten der jeweils anderen Mitgliedstaaten in diesem Verfahren Rechnung tragen, und sie sollten in diesem Zusammenhang die Unterstützung der Kooperationsgruppe anfordern können.

(25) Als Ergebnis des Ermittlungsprozesses sollten die Mitgliedstaaten nationale Maßnahmen erlassen, in denen bestimmt wird, welche Einrichtungen Pflichten im Zusammenhang mit Netz- und Informationssystemen unterliegen. Dies könnte durch die Festlegung eines Verzeichnisses sämtlicher Betreiber wesentlicher Dienste oder durch die Annahme nationaler Maßnahmen einschließlich objektiv quantifizierbarer Kriterien wie beispielsweise Leistung des Betreibers oder Anzahl der Nutzer erfolgen, die die Festlegung derjenigen Einrichtungen ermöglichen, die Pflichten im Hinblick auf Netz- und Informationssysteme unterliegen. Die nationalen Maßnahmen, gleich, ob sie bereits gelten oder im Rahmen dieser Richtlinie angenommen werden, sollten sämtliche rechtlichen und administrativen Maßnahmen und Strategien umfassen, die die Ermittlung von Betreibern wesentlicher Dienste im Sinne dieser Richtlinie ermöglichen.

(26) Als Indikator für die Bedeutung der ermittelten Betreiber wesentlicher Dienste für den jeweiligen Sektor sollten die Mitgliedstaaten der Anzahl und der Größe dieser Betreiber Rechnung tragen, beispielsweise gemessen an deren Marktanteil oder der produzierten oder transportierten Datenmenge, ohne dabei verpflichtet zu sein, Informationen preiszugeben, aus denen hervorgeht, welche Betreiber ermittelt wurden.

(27) Um festzustellen, ob ein Sicherheitsvorfall zu erheblichen Störungen bei der Bereitstellung eines wesentlichen Dienstes führen würde, sollten die Mitgliedstaaten eine Reihe unterschiedlicher Faktoren berücksichtigen, wie die Anzahl der Nutzer, die diesen Dienst zu privaten oder beruflichen Zwecken in Anspruch nehmen. Die Nutzung dieses Dienstes kann unmittelbar, mittelbar oder durch Vermittlung erfolgen. Bei der Beurteilung, in welchem Ausmaß und wie lange sich ein Sicherheitsvorfall auf wirtschaftliche und gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit auswirken könnte, sollten die Mitgliedstaaten außerdem die Zeitspanne abschätzen, die voraussichtlich vergeht, bevor die Unterbrechung nachteilige Auswirkungen hätte.

(28) Zusätzlich zu den sektorübergreifenden Faktoren sollten auch sektorspezifische Faktoren berücksichtigt werden, um zu bestimmen, ob ein Sicherheitsvorfall zu erheblichen Störungen bei der Bereitstellung eines Dienstes führen würde. Bei Energieversorgern könnten hierzu die Menge oder der Anteil der landesweit produzierten Energie gehören, bei Öllieferanten die Fördermenge pro Tag, beim Luftverkehr, einschließlich Flughäfen und Luftfahrtunternehmen, Schienenverkehr und bei Seehäfen der Anteil des landesweiten Verkehrsvolumens und die Anzahl der Passagiere oder der Frachtdienste pro Jahr, bei Bank- oder Finanzmarktinfrastrukturen deren Systemrelevanz aufgrund der Bilanzsumme oder des Anteils dieser Bilanzsumme am BIP, im Gesundheitsbereich die Anzahl der vom Anbieter jährlich versorgten Patienten, bei der Wassergewinnung, -aufbereitung und -versorgung die Wassermenge, die Anzahl und die Arten der belieferten Verbraucher, einschließlich beispielsweise Krankenhäuser, öffentliche Dienstleister oder Einzelpersonen sowie das Vorhandensein alternativer Wasserquellen zur Versorgung desselben geografischen Gebiets.

(29) Um ein hohes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen und aufrechtzuerhalten, sollte jeder Mitgliedstaat über eine nationale Strategie zur Sicherheit von Netz- und Informationssystemen verfügen, in der die strategischen Ziele sowie konkrete politische Maßnahmen vorgesehen sind.

(30) Angesichts der unterschiedlichen nationalen Verwaltungsstrukturen und zur Beibehaltung bereits bestehender sektorbezogener Vereinbarungen oder von Aufsichts- oder Regulierungsstellen der Union sowie zur Vermeidung von Doppelarbeit sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste gemäß dieser Richtlinie verantwortlich sind.

(31) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation und um die effektive Umsetzung dieser Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat unbeschadet sektorbezogener regulatorischer Vereinbarungen eine nationale zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der Sicherheit von Netz-und Informationssystemen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist. Die zuständigen Behörden und die zentralen Anlaufstellen sollten mit angemessenen technischen, finanziellen und personellen Ressourcen ausgestattet sein, um die ihnen übertragenen Aufgaben wirksam und effizient erfüllen und somit die Ziele dieser Richtlinie erreichen zu können. Da mit dieser Richtlinie durch den Aufbau von Vertrauen ein besseres Funktionieren des Binnenmarkts bezweckt wird, müssen die Stellen der Mitgliedstaaten wirksam mit den Wirtschaftsteilnehmern zusammenarbeiten können und über entsprechende Strukturen verfügen.

(32) Sicherheitsvorfälle sollten den zuständigen Behörden oder den Computer-Notfallteams (CSIRTs — Computer Security Incident Response Teams) gemeldet werden. Sicherheitsvorfälle sollten nicht unmittelbar den zentralen Anlaufstellen gemeldet werden, es sei denn, diese üben außerdem die Funktion einer zuständigen Behörde oder eines CSIRT aus. Eine zuständige Behörde oder ein CSIRT sollte allerdings in der Lage sein, die zentrale Anlaufstelle damit zu beauftragen, Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten.

(33) Damit sichergestellt ist, dass die Mitgliedstaaten und die Kommission wirksam informiert werden, sollte die zentrale Anlaufstelle der Kooperationsgruppe einen zusammenfassenden Bericht vorlegen, der anonymisiert sein sollte, um die Vertraulichkeit der Meldungen und der Identität der Betreiber wesentlicher Dienste oder der Anbieter digitaler Dienste zu wahren, da die Identität der meldenden Einrichtungen für den Austausch bewährter Verfahren innerhalb der Kooperationsgruppe nicht erforderlich ist. In dem zusammenfassenden Bericht sollten Informationen über die Anzahl der eingegangenen Meldungen sowie Angaben über die Art der gemeldeten Sicherheitsvorfälle, wie beispielsweise die Arten der Sicherheitsverletzungen, deren Schwere oder Dauer, enthalten sein.

(34) Die Mitgliedstaaten sollten über angemessene technische und organisatorische Fähigkeiten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen. Die Mitgliedstaaten sollten daher gewährleisten, dass sie über gut funktionierende CSIRTs — auch Computer-Notfallteams (CERTs — Computer Emergency Response Teams) genannt — verfügen, die die grundlegenden Anforderungen zur Gewährleistung wirksamer und kompatibler Fähigkeiten zur Bewältigung von Vorfällen und Risiken und einer effizienten Zusammenarbeit auf Unionsebene erfüllen. Damit alle Arten von Betreibern wesentlicher Dienste und von Anbietern digitaler Dienste diese Fähigkeiten und diese Zusammenarbeit nutzen können, sollten die Mitgliedstaaten sicherstellen, dass alle Arten von einem eingerichteten CSIRT abgedeckt sind. Wegen der Bedeutung der internationalen Zusammenarbeit zur Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch diese Richtlinie geschaffenen CSIRTs-Netzwerk an internationalen Kooperationsnetzen beteiligen können.

(35) Da die meisten Netz- und Informationssysteme privat betrieben werden, ist die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor von zentraler Bedeutung. Die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste sollten angehalten werden, sich eines eigenen informellen Kooperationsmechanismus zur Gewährleistung der Sicherheit von Netz- und Informationssystemen zu bedienen. Die Kooperationsgruppe sollte gegebenenfalls relevante Interessenträger zu Beratungen einladen können. Zur wirksamen Unterstützung des Austauschs von Informationen und bewährten Verfahren muss unbedingt sichergestellt werden, dass Betreiber wesentlicher Dienste und Anbieter digitaler Dienste, die an einem solchen Austausch beteiligt sind, keine Benachteiligung aufgrund ihrer Zusammenarbeit erfahren.

(36) Die ENISA sollte die Mitgliedstaaten und die Kommission mit Fachkompetenz, als Berater und als Mittler für den Austausch bewährter Verfahren unterstützen. Insbesondere sollte die Kommission die ENISA bei der Anwendung dieser Richtlinie zurate ziehen, und die Mitgliedstaaten sollten berechtigt sein, die ENISA zurate zu ziehen. Um Kapazitäten und Fachwissen unter den Mitgliedstaaten aufbauen zu können, sollte die Kooperationsgruppe auch als Instrument für den Austausch bewährter Verfahren, für die Beratung über Fähigkeiten und die Abwehrbereitschaft der Mitgliedstaaten dienen und damit ihren Mitgliedern — auf freiwilliger Basis — bei der Evaluierung der nationalen Strategien für die Sicherheit von Netz- und Informationssystemen, beim Kapazitätsaufbau und bei der Evaluierung von Übungen zur Sicherheit von Netz- und Informationssystemen helfen.

(37) Bei der Anwendung dieser Richtlinie sollten die Mitgliedstaaten gegebenenfalls bestehende Organisationsstrukturen oder -strategien nutzen oder anpassen können.

(38) Die jeweiligen Aufgaben der Kooperationsgruppe und der ENISA bedingen einander und ergänzen sich. Im Einklang mit ihrem in der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates ([1]) festgelegten Ziel, nämlich die Organe, Einrichtungen und sonstigen Stellen der Union und die Mitgliedstaaten dabei zu unterstützen, die politischen Maßnahmen durchzuführen, die erforderlich sind, um die rechtlichen und regulatorischen Anforderungen in Bezug auf die Sicherheit von Netz- und Informationssystemen gemäß den geltenden und künftigen Rechtsakten der Union zu erfüllen, sollte die ENISA die Kooperationsgruppe bei der Ausführung ihrer Aufgaben unterstützen. Die ENISA sollte insbesondere in den Bereichen Unterstützung leisten, die ihren eigenen, in der Verordnung (EU) Nr. 526/2013 festgelegten Aufgaben entsprechen, nämlich Strategien zur Sicherheit von Netz- und Informationssystemen zu analysieren, die Organisation und Durchführung von Übungen zur Sicherheit von Netz- und Informationssystemen auf Unionsebene zu unterstützen und Informationen und bewährte Verfahren in den Bereichen Öffentlichkeitsarbeit und Fortbildung auszutauschen. Die ENISA sollte außerdem an der Entwicklung von Leitlinien für sektorspezifische Kriterien zur Bestimmung der Bedeutung der Auswirkungen eines Sicherheitsvorfalls beteiligt sein.

([1]) Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004 (ABl. L 165 vom 18.6.2013, S. 41).

(39) Zur Förderung verbesserter Sicherheit von Netz- und Informationssystemen sollte die Kooperationsgruppe gegebenenfalls mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union zusammenarbeiten, um Know-how und bewährte Verfahren mit ihnen auszutauschen und sie bezüglich Sicherheitsaspekten der Netz- und Informationssysteme, die Auswirkungen auf ihre Arbeit haben könnten, zu beraten, wobei die geltenden Vereinbarungen für den Austausch von einem eingeschränkten Zugang unterliegenden Informationen einzuhalten sind. Bei ihrer Zusammenarbeit mit Strafverfolgungsbehörden im Zusammenhang mit Sicherheitsaspekten der Netz- und Informationssysteme, die sich möglicherweise auf ihre Arbeit auswirken, sollte die Kooperationsgruppe vorhandene Informationskanäle und bestehende Netze beachten.

(40) Informationen über Sicherheitsvorfälle sind für die allgemeine Öffentlichkeit und Unternehmen, insbesondere für kleine und mittlere Unternehmen, zunehmend von Bedeutung. In manchen Fällen werden derartige Informationen bereits über das Internet auf nationaler Ebene in der jeweiligen Landessprache und mit besonderem Schwerpunkt auf Sicherheitsvorfälle und Sicherheitsereignisse mit nationalem Bezug bereitgestellt. Da Unternehmen immer stärker grenzüberschreitend tätig sind und die Bürger Online-Dienste nutzen, sollten die Informationen über Sicherheitsvorfälle auf Unionsebene in aggregierter Form bereitgestellt werden. Das Sekretariat des CSIRTs-Netzwerks wird aufgefordert, eine Website zu unterhalten oder eine entsprechende Seite auf einer bestehenden Website einzustellen, auf der allgemeine Informationen über größere in der Union aufgetretene Sicherheitsvorfälle mit einem besonderen Schwerpunkt auf die Interessen und den Bedarf von Unternehmen der allgemeinen Öffentlichkeit zur Verfügung gestellt werden. CSIRTs, die sich am CSIRTs-Netzwerk beteiligen, werden aufgefordert, freiwillig die auf dieser Website zu veröffentlichenden Informationen bereitzustellen, ohne vertrauliche oder sensible Informationen darin aufzunehmen.

(41) Gelten die betreffenden Informationen nach Vorschriften der Union und der Mitgliedstaaten über das Geschäftsgeheimnis als vertraulich, sollte deren Vertraulichkeit bei den in dieser Richtlinie vorgesehenen Tätigkeiten und bei der Erreichung der darin gesetzten Ziele sichergestellt werden.

(42) Übungen, bei denen Szenarien für Sicherheitsvorfälle in Echtzeit simuliert werden, sind wesentlich, um die Abwehrbereitschaft der Mitgliedstaaten und deren Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen zu prüfen. Der von der ENISA unter Beteiligung der Mitgliedstaaten koordinierte Übungszyklus Cyber Europe ist ein nützliches Instrument zur Prüfung und für die Abfassung von Empfehlungen dazu, wie auf Unionsebene die Reaktion auf Sicherheitsvorfälle mit der Zeit verbessert werden sollte. In Anbetracht dessen, dass die Mitgliedstaaten gegenwärtig nicht verpflichtet sind, Übungen zu planen oder an ihnen teilzunehmen, sollte die Schaffung des CSIRTs-Netzwerks im Rahmen dieser Richtlinie es den Mitgliedstaaten ermöglichen, auf der Grundlage präziser Planungen und strategischer Entscheidungen an Übungen teilzunehmen. Die durch diese Richtlinie eingesetzte Kooperationsgruppe sollte die strategischen Entscheidungen für Übungen diskutieren, insbesondere, aber nicht ausschließlich, diejenigen, die die Regelmäßigkeit der Übungen und die Ausgestaltung der Szenarien betreffen. Im Einklang mit ihrem Mandat sollte die ENISA die Organisation und die Durchführung der unionsweiten Übungen unterstützen, indem sie die Kooperationsgruppe und das CSIRTs-Netzwerk mit ihrer Fachkompetenz berät.

(43) Angesichts des globalen Charakters von Sicherheitsproblemen, die Netz- und Informationssysteme beeinträchtigen, bedarf es einer engeren internationalen Zusammenarbeit, damit die Sicherheitsstandards und der Informationsaustausch verbessert werden können und ein gemeinsames umfassendes Konzept für Sicherheitsfragen gefördert werden kann.

(44) Die Verantwortung für die Gewährleistung der Sicherheit von Netz-und Informationssystemen liegt in erheblichem Maße bei den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste. Durch geeignete rechtliche Anforderungen und freiwillige Branchenpraxis sollte eine Risikomanagementkultur gefördert und entwickelt werden, die unter anderem die Risikobewertung und die Anwendung von Sicherheitsmaßnahmen, die den jeweiligen Risiken angemessen sind, umfassen sollte. Ferner ist es für ein Funktionieren der Kooperationsgruppe und des CSIRTs-Netzwerks von großer Bedeutung, verlässliche gleiche Ausgangsbedingungen zu schaffen, damit eine wirksame Zusammenarbeit aller Mitgliedstaaten sichergestellt ist.

(45) Diese Richtlinie gilt nur für öffentliche Verwaltungen, die als Betreiber wesentlicher Dienste ermittelt werden. Daher sind die Mitgliedstaaten für die Gewährleistung der Sicherheit von Netz- und Informationssystemen der öffentlichen Verwaltungen verantwortlich, die nicht in den Anwendungsbereich dieser Richtlinie fallen.

(46) Die Maßnahmen für das Risikomanagement umfassen Maßnahmen zur Ermittlung jeder Gefahr eines Vorfalls, zur Verhinderung, Aufdeckung und Bewältigung von Sicherheitsvorfällen sowie der Minderung ihrer Folgen. Die Sicherheit von Netz- und Informationssystemen umfasst die Sicherheit gespeicherter, übermittelter und verarbeiteter Daten.

(47) Zuständige Behörden sollten weiterhin nationale Leitlinien festlegen können, die die Umstände betreffen, unter denen Betreiber wesentlicher Dienste verpflichtet sind, Sicherheitsvorfälle zu melden.

(48) Viele Unternehmen in der Union verlassen sich bei der Bereitstellung ihrer Dienste auf Anbieter digitaler Dienste. Da manche digitale Dienste für ihre Nutzer, darunter auch Betreiber wesentlicher Dienste, eine wichtige Ressource darstellen könnten und da derartigen Nutzern möglicherweise nicht immer Alternativen zur Verfügung stehen, sollte diese Richtlinie auch für die Anbieter derartiger Dienste gelten. Die Sicherheit, Verfügbarkeit und Verlässlichkeit der in dieser Richtlinie aufgeführten Art von digitalen Diensten sind für das reibungslose Funktionieren vieler Unternehmen von wesentlicher Bedeutung. Eine Störung eines solchen digitalen Dienstes könnte die Bereitstellung anderer, von ihnen abhängiger Dienste verhindern und somit wesentliche wirtschaftliche und gesellschaftliche Tätigkeiten in der Union beeinträchtigen. Derartige digitale Dienste könnten daher für das reibungslose Funktionieren von Unternehmen, die von diesen Diensten abhängen, und darüber hinaus für die Beteiligung derartiger Unternehmen am Binnenmarkt und am grenzüberschreitenden Handel in der gesamten Union eine wesentliche Rolle spielen. Die Anbieter digitaler Dienste, die unter diese Richtlinie fallen, sind diejenigen, von denen angenommen wird, dass sie digitale Dienste anbieten, von denen viele Unternehmen in der Union zunehmend abhängig sind.

(49) Angesichts der Bedeutung ihrer Dienste für die Tätigkeit anderer Unternehmen in der Union sollten Anbieter digitaler Dienste ein Sicherheitsniveau gewährleisten, das der Höhe des Risikos für die Sicherheit der von ihnen gebotenen Dienste angemessen ist. In der Praxis ist das Risiko für den Betreiber wesentlicher Dienste, die oft für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung sind, höher als das Risiko für den Anbieter digitaler Dienste. Daher sollten die an Anbieter digitaler Dienste gestellten Sicherheitsanforderungen geringer sein. Anbietern digitaler Dienste sollte es freigestellt sein, die Maßnahmen zu ergreifen, die sie für die Bewältigung der Risiken für die Sicherheit ihrer Netz- und Informationssysteme für angemessen halten. Aufgrund des grenzüberschreitenden Charakters ihrer Tätigkeiten sollten die Anbieter digitaler Dienste einem auf Unionsebene stärker harmonisierten Konzept unterliegen. Durchführungsrechtsakte sollten die Spezifikation und die Umsetzung derartiger Maßnahmen erleichtern.

(50) Zwar sind Hersteller von Hardware und Softwareentwickler keine Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste, jedoch verstärken ihre Produkte die Sicherheit von Netz- und Informationssystemen. Daher spielen sie eine wichtige Rolle dabei, die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste in die Lage zu versetzen, ihre Netz- und Informationssysteme sichern zu können. Derartige Hardware- und Softwareprodukte unterliegen bereits geltenden Produkthaftungsvorschriften.

(51) Zu den von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste zu ergreifenden technischen und organisatorischen Maßnahmen sollte nicht die Verpflichtung gehören, bestimmte geschäftliche Informationen und Produkte der Kommunikationstechnik in bestimmter Weise zu konzipieren, zu entwickeln oder herzustellen.

(52) Die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste sollten die Sicherheit der von ihnen verwendeten Netz- und Informationssysteme gewährleisten. Dabei handelt es sich hauptsächlich um private Netz- und Informationssysteme, die entweder von internem IT-Personal verwaltet werden oder deren Sicherheit Dritten anvertraut wurde. Die Sicherheitsanforderungen und die Meldepflicht sollten für die einschlägigen Betreiber wesentlicher Dienste und Anbieter digitaler Dienste unabhängig davon gelten, ob sie ihre Netz- und Informationssysteme intern warten oder diese Aufgabe ausgliedern.

(53) Damit keine unverhältnismäßige finanzielle und administrative Belastung für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste entsteht, sollten die Verpflichtungen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei wird dem bei solchen Maßnahmen geltenden neuesten Stand Rechnung getragen. Im Fall von Anbietern digitaler Dienste sollten diese Bestimmungen nicht für Kleinst- und Kleinunternehmen gelten.

(54) Nehmen öffentliche Verwaltungen in den Mitgliedstaaten die Dienste von Anbietern digitaler Dienste in Anspruch, insbesondere Cloud-Computing-Dienste, so verlangen sie möglicherweise vom Anbieter derartiger Dienste zusätzliche Sicherheitsmaßnahmen über das üblicherweise von Anbietern digitaler Dienste gemäß dieser Richtlinie Angebotene hinaus. Sie sollten berechtigt sein, dies über vertragliche Verpflichtungen zu regeln.

(55) Die in dieser Richtlinie enthaltenen Begriffsbestimmungen für Online-Marktplatz, Online-Suchmaschinen und Cloud-Computing-Dienste gelten für die besonderen Zwecke dieser Richtlinie und unbeschadet anderer Rechtsakte.

(56) Diese Richtlinie sollte die Mitgliedstaaten nicht daran hindern, nationale Maßnahmen zu erlassen, die öffentliche Stellen dazu verpflichten, besondere Sicherheitsanforderungen zu erfüllen, wenn sie mit Cloud-Computing-Diensten Verträge schließen. Jede dieser nationalen Maßnahmen sollte für die betreffende öffentliche Stelle und nicht für den Anbieter des Cloud-Computing-Dienstes gelten.

(57) Wegen der grundlegenden Unterschiede zwischen Betreibern wesentlicher Dienste, insbesondere wegen deren unmittelbarer Verbindung mit einer physischen Infrastruktur, und Anbietern digitaler Dienste, insbesondere wegen deren grenzüberschreitender Art, sollte die Richtlinie in Bezug auf das Maß der Harmonisierung im Hinblick auf diese beiden Gruppen jeweils einen unterschiedlichen Ansatz verfolgen. Bei Betreibern wesentlicher Dienste sollten die Mitgliedstaaten in der Lage sein, die relevanten Betreiber zu bestimmen und an sie strengere Anforderungen zu stellen als die in dieser Richtlinie festgelegten. Die Mitgliedstaaten sollten keine Anbieter digitaler Dienste bestimmen, da diese Richtlinie im Rahmen ihres Geltungsbereichs für alle Anbieter digitaler Dienste gelten sollte. Darüber hinaus sollten diese Richtlinie und die auf ihrer Grundlage erlassenen Durchführungsrechtsakte ein hohes Maß an Harmonisierung im Hinblick auf die Sicherheitsanforderungen und Meldepflichten für Anbieter digitaler Dienste gewährleisten. Das sollte zu einer einheitlichen Behandlung der Anbieter digitaler Dienste in der Union führen, die ihrer Art und der Höhe des Risikos, dem sie unterliegen könnten, angemessen ist.

(58) Diese Richtlinie sollte die Mitgliedstaaten nicht daran hindern, Einrichtungen, die keine Anbieter digitaler Dienste innerhalb des Geltungsbereichs dieser Richtlinie sind, unbeschadet der den Mitgliedstaaten nach Unionsrecht auferlegten Pflichten Sicherheitsanforderungen und Meldepflichten aufzuerlegen.

(59) Die zuständigen Behörden sollten dafür Sorge tragen, dass informelle, vertrauenswürdige Kanäle für den Informationsaustausch erhalten bleiben. Bei der Bekanntmachung von Sicherheitsvorfällen, die den zuständigen Behörden gemeldet werden, sollte das Interesse der Öffentlichkeit, über Bedrohungen informiert zu werden, sorgfältig gegen einen möglichen wirtschaftlichen Schaden bzw. einen Imageschaden abgewogen werden, der den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste, die solche Vorfälle melden, entstehen kann. Bei der Erfüllung der Meldepflichten sollten die zuständigen Behörden und die CSIRTs besonders darauf achten, dass Informationen über die Anfälligkeit von Produkten bis zur Veröffentlichung der entsprechenden Sicherheitsfixes streng vertraulich bleiben.

(60) Anbieter digitaler Dienste sollten weniger strikten reaktiven Aufsichtstätigkeiten (ex post) unterliegen, die durch die Art ihrer Dienste und Tätigkeiten gerechtfertigt sind. Die betreffenden zuständigen Behörden sollten daher nur dann tätig werden, wenn ihnen z. B. durch den Anbieter digitaler Dienste selbst, durch eine andere zuständige Behörde — auch der eines anderen Mitgliedstaats — oder durch einen Nutzer des Dienstes Nachweise dafür vorgelegt werden, dass ein Anbieter digitaler Dienste die Anforderungen dieser Richtlinie nicht erfüllt, vor allem dann, wenn sich ein Sicherheitsvorfall ereignet hat. Die zuständige Behörde sollte daher keine generelle Verpflichtung zur Beaufsichtigung von Anbietern digitaler Dienste haben.

(61) Die zuständigen Behörden sollten mit den für die Erfüllung ihrer Aufgaben erforderlichen Mitteln ausgestattet sein; sie sollten auch befugt sein, hinreichende Auskünfte einzuholen, damit sie die Sicherheit von Netz- und Informationssystemen beurteilen können.

(62) Sicherheitsvorfälle können das Ergebnis krimineller Handlungen sein, die durch Unterstützung der Koordination und der Zusammenarbeit zwischen den Betreibern wesentlicher Dienste, den Anbietern digitaler Dienste, den zuständigen Behörden und den Strafverfolgungsbehörden verhindert, aufgedeckt und strafrechtlich verfolgt werden. Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen nach Unionsrecht oder nationalem Recht steht, so sollten die Mitgliedstaaten die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste dazu anhalten, diese Sicherheitsvorfälle mit einem mutmaßlichen schwerwiegenden kriminellen Hintergrund den entsprechenden Strafverfolgungsbehörden zu melden. Gegebenenfalls ist die Unterstützung durch das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und der ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden der verschiedenen Mitgliedstaaten wünschenswert.

(63) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. Deshalb sollten die zuständigen Behörden und die Datenschutzbehörden zusammenarbeiten und Informationen zu allen einschlägigen Fragen austauschen, um Verletzungen des Schutzes personenbezogener Daten aufgrund von Sicherheitsvorfällen zu begegnen.

(64) Ein Anbieter digitaler Dienste sollte der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem der betreffende Anbieter digitaler Dienste seine Hauptniederlassung in der Union hat; dies ist im Allgemeinen der Ort, an dem er seinen Hauptsitz in der Union hat. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob sich der physische Standort der Netz- und der

Informationssysteme an einem bestimmten Ort befindet; das Vorhandensein und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein Kriterium für die Bestimmung der Hauptniederlassung.

(65) Bietet ein Anbieter digitaler Dienste, der keine Niederlassung in der Union hat, Dienste in der Union an, so sollte er einen Vertreter benennen. Um festzustellen, ob ein solcher Anbieter digitaler Dienste in der Union Dienste anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, Personen in einem oder mehreren Mitgliedstaaten Dienste anzubieten. Die bloße Zugänglichkeit der Website eines Anbieters digitaler Dienste oder eines Vermittlers von der Union aus oder einer E-Mail-Adresse oder anderer Kontaktdaten sind zur Feststellung einer solchen Absicht ebenso wenig ausreichend wie die Verwendung einer Sprache, die in dem Drittland, in dem der Anbieter digitaler Dienste niedergelassen ist, allgemein gebräuchlich ist. Jedoch können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Dienste in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern in der Union darauf hindeuten, dass der Anbieter digitaler Dienste beabsichtigt, in der Union Dienste anzubieten. Der Vertreter sollte im Auftrag des Anbieters digitaler Dienste handeln, und es sollte für die zuständigen Behörden oder die CSIRTs möglich sein, mit ihm Kontakt aufzunehmen. Der Vertreter sollte vom Anbieter digitaler Dienste ausdrücklich schriftlich beauftragt werden, im Rahmen der Pflichten des Letztgenannten gemäß dieser Richtlinie in dessen Auftrag zu handeln; hierzu zählt auch das Melden von Sicherheitsvorfällen.

(66) Die Normung von Sicherheitsanforderungen ist ein vom Markt ausgehender Vorgang. Um die Sicherheitsstandards einander anzunähern, sollten die Mitgliedstaaten die Anwendung oder Einhaltung konkreter Normen fördern, damit ein hohes Sicherheitsniveau von Netz- und Informationssystemen auf Unionsebene gewährleistet wird. Die ENISA sollte den Mitgliedstaaten mit Leitlinien beratend zur Seite stehen. Zu diesem Zweck könnte es hilfreich sein, harmonisierte Normen auszuarbeiten; dies sollte nach der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([1]) geschehen.

(67) Einrichtungen, die nicht in den Geltungsbereich dieser Richtlinie fallen, können mit Sicherheitsvorfällen konfrontiert sein, die sich in erheblichem Maße auf die von ihnen bereitgestellten Dienste auswirken. Sind diese Einrichtungen der Ansicht, dass es im öffentlichen Interesse liegt, das Auftreten derartiger Sicherheitsvorfälle zu melden, sollten sie dies auf freiwilliger Basis tun können. Solche Meldungen sollten von der zuständigen Behörde oder dem CSIRT bearbeitet werden, wenn diese Bearbeitung keinen unverhältnismäßigen oder ungebührlichen Aufwand für die betreffenden Mitgliedstaaten darstellt.

(68) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Richtlinie sollten der Kommission Durchführungsbefugnisse zur Festlegung der Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, und der Sicherheitsanforderungen und Meldepflichten für Anbieter digitaler Dienste übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([2]) ausgeübt werden. Wenn die Kommission Durchführungsrechtsakte zu Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, erlässt, sollte sie der Stellungnahme der ENISA so weit wie möglich Rechnung tragen.

(69) Wenn die Kommission Durchführungsrechtsakte zu Sicherheitsanforderungen für Anbieter digitaler Dienste erlässt, sollte sie der Stellungnahme der ENISA weitestgehend Rechnung tragen und Interessenträger anhören. Darüber hinaus wird die Kommission aufgefordert, den folgenden Beispielen Rechnung zu tragen: im Zusammenhang mit der Sicherheit der Systeme und Anlagen: physische Sicherheit und Sicherheit des Umfelds, Sicherheit des Materials, Kontrolle des Zugangs zu Netz- und Informationssystemen sowie Integrität der Netz- und Informationssysteme; im Hinblick auf die Bewältigung von Sicherheitsvorfällen: Verfahren für die Bewältigung von Sicherheitsvorfällen, Kapazitäten zum Aufspüren von Sicherheitsvorfällen, Meldung und Mitteilung von Sicherheitsvorfällen; in Bezug auf Betriebskontinuitätsmanagement: Strategie für die Verfügbarkeit der Dienste sowie Notfallpläne, Kapazitäten zur Wiederherstellung im Falle eines Systemabsturzes; und in Bezug auf Überwachung, Überprüfung und Erprobung: Strategien für die Überwachung und Protokollierung, Beübung von Notfallplänen, Erprobung der Netz- und Informationssysteme, Sicherheitsbewertungen und Überwachung der Einhaltung der Anforderungen.

(70) Bei der Durchführung dieser Richtlinie sollte die Kommission gegebenenfalls zu den einschlägigen sektoralen Ausschüssen und einschlägigen Einrichtungen auf Unionsebene in den von dieser Richtlinie betroffenen Bereichen Kontakt halten.

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

([2]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

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

(72) Der Austausch von Informationen über Risiken und Vorfälle in der Kooperationsgruppe und im CSIRTs-Netzwerk und die Einhaltung der Verpflichtung zur Meldung von Sicherheitsvorfällen bei den zuständigen nationalen Behörden oder den CSIRTs könnte die Verarbeitung personenbezogener Daten erfordern. Diese Verarbeitung sollte mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ([1]) und der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ([2]) vereinbar sein. Bei der Anwendung dieser Richtlinie sollte je nach Einzelfall die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([3]) gelten.

(73) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat am 14. Juni 2013 eine Stellungnahme ([4]) abgegeben.

(74) Da das Ziel dieser Richtlinie, nämlich ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union zu erreichen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen der Wirkung der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union in Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

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

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Anwendungsbereich

(1) Mit dieser Richtlinie werden Maßnahmen festgelegt, mit denen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union erreicht werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.

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

a) die Pflicht für alle Mitgliedstaaten, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen;

b) die Schaffung einer Kooperationsgruppe, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zu unterstützen und zu erleichtern und Vertrauen zwischen ihnen aufzubauen;

c) die Schaffung eines Netzwerks von Computer-Notfallteams (CSIRTs-Netzwerk — Computer Security Incident Response Teams Network), um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zu fördern;

([1]) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).
([2]) Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).
([3]) 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).
([4]) ABl. C 32 vom 4.2.2014, S. 19.

d) Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste;

e) die Pflicht für die Mitgliedstaaten, nationale zuständige Behörden, zentrale Anlaufstellen und CSIRTs mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen zu benennen.

(3) Die in dieser Richtlinie vorgesehenen Sicherheitsanforderungen und Meldepflichten gelten nicht für Unternehmen, die den Anforderungen der Artikel 13a und 13b der Richtlinie 2002/21/EG unterliegen, und nicht für Vertrauensdiensteanbieter, die den Anforderungen des Artikels 19 der Verordnung (EU) Nr. 910/2014 unterliegen.

(4) Diese Richtlinie gilt unbeschadet der Richtlinie 2008/114/EG des Rates ([1]) und der Richtlinien 2011/93/EU ([2]) und 2013/40/EU des Europäischen Parlaments und des Rates ([3]).

(5) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf das beschränkt, was für das verfolgte Ziel relevant und angemessen ist. Bei diesem Informationsaustausch werden die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen der Betreiber wesentlicher Dienste und der Anbieter digitaler Dienste geschützt.

(6) Diese Richtlinie berührt nicht die von den Mitgliedstaaten getroffenen Maßnahmen zum Schutz ihrer grundlegenden staatlichen Funktionen, insbesondere Maßnahmen zum Schutz der nationalen Sicherheit, einschließlich Maßnahmen zum Schutz von Informationen, deren Preisgabe nach Erachten der Mitgliedstaaten ihren wesentlichen Sicherheitsinteressen widerspricht, und zur Aufrechterhaltung von Recht und Ordnung, insbesondere zur Ermöglichung der Ermittlung, Aufklärung und Verfolgung von Straftaten.

(7) Wird nach Maßgabe eines sektorspezifischen Rechtsakts der Union von den Betreibern wesentlicher Dienste oder den Anbietern digitaler Dienste gefordert, entweder die Sicherheit ihrer Netz- und Informationssysteme oder die Meldung von Sicherheitsvorfällen zu gewährleisten, und sind diese Anforderungen in ihrer Wirkung den in dieser Richtlinie enthaltenen Pflichten mindestens gleichwertig, so gelten die einschlägigen Bestimmungen jenes sektorspezifischen Rechtsakts der Union.

Artikel 2

Verarbeitung personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten gemäß dieser Richtlinie erfolgt nach Maßgabe der Richtlinie 95/46/EG.

(2) Die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Union gemäß dieser Richtlinie erfolgt nach Maßgabe der Verordnung (EG) Nr. 45/2001.

Artikel 3

Mindestharmonisierung

Unbeschadet des Artikels 16 Absatz 10 und ihrer Verpflichtungen nach dem Unionsrecht können die Mitgliedstaaten Bestimmungen erlassen oder aufrechterhalten, mit denen ein höheres Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll.

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

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

([3]) Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8).

Artikel 4

Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

1. „Netz- und Informationssystem“

   a) ein elektronisches Kommunikationsnetz im Sinne des Artikels 2 Buchstabe a der Richtlinie 2002/21/EG,

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

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

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

3. „nationale Strategie für die Sicherheit von Netz- und Informationssystemen“ ein Rahmen mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen auf nationaler Ebene;

4. „Betreiber wesentlicher Dienste“ eine öffentliche oder private Einrichtung einer in Anhang II genannten Art, die den Kriterien des Artikels 5 Absatz 2 entspricht;

5. „digitaler Dienst“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([1]), der einer in Anhang III genannten Art entspricht;

6. „Anbieter digitaler Dienste“ eine juristische Person, die einen digitalen Dienst anbietet;

7. „Sicherheitsvorfall“ alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben;

8. „Bewältigung von Sicherheitsvorfällen“ alle Verfahren zur Unterstützung der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf;

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

10. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines nicht in der Union niedergelassenen Anbieters digitaler Dienste zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT — statt an den Anbieter digitaler Dienste — hinsichtlich der Pflichten dieses Anbieters digitaler Dienste gemäß dieser Richtlinie wenden kann;

11. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012;

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

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

14. „Domain-Namen-System (DNS)“ ein hierarchisch unterteiltes Bezeichnungssystem in einem Netz zur Beantwortung von Anfragen zu Domain-Namen;

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

15. „DNS-Diensteanbieter“ eine Einrichtung, die DNS-Dienste im Internet anbietet;

16. „Top-Level-Domain-Name-Registry“ eine Einrichtung, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt;

17. „Online-Marktplatz“ einen digitalen Dienst, der es Verbrauchern und/oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a bzw. Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates ([1]) ermöglicht, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern entweder auf der Website des Online-Marktplatzes oder auf der Website eines Unternehmers, die von dem Online-Marktplatz bereitgestellte Rechendienste verwendet, abzuschließen;

18. „Online-Suchmaschine“ einen digitalen Dienst, der es Nutzern ermöglicht, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, und der daraufhin Links anzeigt, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können;

19. „Cloud-Computing-Dienst“ einen digitalen Dienst, der den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht.

Artikel 5

Ermittlung der Betreiber wesentlicher Dienste

(1) Die Mitgliedstaaten ermitteln bis zum 9. November 2018 für jeden in Anhang II genannten Sektor und Teilsektor die Betreiber wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet.

(2) Die in Artikel 4 Nummer 4 genannten Kriterien zur Ermittlung von Betreibern wesentlicher Dienste sind folgende:

a) Eine Einrichtung stellt einen Dienst bereit, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist;

b) die Bereitstellung dieses Dienstes ist abhängig von Netz- und Informationssystemen; und

c) ein Sicherheitsvorfall würde eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken.

(3) Für die Zwecke des Absatzes 1 erstellt jeder Mitgliedstaat eine Liste der in Absatz 2 Buchstabe a genannten Dienste.

(4) Stellt eine Einrichtung einen in Absatz 2 Buchstabe a genannten Dienst in zwei oder mehr Mitgliedstaaten bereit, so nehmen diese Mitgliedstaaten für die Zwecke des Absatzes 1 Konsultationen miteinander auf. Diese Konsultation erfolgt, bevor eine Entscheidung über die Ermittlung getroffen wird.

(5) Die Mitgliedstaaten überprüfen die Liste der ermittelten Betreiber wesentlicher Dienste regelmäßig, mindestens jedoch alle zwei Jahre nach dem 9. Mai 2018, und aktualisieren diese gegebenenfalls.

(6) Im Einklang mit den in Artikel 11 genannten Aufgaben hat die Kooperationsgruppe die Aufgabe, die Mitgliedstaaten dabei zu unterstützen, einen einheitlichen Ansatz für die Ermittlung der Betreiber wesentlicher Dienste zu verfolgen.

(7) Für die Zwecke der Überprüfung gemäß Artikel 23 übermitteln die Mitgliedstaaten bis zum 9. November 2018 und danach alle zwei Jahre der Kommission die Informationen, die sie benötigt, um die Umsetzung dieser Richtlinie zu bewerten, insbesondere ob die Mitgliedstaaten bei der Ermittlung der Betreiber wesentlicher Dienste einen einheitlichen Ansatz verfolgen. Diese Informationen müssen mindestens Folgendes umfassen:

a) die nationalen Maßnahmen zur Ermittlung der Betreiber wesentlicher Dienste;

([1]) Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom 18.6.2013, S. 63).

b) die Liste der Dienste gemäß Absatz 3;

c) die Zahl der Betreiber wesentlicher Dienste, die in jedem der in Anhang II genannten Sektoren ermittelt werden, und einen Hinweis auf ihre Bedeutung für den jeweiligen Sektor;

d) soweit vorhanden, Schwellenwerte zur Bestimmung des einschlägigen Versorgungsgrads unter Bezugnahme auf die Zahl der Nutzer, die den jeweiligen Dienst gemäß Artikel 6 Absatz 1 Buchstabe a in Anspruch nehmen oder unter Bezugnahme auf die Bedeutung des betreffenden Betreibers wesentlicher Dienste gemäß Artikel 6 Absatz 1 Buchstabe f.

Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die Kommission — unter größtmöglicher Berücksichtigung der Stellungnahme der ENISA — geeignete technische Leitlinien zu den Parametern für die in diesem Absatz genannten Informationen festlegen.

Artikel 6

Erhebliche Störung

(1) Bei der Bestimmung des Ausmaßes einer Störung gemäß Artikel 5 Absatz 2 Buchstabe c berücksichtigen die Mitgliedstaaten mindestens die folgenden sektorübergreifenden Faktoren:

a) Zahl der Nutzer, die den von der jeweiligen Einrichtung angebotenen Dienst in Anspruch nehmen;

b) Abhängigkeit anderer in Anhang II genannter Sektoren von dem von dieser Einrichtung angebotenen Dienst;

c) mögliche Auswirkungen von Sicherheitsvorfällen — hinsichtlich Ausmaß und Dauer — auf wirtschaftliche und gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit;

d) Marktanteil dieser Einrichtung;

e) geografische Ausbreitung des Gebiets, das von einem Sicherheitsvorfall betroffen sein könnte;

f) Bedeutung der Einrichtung für die Aufrechterhaltung des Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Bereitstellung des jeweiligen Dienstes.

(2) Bei der Bestimmung, ob ein Sicherheitsvorfall eine erhebliche Störung bewirken würde, berücksichtigen die Mitgliedstaaten gegebenenfalls auch sektorspezifische Faktoren.

KAPITEL II

NATIONALE RAHMEN FÜR DIE SICHERHEIT VON NETZ- UND INFORMATIONSSYSTEMEN

Artikel 7

Nationale Strategie für die Sicherheit von Netz- und Informationssystemen

(1) Jeder Mitgliedstaat legt eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen fest, in der die strategischen Ziele und angemessene Politik- und Regulierungsmaßnahmen bestimmt werden, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll, und die mindestens die in Anhang II genannten Sektoren und die in Anhang III genannten Dienste abdeckt. Die nationale Strategie für die Sicherheit von Netz-und Informationssystemen behandelt insbesondere die folgenden Aspekte:

a) die Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

b) einen Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen, einschließlich der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure;

c) die Bestimmung von Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;

d) eine Aufstellung der Ausbildungs-, Aufklärungs- und Schulungsprogramme im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

e) eine Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;

f) einen Risikobewertungsplan zur Bestimmung von Risiken;

g) eine Liste der verschiedenen Akteure, die an der Umsetzung der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen beteiligt sind.

(2) Die Mitgliedstaaten können die ENISA um Unterstützung bei der Ausarbeitung der nationalen Strategien für die Sicherheit von Netz- und Informationssystemen ersuchen.

(3) Die Mitgliedstaaten teilen ihre nationalen Strategien für die Sicherheit von Netz- und Informationssystemen der Kommission innerhalb von drei Monaten nach ihrer Festlegung mit. Dabei können die Mitgliedstaaten die Elemente der Strategie, die die nationale Sicherheit berühren, ausklammern.

Artikel 8

Nationale zuständige Behörden und zentrale Anlaufstelle

(1) Jeder Mitgliedstaat benennt eine oder mehrere für die Sicherheit von Netz- und Informationssystemen zuständige nationale Behörden (im Folgenden „zuständige Behörde“), die mindestens die in Anhang II genannten Sektoren und die in Anhang III genannten Dienste abdecken. Die Mitgliedstaaten können diese Funktion einer oder mehreren bereits bestehenden Behörden zuweisen.

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

(3) Jeder Mitgliedstaat benennt eine für die Sicherheit von Netz- und Informationssystemen zuständige nationale zentrale Anlaufstelle (im Folgenden „zentrale Anlaufstelle“). Die Mitgliedstaaten können diese Funktion einer bestehenden Behörde zuweisen. Benennt ein Mitgliedstaat nur eine zuständige Behörde, so ist diese zuständige Behörde auch die zentrale Anlaufstelle.

(4) Die zentrale Anlaufstelle dient als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit der Behörden der Mitgliedstaaten und der Zusammenarbeit mit den entsprechenden Behörden in anderen Mitgliedsaaten sowie mit der in Artikel 11 genannten Kooperationsgruppe und dem in Artikel 12 genannten CSIRTs-Netzwerk.

(5) Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden und zentralen Anlaufstellen mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen können und die Ziele dieser Richtlinie somit erreicht werden. Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit der benannten Vertreter in der Kooperationsgruppe sicher.

(6) Die zuständigen Behörden und die zentrale Anlaufstelle konsultieren gegebenenfalls und nach Maßgabe des nationalen Rechts die zuständigen nationalen Strafverfolgungsbehörden und nationalen Datenschutzbehörden und arbeiten mit ihnen zusammen.

(7) Die Mitgliedstaaten teilen der Kommission unverzüglich die Benennung der zuständigen Behörde und der zentralen Anlaufstelle, deren Aufgaben sowie etwaige spätere Änderungen dieser Angaben mit. Die Mitgliedstaaten machen die Benennung der zuständigen Behörde und der zentralen Anlaufstelle öffentlich bekannt. Die Kommission veröffentlicht eine Liste der benannten zentralen Anlaufstellen.

Artikel 9

Computer-Notfallteams (CSIRTs)

(1) Jeder Mitgliedstaat benennt ein oder mehrere CSIRTs, die die Anforderungen des Anhangs I Nummer 1 erfüllen und mindestens die in Anhang II genannten Sektoren und die in Anhang III genannten Dienste abdecken und die für die Bewältigung von Risiken und Vorfällen nach einem genau festgelegten Ablauf zuständig sind. Ein CSIRT kann innerhalb einer zuständigen Behörde eingerichtet werden.

(2) Die Mitgliedstaaten gewährleisten, dass die CSIRTs mit angemessenen Ressourcen ausgestattet sind, damit sie ihre in Anhang I Nummer 2 aufgeführten Aufgaben wirksam erfüllen können.

Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs in dem in Artikel 12 genannten CSIRTs-Netzwerk wirksam, effizient und sicher zusammenarbeiten.

(3) Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs Zugang zu einer angemessenen, sicheren und robusten Kommunikations- und Informationsinfrastruktur auf nationaler Ebene haben.

(4) Die Mitgliedstaaten unterrichten die Kommission über den Zuständigkeitsbereich der CSIRTs sowie über die wichtigsten Elemente der Verfahren ihrer CSIRTs zur Bewältigung von Sicherheitsvorfällen.

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

Artikel 10

Zusammenarbeit auf nationaler Ebene

(1) Handelt es sich bei der zuständigen Behörde, der zentralen Anlaufstelle und dem CSIRT desselben Mitgliedstaats um getrennte Einrichtungen, so arbeiten sie bei der Erfüllung der in dieser Richtlinie festgelegten Pflichten zusammen.

(2) Die Mitgliedstaaten stellen sicher, dass entweder die zuständigen Behörden oder die CSIRTs die gemäß dieser Richtlinie übermittelten Meldungen von Sicherheitsvorfällen erhalten. Entscheidet ein Mitgliedstaat, dass die CSIRTs keine Meldungen erhalten, so wird den CSIRTs in dem zur Erfüllung ihrer Aufgaben erforderlich Umfang Zugang zu den Daten über Sicherheitsvorfälle gewährt, die von Betreibern wesentlicher Dienste gemäß Artikel 14 Absätze 3 und 5 oder von Anbietern digitaler Dienste gemäß Artikel 16 Absätze 3 und 6 gemeldet werden.

(3) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden oder die CSIRTs die zentralen Anlaufstellen über die gemäß dieser Richtlinie übermittelten Meldungen von Sicherheitsvorfällen unterrichten.

Bis zum 9. August 2018 und danach jährlich legt die zentrale Anlaufstelle der Kooperationsgruppe einen zusammenfassenden Bericht über die eingegangenen Meldungen, einschließlich der Zahl der Meldungen und der Art der gemeldeten Sicherheitsvorfälle, und über die gemäß Artikel 14 Absätze 3 und 5 und Artikel 16 Absätze 3 und 6 ergriffenen Maßnahmen vor.

KAPITEL III

ZUSAMMENARBEIT

Artikel 11

Kooperationsgruppe

(1) Zur Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustauschs zwischen den Mitgliedstaaten zum Aufbau von Vertrauen und zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union wird eine Kooperationsgruppe eingesetzt.

Die Kooperationsgruppe nimmt ihre Aufgaben auf der Grundlage von zweijährlichen Arbeitsprogrammen gemäß Absatz 3 Unterabsatz 2 wahr.

(2) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen.

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

Die Sekretariatsgeschäfte werden von der Kommission geführt.

(3) Die Kooperationsgruppe hat folgende Aufgaben:

a) Bereitstellung strategischer Leitlinien für die Tätigkeiten des gemäß Artikel 12 errichteten CSIRTs-Netzwerks;

b) Austausch von bewährten Verfahren über den Informationsaustausch im Zusammenhang mit der Meldung von Sicherheitsvorfällen gemäß Artikel 14 Absätze 3 und 5 sowie Artikel 16 Absätze 3 und 6;

c) Austausch bewährter Verfahren zwischen den Mitgliedstaaten und — in Zusammenarbeit mit der ENISA — Unterstützung der Mitgliedstaaten beim Kapazitätenaufbau zur Gewährleistung der Sicherheit von Netz- und Informationssystemen;

d) Erörterung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Bewertung — auf freiwilliger Basis — der nationalen Strategien für die Sicherheit von Netz- und Informationssystemen und der Wirksamkeit der CSIRTs sowie Bestimmung bewährter Verfahren;

e) Austausch von Informationen und bewährten Verfahren zu Sensibilisierung und Schulung;

f) Austausch von Informationen und bewährten Verfahren zu Forschung und Entwicklung bezüglich der Sicherheit von Netz- und Informationssystemen;

g) gegebenenfalls Erfahrungsaustausch zu Angelegenheiten der Sicherheit von Netz- und Informationssystemen mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union;

h) Erörterung der in Artikel 19 genannten Normen und Spezifikationen mit Vertretern der einschlägigen europäischen Normungsorganisationen;

i) Sammlung von Informationen über bewährte Verfahren bei Risiken und Sicherheitsvorfällen;

j) jährliche Prüfung der in Artikel 10 Absatz 3 Unterabsatz 2 genannten zusammenfassenden Berichte;

k) Erörterung der durchgeführten Arbeiten im Zusammenhang mit Übungen für die Sicherheit von Netz- und Informationssystemen, Ausbildungsprogrammen und Schulung, einschließlich der Arbeit der ENISA;

l) Austausch bewährter Verfahren — mit Unterstützung der ENISA — zur Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten, auch im Zusammenhang mit grenzüberschreitenden Abhängigkeiten, im Hinblick auf Risiken und Sicherheitsvorfälle;

m) Erörterung der Modalitäten für die Berichterstattung über die Meldung von Sicherheitsvorfällen gemäß den Artikeln 14 und 16.

Bis spätestens 9. Februar 2018 und danach alle zwei Jahre erstellt die Kooperationsgruppe ein Arbeitsprogramm bezüglich der Maßnahmen, die zur Umsetzung ihrer Ziele und Aufgaben im Einklang mit den Zielen dieser Richtlinie zu ergreifen sind;

(4) Für die Zwecke der Überprüfung gemäß Artikel 23 erstellt die Kooperationsgruppe bis zum 9. August 2018 und danach alle eineinhalb Jahre einen Bericht, in dem die im Rahmen der strategischen Zusammenarbeit nach diesem Artikel gewonnenen Erfahrungen bewertet werden.

(5) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind. Diese Durchführungsrechtsakte werden nach dem in Artikel 22 Absatz 2 genannten Prüfverfahren erlassen.

Für die Zwecke des Unterabsatzes 1 legt die Kommission dem in Artikel 22 Absatz 1 genannten Ausschuss den ersten Entwurf eines Durchführungsrechtsakts spätestens am 9. Februar 2017 vor.

Artikel 12

CSIRTs-Netzwerk

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

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

(3) Das CSIRTs-Netzwerk hat folgende Aufgaben:

a) Informationsaustausch zu den Diensten, Tätigkeiten und Kooperationsfähigkeiten der CSIRTs;

b) auf Antrag des Vertreters eines CSIRT eines von einem Sicherheitsvorfall potenziell betroffenen Mitgliedstaats Austausch und Erörterung von wirtschaftlich nicht sensiblen Informationen im Zusammenhang mit diesem Vorfall und damit verbundenen Risiken; das CSIRT eines jeden Mitgliedstaats kann jedoch die Beteiligung an diesen Erörterungen ablehnen, wenn die Gefahr einer Beeinträchtigung der Untersuchung des Vorfalls besteht;

c) Austausch und Bereitstellung auf freiwilliger Basis von nicht vertraulichen Informationen zu einzelnen Sicherheitsvorfällen;

d) auf Antrag des Vertreters des CSIRT eines Mitgliedstaats Erörterung und — sofern möglich — Ausarbeitung einer koordinierten Reaktion auf einen Sicherheitsvorfall, der im Gebiet dieses Mitgliedstaats festgestellt wurde;

e) Unterstützung der Mitgliedstaaten bei der Bewältigung grenzüberschreitender Sicherheitsvorfälle auf der Grundlage einer freiwilligen gegenseitigen Unterstützung;

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

   i) Kategorien von Risiken und Sicherheitsvorfällen,

   ii) Frühwarnungen,

   iii) gegenseitiger Unterstützung,

   iv) Grundsätzen und Modalitäten der Koordinierung bei der Reaktion der Mitgliedstaaten auf grenzüberschreitende Risiken und Vorfälle;

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

h) Erörterung der aus den Übungen zur Sicherheit von Netz- und Informationssystemen — auch den von der ENISA organisierten derartigen Übungen — gezogenen Lehren;

i) auf Antrag eines einzelnen CSIRT Erörterung der Fähigkeiten und der Abwehrbereitschaft dieses CSIRT;

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

(4) Für die Zwecke der Überprüfung gemäß Artikel 23 erstellt das CSIRTs-Netzwerk bis zum 9. August 2018 und danach alle eineinhalb Jahre einen Bericht, in dem die im Rahmen der operativen Zusammenarbeit nach diesem Artikel gewonnenen Erfahrungen, wozu auch Schlussfolgerungen und Empfehlungen gehören, bewertet werden. Dieser Bericht wird auch der Kooperationsgruppe übermittelt.

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

Artikel 13

Internationale Zusammenarbeit

Die Union kann im Einklang mit Artikel 218 AEUV internationale Übereinkünfte mit Drittländern oder internationalen Organisationen schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe ermöglicht und geregelt wird. In solchen Übereinkünften wird der Notwendigkeit zur Gewährleistung eines angemessenen Schutzes von Daten Rechnung getragen.

KAPITEL IV

SICHERHEIT DER NETZ- UND INFORMATIONSSYSTEME DER BETREIBER WESENTLICHER DIENSTE

Artikel 14

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

(1) Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

(2) Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete Maßnahmen ergreifen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit der von ihnen für die Bereitstellung dieser wesentlichen Dienste genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.

(3) Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste der zuständigen Behörde oder dem CSIRT Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben, unverzüglich melden. Die Meldungen müssen die Informationen enthalten, die es der zuständigen Behörde oder dem CSIRT ermöglichen, zu bestimmen, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat. Mit der Meldung wird keine höhere Haftung der meldenden Partei begründet.

(4) Zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls werden insbesondere folgende Parameter berücksichtigt:

a) Zahl der von der Unterbrechung der Erbringung des wesentlichen Dienstes betroffenen Nutzer;

b) Dauer des Sicherheitsvorfalls;

c) geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet.

(5) Auf der Grundlage der in der Meldung durch den Betreiber wesentlicher Dienste bereitgestellten Informationen unterrichtet die zuständige Behörde oder das CSIRT den bzw. die anderen betroffenen Mitgliedstaaten, sofern der Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in jenem Mitgliedstaat hat. Dabei wahrt die zuständige Behörde oder das CSIRT im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse des Betreibers wesentlicher Dienste sowie die Vertraulichkeit der in dessen Meldung bereitgestellten Informationen.

Wenn es nach den Umständen möglich ist, stellt die zuständige Behörde oder das CSIRT dem die Meldung erstattenden Betreiber wesentlicher Dienste einschlägige Informationen für die weitere Behandlung der Meldung, wie etwa Informationen, die für die wirksame Bewältigung des Sicherheitsvorfalls von Nutzen sein könnten, zur Verfügung.

Auf Ersuchen der zuständigen Behörde oder des CSIRT leitet die zentrale Anlaufstelle die in Unterabsatz 1 genannten Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.

(6) Nach Anhörung des meldenden Betreibers wesentlicher Dienste können die zuständige Behörde oder das CSIRT die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist.

(7) Die im Rahmen der Kooperationsgruppe gemeinsam handelnden zuständigen Behörden können Leitlinien zu den Umständen, unter denen die Betreiber wesentlicher Dienste Sicherheitsvorfälle melden müssen, ausarbeiten und annehmen; dies gilt auch für die Parameter zur Feststellung des Ausmaßes der Auswirkungen eines Sicherheitsvorfalls gemäß Absatz 4.

Artikel 15

Umsetzung und Durchsetzung

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über die Befugnisse und Mittel verfügen, die erforderlich sind, um zu bewerten, ob die Betreiber wesentlicher Dienste ihren Pflichten nach Artikel 14 nachkommen und inwieweit sich dies auf die Sicherheit der Netz- und Informationssysteme auswirkt.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über die Befugnisse und Mittel verfügen, um von den Betreibern wesentlicher Dienste verlangen zu können, dass sie

a) die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der dokumentierten Sicherheitsmaßnahmen, zur Verfügung stellen;

b) Nachweise für die wirksame Umsetzung der Sicherheitsmaßnahmen zur Verfügung stellen, wie etwa die Ergebnisse einer von der zuständigen Behörde oder einem qualifizierten Prüfer durchgeführten Sicherheitsüberprüfung, und im letztgenannten Fall die Ergebnisse der Überprüfung einschließlich der zugrunde gelegten Nachweise der zuständigen Behörde zur Verfügung stellen.

Bei der Anforderung dieser Informationen oder Nachweise nennt die zuständige Behörde den Zweck und gibt an, welche Informationen verlangt werden.

(3) Im Anschluss an die Bewertung der in Absatz 2 genannten Informationen oder an die Ergebnisse der Sicherheitsüberprüfungen kann die zuständige Behörde den Betreibern wesentlicher Dienste verbindliche Anweisungen zur Abhilfe der festgestellten Mängel erteilen.

(4) Bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, arbeitet die zuständige Behörde eng mit den Datenschutzbehörden zusammen.

KAPITEL V

SICHERHEIT DER NETZ- UND INFORMATIONSSYSTEME DER ANBIETER DIGITALER DIENSTE

Artikel 16

Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

(1) Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung der in Anhang III aufgeführten Dienste innerhalb der Union nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

a) Sicherheit der Systeme und Anlagen,

b) Bewältigung von Sicherheitsvorfällen,

c) Business continuity management,

d) Überwachung, Überprüfung und Erprobung,

e) Einhaltung der internationalen Normen.

(2) Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste Maßnahmen treffen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit ihrer Netze und Informationssysteme beeinträchtigen, auf die in Anhang III genannten, innerhalb der Union erbrachten Dienste vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.

(3) Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste der zuständigen Behörde oder dem CSIRT jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines der in Anhang III genannten, von ihnen innerhalb der Union erbrachten Dienste hat, unverzüglich melden. Die Meldungen müssen die Informationen enthalten, die es der zuständigen Behörde oder dem CSIRT ermöglichen, das Ausmaß etwaiger grenzübergreifender Auswirkungen des Sicherheitsvorfalls festzustellen. Mit der Meldung wird keine höhere Haftung der meldenden Partei begründet.

(4) Zur Feststellung, ob die Auswirkungen eines Sicherheitsvorfalls erheblich sind, werden insbesondere folgende Parameter berücksichtigt:

a) die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen;

b) Dauer des Sicherheitsvorfalls;

c) geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet;

d) Ausmaß der Unterbrechung der Bereitstellung des Dienstes;

e) Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Die Pflicht zur Meldung eines Sicherheitsvorfalls gilt nur, wenn der Anbieter digitaler Dienste Zugang zu den Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern gemäß Unterabsatz 1 zu bewerten.

(5) Nimmt ein Betreiber wesentlicher Dienste für die Bereitstellung eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung ist, die Dienste eines Dritten als Anbieter digitaler Dienste in Anspruch, so ist jede erhebliche Auswirkung auf die Verfügbarkeit der wesentlichen Dienste, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, von diesem Betreiber zu melden.

(6) Gegebenenfalls und insbesondere, wenn der in Absatz 3 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten. Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse des Anbieters digitaler Dienste sowie die Vertraulichkeit der bereitgestellten Informationen.

(7) Nach Anhörung des betreffenden Anbieters digitaler Dienste können die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, und gegebenenfalls die Behörden oder die CSIRTs anderer betroffener Mitgliedstaaten die Öffentlichkeit über einzelne Sicherheitsvorfälle unterrichten oder verlangen, dass der Anbieter digitaler Dienste dies unternimmt, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist, oder wenn die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

(8) Die Kommission erlässt Durchführungsrechtsakte, um die in Absatz 1 genannten Elemente und die in Absatz 4 aufgeführten Parameter genauer zu bestimmen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 22 Absatz 2 genannten Prüfverfahren bis zum 9. August 2017 erlassen.

(9) Die Kommission kann Durchführungsrechtsakte zur Festlegung der Form und des Verfahrens, welche für Meldepflichten gelten, erlassen. Diese Durchführungsrechtsakte werden nach dem in Artikel 22 Absatz 2 genannten Prüfverfahren erlassen.

(10) Die Mitgliedstaaten erlegen unbeschadet des Artikels 1 Absatz 6 den Anbietern digitaler Dienste keine weiteren Sicherheits- oder Meldepflichten auf.

(11) Kapitel V gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission ([1]).

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

Artikel 17

Umsetzung und Durchsetzung

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von Ex-post-Überwachungsmaßnahmen tätig werden, wenn ihnen Nachweise dafür vorlegt werden, dass ein Anbieter digitaler Dienste die in Artikel 16 niedergelegten Anforderungen nicht einhält. Derartige Nachweise können von der zuständigen Behörde eines anderen Mitgliedstaats, in dem der Dienst bereitgestellt wird, vorgelegt werden.

(2) Für die Zwecke des Absatzes 1 müssen die zuständigen Behörden über die erforderlichen Befugnisse und Mittel verfügen, um von den Anbietern digitaler Dienste zu verlangen,

a) die zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der nachweislichen Sicherheitsmaßnahmen, zur Verfügung zu stellen;

b) bei jedem Fall von Nichteinhaltung der in Artikel 16 niedergelegten Anforderungen Abhilfe zu schaffen.

(3) Hat ein Anbieter digitaler Dienste seine Hauptniederlassung oder einen Vertreter in einem Mitgliedstaat, aber seine Netz- und Informationssysteme befinden sich in einem oder mehreren anderen Mitgliedstaaten, so arbeiten die zuständige Behörde des Mitgliedstaats der Hauptniederlassung oder des Vertreters und die zuständigen Behörden der betreffenden anderen Mitgliedstaaten zusammen und unterstützen einander. Diese Unterstützung und Zusammenarbeit kann den Informationsaustausch zwischen den betreffenden zuständigen Behörden und das Ersuchen umfassen, die in Absatz 2 genannten Überwachungsmaßnahmen zu ergreifen.

Artikel 18

Gerichtliche Zuständigkeit und Territorialität

(1) Für die Zwecke dieser Richtlinie gilt, dass ein Anbieter digitaler Dienste der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem er seine Hauptniederlassung hat. Es gilt, dass ein Anbieter digitaler Dienste seine Hauptniederlassung in einem Mitgliedstaat hat, wenn er seinen Hauptsitz in diesem Mitgliedstaat hat.

(2) Ein Anbieter digitaler Dienste, der nicht in der Union niedergelassen ist, aber innerhalb der Union in Anhang III aufgeführte Dienste bereitstellt, benennt einen Vertreter in der Union. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es gilt, dass ein Anbieter digitaler Dienste der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegt, in dem der Vertreter niedergelassen ist.

(3) Die Benennung eines Vertreters durch den Anbieter digitaler Dienste erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Anbieter digitaler Dienste.

KAPITEL VI

NORMUNG UND FREIWILLIGE MELDUNG

Artikel 19

Normung

(1) Um eine einheitliche Anwendung des Artikels 14 Absätze 1 und 2 und des Artikels 16 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

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

Artikel 20

Freiwillige Meldung

(1) Unbeschadet des Artikels 3 können Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und die keine Anbieter digitaler Dienste sind, auf freiwilliger Basis Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen angebotenen Dienste haben.

(2) Bei der Bearbeitung dieser Meldungen werden die Mitgliedstaaten gemäß dem in Artikel 14 vorgesehenen Verfahren tätig. Die Mitgliedstaaten können Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten. Freiwillige Meldungen werden nur bearbeitet, wenn diese Bearbeitung keinen unverhältnismäßigen oder unzumutbaren Aufwand für die betreffenden Mitgliedstaaten darstellt.

Eine freiwillige Meldung darf nicht dazu führen, dass der meldenden Einrichtung Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie den Vorfall nicht gemeldet hätte.

KAPITEL VII

SCHLUSSBESTIMMUNGEN

Artikel 21

Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen für Verstöße gegen die nach dieser Richtlinie erlassenen nationalen Bestimmungen und treffen alle erforderlichen Maßnahmen, um deren Anwendung sicherzustellen. Die vorgesehenen Sanktionen müssen wirksam, angemessen und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum 9. Mai 2018 mit und melden ihr unverzüglich etwaige spätere Änderungen.

Artikel 22

Ausschussverfahren

(1) Die Kommission wird von dem Ausschuss für die Sicherheit von Netz- und Informationssystemen unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Artikel 23

Überprüfung

(1) Die Kommission legt dem Europäischen Parlament und dem Rat bis zum 9. Mai 2019 einen Bericht vor, in dem die Kohärenz der Ansätze der Mitgliedstaaten für die Ermittlung der Betreiber wesentlicher Dienste bewertet wird.

(2) Die Kommission überprüft regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRTs-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Bei ihrer Überprüfung bewertet die Kommission ferner die in den Anhängen II und III enthaltenen Listen und die Kohärenz bei der Ermittlung der Betreiber wesentlicher Dienste und der Dienste in den in Anhang II genannten Sektoren. Der erste Bericht wird bis zum 9. Mai 2021 vorgelegt.

Artikel 24

Übergangsmaßnahmen

(1) Unbeschadet des Artikels 25 beginnen die Kooperationsgruppe und das CSIRTs-Netzwerk mit der Erfüllung ihrer in Artikel 11 Absatz 3 beziehungsweise Artikel 12 Absatz 3 niedergelegten Aufgaben bis zum 9. Februar 2017 mit dem Ziel, den Mitgliedstaaten weitere Optionen für eine angemessene Zusammenarbeit während des Übergangszeitraums zu ermöglichen.

(2) Im Zeitraum vom 9. Februar 2017 bis zum 9. November 2018 erörtert die Kooperationsgruppe im Hinblick auf die Unterstützung der Mitgliedstaaten bei einem kohärenten Ansatz für den Prozess der Ermittlung der Betreiber wesentlicher Dienste das Verfahren, den Inhalt und die Art der nationalen Maßnahmen, die die Ermittlung der Betreiber wesentlicher Dienste in einem spezifischen Sektor gemäß den in den Artikeln 5 und 6 festgelegten Kriterien gestatten. Die Kooperationsgruppe erörtert ferner auf Ersuchen eines Mitgliedstaats einen Entwurf spezifischer nationaler Maßnahmen dieses Mitgliedstaats, die die Ermittlung von Betreibern wesentlicher Dienste in einem spezifischen Sektor gemäß den in den Artikeln 5 und 6 festgelegten Kriterien gestatten.

(3) Bis zum 9. Februar 2017 sorgen die Mitgliedstaaten für die Zwecke dieses Artikels für ihre angemessene Vertretung in der Kooperationsgruppe und im CSIRTs-Netzwerk.

Artikel 25

Umsetzung

(1) Die Mitgliedstaaten erlassen und veröffentlichen bis zum 9. Mai 2018 die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Maßnahmen ab dem 10. Mai 2018 an.

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

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 26

Inkrafttreten

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

Artikel 27

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 6. Juli 2016.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
M. SCHULZ	I. KORČOK

ANHANG I

COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs) — ANFORDERUNGEN UND AUFGABEN

Die Anforderungen an CSIRTs und ihre Aufgaben werden angemessen und genau festgelegt und durch nationale Strategien und/oder Vorschriften gestützt. Sie müssen Folgendes umfassen:

1. Anforderungen an CSIRTs

   a) CSIRTs sorgen für einen hohen Grad der Verfügbarkeit ihrer Kommunikationsdienste, indem sie punktuellen Ausfällen vorbeugen und mehrere Kanäle bereitstellen, damit sie jederzeit erreichbar bleiben und selbst Kontakt aufnehmen können. Die Kommunikationskanäle müssen zudem genau spezifiziert und den CSIRT-Nutzern („Constituency“) und den Kooperationspartnern wohlbekannt sein.

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

   c) Betriebskontinuität:

      i) CSIRTs müssen über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügen, um Übergaben zu erleichtern.

      ii) CSIRTs müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft gewährleisten können.

      iii) CSIRTs müssen auf eine Infrastruktur gestützt sein, deren Verfügbarkeit sichergestellt ist. Zu diesem Zweck müssen Redundanzsysteme und Ausweicharbeitsräume zur Verfügung stehen.

   d) CSIRTs müssen die Möglichkeit haben, sich an internationalen Kooperationsnetzen zu beteiligen, wenn sie es wünschen.

2. Aufgaben der CSIRTs

   a) Die Aufgaben der CSIRTs umfassen mindestens Folgendes:

      i) Überwachung von Sicherheitsvorfällen auf nationaler Ebene;

      ii) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken und Vorfälle unter den einschlägigen Interessenträgern;

      iii) Reaktion auf Sicherheitsvorfälle;

      iv) dynamische Analyse von Risiken und Vorfällen und Lagebeurteilung;

      v) Beteiligung am CSIRTs-Netzwerk.

   b) CSIRTs bauen Kooperationsbeziehungen zum Privatsektor auf.

   c) Zur Erleichterung der Zusammenarbeit fördern CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für:

      i) Abläufe zur Bewältigung von Sicherheitsvorfällen und Risiken;

      ii) Systeme zur Klassifizierung von Sicherheitsvorfällen, Risiken und Informationen.

ANHANG II

ARTEN VON EINRICHTUNGEN FÜR DIE ZWECKE DES ARTIKELS 4 NUMMER 4

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 35 der Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates ([1]), die die Funktion „Versorgung" im Sinne des Artikels 2 Nummer 19 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/72/EG
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/72/EG
	b) Erdöl	— Betreiber von Erdöl-Fernleitungen
		— Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
	c) Erdgas	— Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates ([2]);
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/73/EG
		— Fernleitungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/73/EG
		— Betreiber einer Speicheranlage im Sinne des Artikels 2 Nummer 10 der Richtlinie 2009/73/EG
		— Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nummer 12 der Richtlinie 2009/73/EG
		— Erdgasunternehmen im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/73/EG
		— Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
2. Verkehr	a) Luftverkehr	— Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates ([3])
		— Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates ([4]), Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates ([5]) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben

Sektor	Teilsektor	Art der Einrichtung
		— Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates ([6]) bereitstellen
	b) Schienenverkehr	— Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates ([7])
		— Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU, einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 der Richtlinie 2012/34/EU
	c) Schifffahrt	— Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates ([8]) für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
		— Leitungsorgane von Häfen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates ([9]), einschließlich ihrer Hafenanlagen im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
		— Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates ([10])
	d) Straßenverkehr	— Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission ([11]), die für Verkehrsmanagement- und Verkehrssteuerung verantwortlich sind
		— Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nummer 1 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates ([12])
3. Bankwesen		Kreditinstitute im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([13])
4. Finanzmarktinfrastrukturen		— Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([14])
		— zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates ([15])
5. Gesundheitswesen	Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäuser und Privatkliniken)	Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([16])

Sektor	Teilsektor	Art der Einrichtung
6. Trinkwasserlieferung und -versorgung		Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“ im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie 98/83/EG des Rates ([17]), jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch nur ein Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist, die nicht als wesentliche Dienste eingestuft werden
7. Digitale Infrastruktur		— IXPs
		— DNS-Diensteanbieter
		— TLS-Name-Registries

([1]) Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG (ABl. L 211 vom 14.8.2009, S. 55).
([2]) Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG (ABl. L 211 vom 14.8.2009, S. 94).
([3]) Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72).
([4]) Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte (ABl. L 70 vom 14.3.2009, S. 11).
([5]) Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348 vom 20.12.2013, S. 1).
([6]) Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums („Rahmenverordnung“) (ABl. L 96 vom 31.3.2004, S. 1).
([7]) Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums (ABl. L 343 vom 14.12.2012, S. 32).
([8]) Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ABl. L 129 vom 29.4.2004, S. 6).
([9]) Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen (ABl. L 310 vom 25.11.2005, S. 28).
([10]) Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates vom 27. Juni 2002 über die Einrichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr und zur Aufhebung der Richtlinie 93/75/EWG des Rates (ABl. L 208 vom 5.8.2002, S. 10).
([11]) Delegierte Verordnung (EU) 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste (ABl. L 157 vom 23.6.2015, S. 21).
([12]) Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (ABl. L 207 vom 6.8.2010, S. 1).
([13]) Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).
([14]) Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).
([15]) Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1).
([16]) Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).
([17]) Richtlinie 98/83/EG des Rates vom 3. November 1998 über die Qualität von Wasser für den menschlichen Gebrauch (ABl. L 330 vom 5.12.1998, S. 32).

ANHANG III

ARTEN DIGITALER DIENSTE IM SINNE DES ARTIKELS 4 NUMMER 5

1. Online-Marktplatz
2. Online-Suchmaschine
3. Cloud-Computing-Dienst

DURCHFÜHRUNGSVERORDNUNG (EU) 2018/151 DER KOMMISSION

vom 30. Januar 2018

über Vorschriften für die Anwendung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates hinsichtlich der weiteren Festlegung der von Anbietern digitaler Dienste beim Risikomanagement in Bezug auf die Sicherheit von Netz- und Informationssystemen zu berücksichtigenden Elemente und der Parameter für die Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union ([1]), insbesondere auf Artikel 16 Absatz 8,

in Erwägung nachstehender Gründe:

(1) Gemäß der Richtlinie (EU) 2016/1148 steht es den Anbietern digitaler Dienste frei, technische und organisatorische Maßnahmen zu ergreifen, die sie zur Bewältigung der Risiken für die Sicherheit ihrer Netz- und Informationssysteme für angemessen und verhältnismäßig halten, sofern diese Maßnahmen ein angemessenes Sicherheitsniveau gewährleisten und den in der Richtlinie vorgesehenen Elementen Rechnung tragen.

(2) Bei der Ermittlung der angemessenen und verhältnismäßigen technischen und organisatorischen Maßnahmen sollten die Anbieter digitaler Dienste die Informationssicherheit systematisch nach einem risikobasierten Ansatz angehen.

(3) Zur Gewährleistung der Sicherheit der Systeme und Anlagen sollten die Anbieter digitaler Dienste Bewertungs- und Analyseverfahren durchführen. Diese Tätigkeiten sollten das systematische Management der Netz- und Informationssysteme, die physische Sicherheit und die Sicherheit des Umfelds, die Versorgungssicherheit und die Kontrolle des Zugangs umfassen.

(4) Bei der Durchführung einer Risikoanalyse im Rahmen des systematischen Managements der Netz- und Informationssysteme sollten Anbieter digitaler Dienste dazu angehalten werden, spezifische Risiken zu ermitteln und hinsichtlich ihrer Bedeutung zu quantifizieren, indem sie beispielsweise ermitteln, welche Gefährdungen für unentbehrliche Anlagen oder Wirtschaftsgüter bestehen und wie sich diese auf den Betrieb auswirken können, und indem sie bestimmen, wie diese Gefährdungen unter Berücksichtigung der vorhandenen Fähigkeiten und des Ressourcenbedarfs am besten eingedämmt werden können.

(5) Maßnahmen im Bereich Humanressourcen könnten das Kompetenzmanagement betreffen, darunter auch Aspekte der sicherheitsrelevanten Kompetenzentwicklung und Bewusstseinsbildung. Bei der Entscheidung über geeignete Maßnahmen für die Betriebssicherheit sollten die Anbieter digitaler Dienste dazu angehalten werden, die Aspekte des Änderungs- und des Schwachstellenmanagements, der Formalisierung betrieblicher und administrativer Verfahren und der Systemerfassung und -abbildung zu berücksichtigen.

(6) Die Maßnahmen im Bereich Sicherheitsarchitektur könnten insbesondere die Trennung von Netzen und Systemen sowie spezifische Sicherheitsvorkehrungen für unentbehrliche Tätigkeiten, wie beispielsweise administrative Tätigkeiten, umfassen. Die Trennung von Netzen und Systemen könnte die Anbieter digitaler Dienste in die Lage versetzen, zwischen Elementen wie Datenströmen und Rechenressourcen zu unterscheiden, die einem Kunden, einer Gruppe von Kunden, dem Anbieter digitaler Dienste selbst oder Dritten gehören.

(7) Die mit Blick auf die physische Sicherheit und die Sicherheit des Umfelds getroffenen Maßnahmen sollten die Sicherheit der Netz- und Informationssysteme einer Organisation vor Schäden durch Vorfälle wie Diebstahl, Brand, Überschwemmung oder andere Wettereinflüsse sowie Telekommunikations- oder Stromausfälle gewährleisten.

(8) Die Sicherheit der Versorgung, z. B. mit elektrischem Strom, Brenn- und Kraftstoffen oder Kühlung, könnte auch die Sicherheit der Lieferkette umfassen, darunter insbesondere die Sicherheit bei Dritten, die Auftragnehmer und Unterauftragnehmer sind, und deren Management. Die Rückverfolgbarkeit unentbehrlicher Güter oder Vorleistungen betrifft die Fähigkeit des Anbieters digitaler Dienste, die Herkunft dieser Güter oder Vorleistungen festzustellen und zu dokumentieren.

(9) Die Nutzer digitaler Dienste sollten natürliche und juristische Personen umfassen, die Kunden oder Teilnehmer eines Online-Marktplatzes oder eines Cloud-Computing-Dienstes sind, oder die die Website einer Online-Suchmaschine besuchen, um Stichwortsuchen durchzuführen.

([1]) ABl. L 194 vom 19.7.2016, S. 1.

(10) Bei der Definition der Erheblichkeit der Auswirkungen eines Sicherheitsvorfalls sollten die in dieser Verordnung genannten Fälle als nicht erschöpfende Liste erheblicher Sicherheitsvorfälle betrachtet werden. Es sollten Lehren aus der Durchführung dieser Verordnung und aus den Arbeiten der Kooperationsgruppe gemäß Artikel 11 Absatz 3 Buchstaben i und m der Richtlinie (EU) 2016/1148 in Bezug auf die Sammlung von Informationen über bewährte Verfahren bei Risiken und Sicherheitsvorfällen sowie in Bezug auf die Modalitäten für die Berichterstattung über die Meldung von Sicherheitsvorfällen gezogen werden. Hieraus könnten sich umfassende Leitlinien für quantitative Schwellenwerte für Meldungsparameter ergeben, die eine Meldepflicht von Anbietern digitaler Dienste gemäß Artikel 16 Absatz 3 der Richtlinie (EU) 2016/1148 auslösen können. Gegebenenfalls könnte die Kommission auch erwägen, die derzeit in dieser Verordnung festgelegten Schwellenwerte zu überprüfen.

(11) Damit die zuständigen Behörden über potenzielle neue Risiken auf dem Laufenden bleiben, sollten die Anbieter digitaler Dienste dazu angehalten werden, jeglichen Sicherheitsvorfall freiwillig zu melden, der ihnen zuvor unbekannte Merkmale wie neue Exploits, Angriffsvektoren oder Angreifer, Anfälligkeiten und Gefahren aufweist.

(12) Diese Verordnung sollte ab dem Tag gelten, der auf den Tag des Ablaufs der Frist für die Umsetzung der Richtlinie (EU) 2016/1148 folgt.

(13) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 22 der Richtlinie (EU) 2016/1148 eingesetzten Ausschusses für die Sicherheit von Netz- und Informationssystemen —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand

In dieser Verordnung werden die Elemente näher festgelegt, die die Anbieter digitaler Dienste zu berücksichtigen haben, wenn sie Maßnahmen ermitteln und ergreifen, die ein bestimmtes Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, die sie im Rahmen der Bereitstellung der in Anhang III der Richtlinie (EU) 2016/1148 genannten Dienste nutzen; ferner werden die Parameter näher festgelegt, die bei der Feststellung zugrunde zu legen sind, ob ein Sicherheitsvorfall erhebliche Auswirkungen auf die Bereitstellung dieser Dienste hat.

Artikel 2

Sicherheitselemente

(1) Die Sicherheit der Systeme und Anlagen gemäß Artikel 16 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/1148 bezeichnet die Sicherheit von Netz- und Informationssystemen und ihrer physischen Umgebung und umfasst die folgenden Elemente:

a) das systematische Management von Netz- und Informationssystemen, d. h. eine Erfassung und Abbildung der Informationssysteme und die Einführung einer Reihe von geeigneten Maßnahmen für das Management der Informationssicherheit, einschließlich Risikoanalyse, Humanressourcen, Betriebssicherheit, Sicherheitsarchitektur, Lebenszyklus-Management gesicherter Daten und Systeme sowie gegebenenfalls Verschlüsselung und Verschlüsselungsmanagement;

b) die physische Sicherheit und die Sicherheit der Umgebung, d. h. das Vorhandensein einer Reihe von Vorkehrungen zum Schutz der Sicherheit der Netz- und Informationssysteme von Anbietern digitaler Dienste vor Schäden anhand eines risikobasierten Allgefahrenansatzes, der beispielsweise Systemversagen, menschliche Fehler, böswillige Handlungen oder Naturereignisse berücksichtigt;

c) die Versorgungssicherheit, d. h. die Einführung und Aufrechterhaltung geeigneter Maßnahmen zur Gewährleistung der Zugänglichkeit und gegebenenfalls der Rückverfolgbarkeit unentbehrlicher Güter oder Vorleistungen, die für die Bereitstellung der Dienste genutzt werden;

d) die Kontrolle des Zugangs zu Netz- und Informationssystemen, d. h. das Vorhandensein einer Reihe von Vorkehrungen, die gewährleisten, dass der physische und logische Zugang zu Netz- und Informationssystemen, einschließlich der administrativen Sicherheit der Netz- und Informationssysteme, auf der Grundlage von Geschäfts- und Sicherheitsanforderungen genehmigt bzw. eingeschränkt wird.

(2) Mit Blick auf die Bewältigung von Sicherheitsvorfällen gemäß Artikel 16 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/1148 umfassen die von dem Anbieter digitaler Dienste getroffenen Vorkehrungen Folgendes:

a) Aufrechterhaltung und Erprobung von Erkennungsprozessen und -verfahren zur Gewährleistung einer rechtzeitigen und angemessenen Lageerfassung bei ungewöhnlichen Ereignissen;

b) Prozesse und Vorgaben für die Meldung von Vorfällen und die Feststellung von Schwachstellen und Anfälligkeiten in ihren Informationssystemen;

c) Reaktion gemäß den festgelegten Verfahren und Berichterstattung über die Ergebnisse der ergriffenen Maßnahme;

d) Bewertung der Schwere des Sicherheitsvorfalls mit einer Dokumentierung der Erkenntnisse aus der Vorfallanalyse und einer Sammlung relevanter Informationen, die als Nachweis dienen können und einen kontinuierlichen Verbesserungsprozess fördern.

(3) Das Betriebskontinuitätsmanagement („*Business continuity management*“) gemäß Artikel 16 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/1148 bezeichnet die Fähigkeit einer Organisation zur Aufrechterhaltung bzw. Wiederherstellung der Erbringung von Diensten auf einem zuvor festgelegten akzeptablen Niveau nach einer Störung und umfasst Folgendes:

a) die Erstellung und Anwendung von Notfallplänen auf der Grundlage einer Analyse der betrieblichen Auswirkungen zur Gewährleistung der Kontinuität der vom Anbieter digitaler Dienste erbrachten Leistungen, die regelmäßig bewertet und erprobt werden, z. B. anhand von Übungen;

b) Wiederherstellungskapazitäten, die regelmäßig bewertet und erprobt werden, z. B. anhand von Übungen.

(4) Die Überwachung, Überprüfung und Erprobung gemäß Artikel 16 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/1148 umfasst die Einführung und Aufrechterhaltung von Maßnahmen in folgenden Bereichen:

a) Durchführung einer planmäßigen Abfolge von Kontrollen oder Messungen, um zu beurteilen, ob die Netz- und Informationssysteme bestimmungsgemäß funktionieren;

b) Kontrolle und Überprüfung, um zu ermitteln, ob eine Norm oder ein Leitlinienkatalog befolgt wird, Aufzeichnungen korrekt sind und die Effizienz- und Wirksamkeitsvorgaben erfüllt werden;

c) Prozess zur Feststellung von Mängeln in den Sicherheitsmechanismen eines Netz- und Informationssystems, die Daten schützen und Funktionen aufrechterhalten sollen. Ein solcher Prozess erstreckt sich auf die technischen Verfahren und das Personal, die in den Betriebsablauf eingebunden sind.

(5) Internationale Normen im Sinne des Artikels 16 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/1148 sind Normen, die von einer internationalen Normungsorganisation im Sinne des Artikels 2 Absatz 1 Buchstabe a der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates [1] angenommen wurden. Gemäß Artikel 19 der Richtlinie (EU) 2016/1148 können auch europäische oder international anerkannte Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen sowie bestehende nationale Normen verwendet werden.

(6) Anbieter digitaler Dienste müssen sicherstellen, dass sie über eine angemessene Dokumentation verfügen, anhand derer die zuständige Behörde die Einhaltung der in den Absätzen 1, 2, 3, 4 und 5 genannten Sicherheitselemente überprüfen kann.

Artikel 3

Bei der Feststellung erheblicher Auswirkungen eines Sicherheitsvorfalls zu berücksichtigende Parameter

(1) Hinsichtlich der in Artikel 16 Absatz 4 Buchstabe a der Richtlinie (EU) 2016/1148 angesprochenen Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen, muss der Anbieter digitaler Dienste in der Lage sein, eine Schätzung einer der folgenden Zahlen vorzunehmen:

a) Zahl der betroffenen natürlichen und juristischen Personen, mit denen ein Vertrag über die Bereitstellung des Dienstes abgeschlossen wurde, oder

b) Zahl der betroffenen Nutzer, die den Dienst genutzt haben, wobei insbesondere frühere Verkehrsdaten zugrunde gelegt werden.

(2) Die Dauer eines Sicherheitsvorfalls im Sinne des Artikels 16 Absatz 4 Buchstabe b bezeichnet die Zeitspanne von der Unterbrechung der ordnungsgemäßen Bereitstellung des Dienstes in Bezug auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit bis zum Zeitpunkt der Wiederherstellung.

(3) Was die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet im Sinne des Artikels 16 Absatz 4 Buchstabe c der Richtlinie (EU) 2016/1148 betrifft, muss der Anbieter digitaler Dienste in der Lage sein zu ermitteln, ob der Sicherheitsvorfall die Bereitstellung seiner Dienste in bestimmten Mitgliedstaaten beeinträchtigt.

(4) Das Ausmaß der Unterbrechung der Bereitstellung des Dienstes im Sinne des Artikels 16 Absatz 4 Buchstabe d der Richtlinie (EU) 2016/1148 wird anhand eines oder mehrerer der folgenden Merkmale beurteilt, die durch den Sicherheitsvorfall beeinträchtigt werden: Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten oder entsprechenden Dienste.

---

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

(5) Was das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten im Sinne des Artikels 16 Absatz 4 Buchstabe e der Richtlinie (EU) 2016/1148 anbelangt, muss der Anbieter digitaler Dienste in der Lage sein, auf der Grundlage von Angaben wie der Art der vertraglichen Beziehungen mit dem Kunden oder gegebenenfalls der potenziellen Zahl der Nutzer festzustellen, ob der Sicherheitsvorfall zu erheblichen materiellen oder immateriellen Verlusten für die Nutzer geführt hat, beispielsweise in Bezug auf die Gesundheit, die Sicherheit oder die Beschädigung von Sachen.

(6) Anbieter digitaler Dienste sind nicht verpflichtet, zu den Zwecken der Absätze 1, 2, 3, 4 und 5 zusätzliche Informationen einzuholen, die ihnen nicht zugänglich sind.

Artikel 4

Erhebliche Auswirkungen eines Sicherheitsvorfalls

(1) Ein Sicherheitsvorfall gilt als mit erheblichen Auswirkungen verbunden, wenn mindestens einer der folgenden Fälle eingetreten ist:

a) der von einem Anbieter digitaler Dienste bereitgestellte Dienst war mehr als 5 000 000 Nutzerstunden lang nicht verfügbar, wobei sich der Begriff Nutzerstunde auf die Zahl der Nutzer in der Union bezieht, die während einer Dauer von sechzig Minuten betroffen waren;

b) der Sicherheitsvorfall hat zu einem Verlust der Integrität, Authentizität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der entsprechenden Dienste, die über ein Netz- und Informationssystem des Anbieters digitaler Dienste angeboten werden bzw. zugänglich sind, geführt, von dem mehr als 100 000 Nutzer in der Union betroffen sind;

c) durch den Sicherheitsvorfall ist eine öffentliche Gefahr oder ein Risiko für die öffentliche Sicherheit entstanden oder es sind Menschen ums Leben gekommen;

d) der Sicherheitsvorfall hat für mindestens einen Nutzer in der Union zu einem Sachschaden in Höhe von mehr als 1 000 000 EUR geführt.

(2) Auf der Grundlage der bewährten Verfahren, die die Kooperationsgruppe im Rahmen ihrer Aufgaben gemäß Artikel 11 Absatz 3 der Richtlinie (EU) 2016/1148 erarbeitet, und der Erörterungen gemäß Artikel 11 Absatz 3 Buchstabe m kann die Kommission die in Absatz 1 genannten Schwellenwerte überprüfen.

Artikel 5

Inkrafttreten

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

(2) Sie gilt ab dem 10. Mai 2018.

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

Brüssel, den 30. Januar 2018

Für die Kommission

Der Präsident

Jean-Claude JUNCKER

I

(Gesetzgebungsakte)

VERORDNUNGEN

VERORDNUNG (EU) 2021/887 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 20. Mai 2021

zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 173 Absatz 3 und Artikel 188 Absatz 1,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Die Mehrheit der Bevölkerung der Union verfügt über einen Internetanschluss. Das tägliche Leben der Menschen und die Wirtschaft werden in zunehmendem Maße von digitalen Technologien bestimmt. Bürger und Unternehmen werden zunehmend der Gefahr schwerwiegender Cybersicherheitsvorfälle ausgesetzt und viele europäische Unternehmen verzeichnen jährlich mindestens einen Cybersicherheitsvorfall. Dies verdeutlicht, dass Abwehrfähigkeit geboten ist, die technischen und industriellen Fähigkeiten verbessert und hohe Cybersicherheitsstandards angewendet und ganzheitliche Lösungen für die Cybersicherheit, die sowohl Menschen als auch Erzeugnisse, Prozesse und Technologie in der Union einbinden, eingesetzt werden müssen sowie die Notwendigkeit, dass die Union auf dem Gebiet der Cybersicherheit und der digitalen Autonomie eine Führungsrolle übernimmt. Die Cybersicherheit kann auch verbessert werden, indem das Bewusstsein für Bedrohungen im Bereich der Cybersicherheit geschärft wird und Kompetenzen, Kapazitäten und Fähigkeiten in der gesamten Union entwickelt werden, wobei die gesellschaftlichen und ethischen Begleiterscheinungen und Bedenken konsequent zu berücksichtigen sind.

(2) Die Union hat ihre Maßnahmen zur Bewältigung der wachsenden Herausforderungen im Bereich der Cybersicherheit nach Vorlage der Cybersicherheitsstrategie durch die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik (im Folgenden „Hohe Vertreterin") in ihrer Gemeinsamen Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 7. Februar 2013 mit dem Titel „Cybersicherheitsstrategie der Europäischen Union — ein offener, sicherer und geschützter Cyberraum" (im Folgenden „Cybersicherheitsstrategie von 2013") kontinuierlich ausgebaut. Mit der Cybersicherheitsstrategie von 2013 sollte ein zuverlässiges, sicheres und offenes Cyberökosystem gefördert werden. Im Jahr 2016 erließ die Union mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([3]) über die Sicherheit von Netz- und Informationssystemen die ersten Maßnahmen im Bereich der Cybersicherheit.

([1]) ABl. C 159 vom 10.5.2019, S. 63.
([2]) Standpunkt des Europäischen Parlaments vom 17. April 2019 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates nach erster Lesung vom 20. April 2021 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 19. Mai 2021 (noch nicht im Amtsblatt veröffentlicht).
([3]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

(3) Im September 2017 legten die Kommission und die Hohe Vertreterin dem Europäischen Parlament und dem Rat eine Gemeinsame Mitteilung mit dem Titel „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“ vor, um die Abwehrfähigkeit, Abschreckung und Abwehr der Union im Bereich der Cyberangriffe weiter zu stärken.

(4) Auf dem Digitalgipfel im September 2017 in Tallinn forderten die Staats- und Regierungschefs, dass die Union bis zum Jahr 2025 weltweit zum Vorreiter in Sachen Cybersicherheit werden müsse, um das Vertrauen, die Zuversicht und den Schutz der Bürger, Verbraucher und Unternehmen online zu sichern und ein freies, von mehr Sicherheit getragenes und durch Gesetze gesichertes Internet zu ermöglichen, und erklärten ihre Absicht, dass zur (Neu-)Entwicklung von Systemen und Lösungen im Bereich Informations- und Kommunikationstechnologie (IKT) verstärkt Open-Source-Lösungen und offene Standards, auch durch Interoperabilitäts- und Standardisierungsprogramme der Union (wie ISA[2]) entwickelte bzw. geförderte Lösungen und Standards, herangezogen würden, insbesondere, um eine Herstellerabhängigkeit (Lock-in-Effekt) zu vermeiden.

(5) Mit dem durch diese Verordnung eingerichteten Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (im Folgenden „Kompetenzzentrum“) sollte dazu beigetragen werden, die Sicherheit von Netz- und Informationssystemen, darunter das Internet und andere für das Funktionieren der Gesellschaft wichtige Infrastrukturen wie Verkehrs-, Gesundheits-, Energie- und Digitalinfrastruktur, Wasserversorgung, die Finanzmärkte und die Bankensysteme, zu erhöhen.

(6) Schwere Störungen von Netz- und Informationssystemen können einzelne Mitgliedstaaten und die Union als Ganzes beeinträchtigen. Daher ist für die Gesellschaft ebenso wie für die Wirtschaft ein hohes Maß an Sicherheit bei Netz- und Informationssystemen in der gesamten Union unerlässlich. Derzeit ist die Union von nichteuropäischen Cybersicherheitsanbietern abhängig. Es liegt jedoch im strategischen Interesse der Union, dass sie sicherstellt, dass wesentliche Forschungs- und Technologiekapazitäten im Bereich der Cybersicherheit gewahrt und weiterentwickelt werden, um die Netz- und Informationssysteme von Bürgern und Unternehmen und insbesondere kritische Netz- und Informationssysteme zu sichern, und dass sie zentrale Cybersicherheitsdienste bereitstellt.

(7) In der Union gibt es eine Fülle von Fachwissen und Erfahrungen bezüglich Forschung, Technologie und industrieller Entwicklung im Bereich der Cybersicherheit, jedoch sind die Anstrengungen in Forschung und Industrie fragmentiert — es mangelt an Einheitlichkeit und einer gemeinsamen Zugrichtung —, worunter die Wettbewerbsfähigkeit und der wirksame Schutz von Netzen und Systemen in diesem Bereich leidet. Solche Anstrengungen und solches Fachwissen müssen in effizienter Weise gebündelt, vernetzt und genutzt werden, um die vorhandenen Forschungs-, Technologie- und Industriekapazitäten sowie die vorhandenen Qualifikationen auf Unionsebene und nationaler Ebene zu stärken und zu ergänzen. Wenngleich die IKT-Branche vor großen Herausforderungen steht, etwa der Befriedigung der Nachfrage nach qualifizierten Arbeitskräften, kann sie doch Nutzen daraus ziehen, wenn sie die Vielfalt der Gesellschaft insgesamt vertritt, eine ausgewogene Vertretung der Geschlechter und der ethnischen Vielfalt und die Gleichbehandlung von Menschen mit Behinderungen erreicht und künftigen Sachverständigen im Bereich Cybersicherheit den Zugang zu Wissen und Fortbildung erleichtert, auch im Rahmen der nichtformalen Bildung solcher Sachverständiger, wie etwa bei Free- und Open-Source-Software-Projekten, Civic-Technology-Projekten, Start-up-Unternehmen und Kleinstunternehmen.

(8) Kleine und mittlere Unternehmen (KMU) sind wichtige Interessenträger in der Cybersicherheitsbranche der Union und können dank ihrer schnellen Reaktionsfähigkeit Spitzenlösungen bereitstellen. Nicht auf Cybersicherheit spezialisierte KMU sind jedoch tendenziell auch stärker durch Cybersicherheitsvorfälle gefährdet, da wirksame Cybersicherheitslösungen hohe Investitionen und umfangreiche Sachkenntnis erfordern. Das Kompetenzzentrum und das Netzwerk nationaler Koordinierungszentren (im Folgenden „Netzwerk“) müssen KMU daher durch einen leichteren Zugang der KMU zu Wissen und einen maßgeschneiderten Zugang zu den Ergebnissen von Forschung und Entwicklung unterstützen, damit die KMU sich hinreichend schützen können und damit im Bereich der Cybersicherheit tätige KMU ihre Wettbewerbsfähigkeit aufrechterhalten und ihren Beitrag zur Führungsrolle der Union auf dem Gebiet der Cybersicherheit leisten können.

(9) Sachverstand ist nicht nur in der Branche selbst und in Forschungskontexten zu finden. Bei den als „Civic-Tech-Projekte“ bezeichneten nichtkommerziellen und vorkommerziellen Projekten werden im Interesse der Gesellschaft und des Gemeinwohls offene Standards, offene Daten und freie und quelloffene Software genutzt.

(10) Der Bereich Cybersicherheit ist vielfältig. Die einschlägigen Interessenträger umfassen Interessenträger von öffentlichen Einrichtungen, der Mitgliedstaaten und der Union, sowie der Industrie, der Zivilgesellschaft, z. B. von Gewerkschaften, von Verbraucherverbänden oder aus der Free- und Open-Source-Software-Gemeinschaft, aus Wissenschaft und Forschung, und anderen Organisationen.

(11) In den im November 2017 angenommenen Schlussfolgerungen des Rates wurde die Kommission aufgefordert, rasch eine Folgenabschätzung der möglichen Optionen für die Einrichtung eines Netzwerks von Cybersicherheitskompetenzzentren und eines Europäischen Forschungs- und Kompetenzzentrums für Cybersicherheit vorzunehmen und bis Mitte 2018 ein einschlägiges Rechtsinstrument für die Einrichtung eines solchen Netzwerks und eines solchen Zentrums vorzuschlagen.

(12) Die Union verfügt nach wie vor nicht über ausreichende technologische und industrielle Kapazitäten und Fähigkeiten, um ihre Wirtschaft und ihre kritischen Infrastrukturen autonom zu sichern und zu einem weltweit führenden Akteur im Bereich der Cybersicherheit zu werden. Das Niveau der strategischen und nachhaltigen Abstimmung und Zusammenarbeit zwischen Branchen, Forschungsgemeinschaften im Bereich der Cybersicherheit und Regierungen ist unzureichend. Die Union leidet unter unzulänglichen Investitionen in und einem eingeschränkten Zugang zu Know-how, Kompetenzen und Einrichtungen im Bereich der Cybersicherheit, und nur wenige Ergebnisse von Forschung und Innovation im Bereich Cybersicherheit der Union werden in marktfähige Lösungen umgesetzt oder in der Wirtschaft großflächig eingesetzt.

(13) Die Errichtung des Kompetenzzentrums sowie des Netzwerks, das über das Mandat verfügt, zur Unterstützung industrieller Technologien und im Bereich Forschung und Innovation Maßnahmen zu ergreifen, ist der beste Weg, die Ziele der vorliegenden Verordnung zu verwirklichen und gleichzeitig die größtmögliche wirtschaftliche, soziale und ökologische Wirkung zu erzielen und die Interessen der Union zu wahren.

(14) Das Kompetenzzentrum sollte das wichtigste Instrument der Union sein, um Investitionen in Forschung, Technologie und industrielle Entwicklung im Bereich der Cybersicherheit zu bündeln sowie einschlägige Projekte und Initiativen zusammen mit dem Netzwerk durchzuführen. Das Kompetenzzentrum sollte aus dem mit der Verordnung (EU) 2021/695 des Europäischen Parlaments und des Rates ([4]) festgelegten Rahmenprogramm für Forschung und Innovation (im Folgenden „„Horizont Europa"") und dem mit der Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates ([5]) aufgestellten Programm „Digitales Europa" finanzielle Unterstützung für den Bereich der Cybersicherheit verwalten und gegebenenfalls auch für andere Programme offenstehen. Dieser Ansatz sollte dazu beitragen, Synergien zu schaffen und die finanzielle Unterstützung im Zusammenhang mit Initiativen der Union auf dem Gebiet der Forschung und Entwicklung, Innovation, Technologie und industriellen Entwicklung im Bereich der Cybersicherheit zu koordinieren und sollte unnötige Doppelarbeit vermeiden.

(15) Es ist wichtig, dass bei Forschungsprojekten im Bereich der Cybersicherheit, die durch das Kompetenzzentrum unterstützt werden, die Achtung der Grundrechte und ethisches Verhalten gewährleistet werden.

(16) Das Kompetenzzentrum sollte keine operativen Cybersicherheitsaufgaben wie Aufgaben im Zusammenhang mit Reaktionsteams für Computersicherheitsverletzungen (CSIRT), einschließlich der Überwachung und Bewältigung von Cybersicherheitsvorfällen, wahrnehmen. Das Kompetenzzentrum sollte jedoch in der Lage sein, im Einklang mit dem Auftrag und den Zielen dieser Verordnung die Entwicklung von IKT-Infrastrukturen im Dienste der Wirtschaftszweige, insbesondere von KMU, der Forschungsgemeinschaften, der Zivilgesellschaft und des öffentlichen Sektors zu erleichtern. Wenn die CSIRT und andere Interessenträger versuchen, die Meldung und Offenlegung von Schwachstellen zu fördern, sollten das Kompetenzzentrum und die Mitglieder der Kompetenzgemeinschaft für Cybersicherheit (im Folgenden „Gemeinschaft") in der Lage sein, diese Interessenträger auf deren Ersuchen im Rahmen ihrer jeweiligen Aufgaben zu unterstützen, und dabei Überschneidungen mit der durch die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([6]) eingerichteten Agentur der Europäischen Union für Cybersicherheit (ENISA) vermeiden.

(17) Das Kompetenzzentrum, die Gemeinschaft und das Netzwerk sollen — was das Management der Gemeinschaft und die Vertretung der Gemeinschaft im Zentrum betrifft — von der Erfahrung und der breiten Vertretung der einschlägigen Interessenträger, die während der Laufzeit von Horizont 2020 — des mit der Verordnung (EU) Nr. 1291/2013 des Europäischen Parlaments und des Rates ([7]) eingerichteten Rahmenprogramms für Forschung und Innovation (2014-2020) — in der vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit zwischen der Kommission und der Europäischen Cybersicherheitsorganisation (ECSO) aufgebaut wurde, von den Erfahrungen, die im Zuge der Anfang 2019 im Rahmen von Horizont 2020 eingeleiteten vier Pilotprojekte — nämlich CONCORDIA, ECHO, SPARTA und CyberSec4Europe — sowie vom Pilotprojekt und von den vorbereitenden Maßnahmen im Rahmen der Prüfung freier und quelloffener Software (EU-FOSSA) gesammelt wurden, profitieren.

(18) Angesichts des Umfangs der mit der Cybersicherheit verbundenen Herausforderungen und der in anderen Teilen der Welt getätigten Investitionen in Cybersicherheitskapazitäten und -fähigkeiten sollten die Union und die Mitgliedstaaten ermutigt werden, ihre finanzielle Unterstützung für Forschung, Entwicklung und Realisierung in diesem Bereich aufzustocken. Um Skaleneffekte zu erzielen und in der gesamten Union ein vergleichbares Schutzniveau zu erreichen, sollten die Bemühungen der Mitgliedstaaten in einen Unionsrahmen fließen, indem sie aktiv zur Arbeit des Kompetenzzentrums und des Netzwerks beitragen.

([4]) Verordnung (EU) 2021/695 des Europäischen Parlaments und des Rates vom 28. April 2021 über das Rahmenprogramm für Forschung und Innovation „Horizont Europa" sowie über die Regeln für die Beteiligung und die Verbreitung der Ergebnisse und zur Aufhebung der Verordnungen (EU) Nr. 1290/2013 und (EU) Nr. 1291/2013 (ABl. L 170 vom 12.5.2021, S. 1).

([5]) Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Aufstellung des Programms „Digitales Europa" und zur Aufhebung des Beschlusses (EU) 2015/2240 (ABl. L 166 vom 11.5.2021, S. 1).

([6]) 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).

([7]) Verordnung (EU) Nr. 1291/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über das Rahmenprogramm für Forschung und Innovation Horizont 2020 (2014-2020) und zur Aufhebung des Beschlusses Nr. 1982/2006/EG (ABl. L 347 vom 20.12.2013, S. 104).

(19) Soweit das für den Auftrag, die Ziele und die Aufgaben des Kompetenzzentrums von Bedeutung ist, sollten das Kompetenzzentrum und die Gemeinschaft zur Förderung der Wettbewerbsfähigkeit der Union und hoher Cybersicherheitsnormen auf internationaler Ebene einen Austausch mit der internationalen Gemeinschaft über Entwicklungen im Bereich Cybersicherheit, einschließlich Produkte und Verfahren, und im Bereich Normen und technische Normen, anstreben. Zu den einschlägigen technischen Normen könnte für die Zwecke dieser Verordnung auch die Erstellung von Referenzimplementierungen gehören, einschließlich Implementierungen, die im Rahmen von auf offenen Standards beruhenden Lizenzen veröffentlicht wurden.

(20) Das Kompetenzzentrum hat seinen Sitz in Bukarest.

(21) Das Kompetenzzentrum sollte bei der Ausarbeitung seines jährlichen Arbeitsprogramms (im Folgenden „jährliches Arbeitsprogramm") die Kommission über seinen Kofinanzierungsbedarf, den es auf der Grundlage der von Mitgliedstaaten geplanten Kofinanzierungsbeiträge für gemeinsame Maßnahmen ermittelt, informieren, damit die Kommission bei der Aufstellung des Entwurfs des Gesamthaushaltsplans der Union für das folgende Jahr einen entsprechenden Unionsbeitrag einstellen kann.

(22) Die Kommission sollte bei der Ausarbeitung des Arbeitsprogramms für „Horizont Europa" bei die Cybersicherheit betreffenden Fragen, auch im Kontext des Verfahrens zur Konsultation der Interessenträger und insbesondere vor der Verabschiedung dieses Arbeitsprogramms, die Beiträge des Kompetenzzentrums berücksichtigen und diese Beiträge auch dem Programmausschuss von „Horizont Europa" zur Verfügung stellen.

(23) Das Kompetenzzentrum sollte als eine mit Rechtspersönlichkeit ausgestattete Einrichtung der Union errichtet werden, auf die die Delegierte Verordnung (EU) 2019/715 der Kommission ([8]) Anwendung findet, um es ihm zu ermöglichen, seine Rolle im Bereich der Cybersicherheit auszuüben, die Einbeziehung des Netzwerks zu unterstützen und die Leitungsrolle der Mitgliedstaaten zu stärken. Das Kompetenzzentrum sollte eine doppelte Funktion wahrnehmen und sowohl spezifische Aufgaben in Bezug auf Industrie, Technologie und Forschung im Bereich der Cybersicherheit gemäß der vorliegenden Verordnung ausführen als auch cybersicherheitsbezogene Finanzierungsmittel aus mehreren Programmen, insbesondere aus „Horizont Europa" und dem Programm „Digitales Europa" sowie gegebenenfalls auch aus weiteren Unionsprogrammen, verwalten. Diese Verwaltung müsste im Einklang mit den für diese Programme geltenden Vorschriften erfolgen. Da die Finanzierungsmittel für den Betrieb des Kompetenzzentrums überwiegend aus „Horizont Europa" und aus dem Programm „Digitales Europa" stammen würden, muss das Kompetenzzentrum dennoch für die Zwecke des Haushaltsvollzugs, einschließlich in der Programmplanungsphase, als Partnerschaft betrachtet werden.

(24) Infolge des Beitrags der Union muss der Zugang zu den Ergebnissen der Tätigkeiten des Kompetenzzentrums und den Projekten so offen wie möglich und so beschränkt wie nötig gestaltet werden und eine Wiederverwendung hat möglich zu sein, soweit das angemessen ist.

(25) Das Kompetenzzentrum sollte die Arbeit des Netzwerks erleichtern und koordinieren. Das Netzwerk sollte aus einem nationalen Koordinierungszentren je Mitgliedstaat bestehen. Die nationalen Koordinierungszentren, die von der Kommission als Einrichtungen anerkannt wurden, die über die notwendigen Kapazitäten zur Mittelverwaltung verfügen, um den Auftrag und die Ziele nach dieser Verordnung zu erfüllen, sollten eine direkte finanzielle Unterstützung durch die Union erhalten, einschließlich Finanzhilfen, die ohne Aufforderung zur Einreichung von Vorschlägen vergeben werden, um ihre Tätigkeiten im Zusammenhang mit dieser Verordnung durchzuführen.

(26) Bei den nationalen Koordinierungszentren sollte es sich um öffentliche Einrichtungen oder Einrichtungen mit mehrheitlich staatlicher Beteiligung handeln, die nach nationalem Recht, einschließlich durch Befugnisübertragung, Aufgaben der öffentlichen Verwaltung wahrnehmen, und sie sollten von den Mitgliedstaaten ausgewählt werden. Die Funktionen eines nationalen Koordinierungszentrums in einem Mitgliedstaat sollten von einer Einrichtung wahrgenommen werden können, die andere nach Unionsrecht vorgesehene Funktionen wahrnimmt, beispielsweise die einer zuständigen nationalen Behörde, einer zentralen Anlaufstelle im Sinne der Richtlinie (EU) 2016/1148 oder anderer Verordnungen der Union oder die eines Digitalen Innovationszentrums im Sinne der Verordnung (EU) 2021/694. Andere Einrichtungen des öffentlichen Sektors oder Einrichtungen, die in einem Mitgliedstaat Aufgaben der öffentlichen Verwaltung wahrnehmen, sollten das nationale Koordinierungszentrum in diesem Mitgliedstaat bei der Wahrnehmung seiner Funktionen unterstützen können.

(27) Die nationalen Koordinierungszentren sollten die erforderlichen Verwaltungskapazitäten haben, über Fachwissen in Bezug auf Industrie, Technologie und Forschung im Bereich der Cybersicherheit verfügen oder Zugang dazu haben sowie in der Lage sein, sich wirksam mit den Fachkreisen der Industrie, des öffentlichen Sektors und der Forschung auszutauschen und abzustimmen.

(28) Die Bedeutung eines angemessenen Bewusstseins für Cybersicherheit und entsprechender Kompetenzen sollte sich in den Bildungssystemen der Mitgliedstaaten niederschlagen. Zu diesem Zweck und unter Berücksichtigung der Rolle der ENISA sowie unbeschadet der Zuständigkeiten der Mitgliedstaaten für Bildung sollten neben den einschlägigen Behörden und Interessenträgern auch die nationalen Koordinierungszentren zur Förderung und Verbreitung von Bildungsprogrammen im Bereich der Cybersicherheit beitragen.

([8]) Delegierte Verordnung (EU) 2019/715 der Kommission vom 18. Dezember 2018 über die Rahmenfinanzregelung für gemäß dem AEUV und dem Euratom-Vertrag geschaffene Einrichtungen nach Artikel 70 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates (ABl. L 122 vom 10.5.2019, S. 1).

(29) Die nationalen Koordinierungszentren sollten vom Kompetenzzentrum Finanzhilfen erhalten können, um Dritten in Form von Finanzhilfen finanzielle Unterstützung zu leisten. Die direkten Kosten, die den nationalen Koordinierungszentren für die Bereitstellung und Verwaltung von finanzieller Unterstützung für Dritte entstehen, sollten unter den entsprechenden Programmen förderfähig sein.

(30) Das Kompetenzzentrum, das Netzwerk und die Gemeinschaft sollten helfen, die neuesten Cybersicherheitsprodukte, -dienste und -verfahren voranzubringen und zu verbreiten. Gleichzeitig sollten das Kompetenzzentrum und das Netzwerk die Cybersicherheitsfähigkeiten der nachfrageseitigen Industrie fördern, indem sie insbesondere Entwicklern und Betreibern in Bereichen wie Verkehr, Energie, Gesundheit, Finanzen, Regierung, Telekommunikation, Fertigung und Raumfahrt Unterstützung leisten, um solchen Entwicklern und Betreibern bei der Bewältigung ihrer Herausforderungen im Bereich der Cybersicherheit, beispielsweise durch die Umsetzung konzeptionsintegrierter Sicherheit („security by design"), zu helfen. Das Kompetenzzentrum und das Netzwerk sollten außerdem die Normung und Realisierung von Cybersicherheitsprodukten, -diensten und -verfahren unterstützen und gleichzeitig, soweit möglich, die Umsetzung des in der Verordnung (EU) 2019/881 festgelegten europäischen Rahmens für die Cybersicherheitszertifizierung fördern.

(31) Da Cyberbedrohungen und Cybersicherheit von schnellen Veränderungen gekennzeichnet sind, muss die Union in der Lage sein, sich schnell und kontinuierlich an neue Entwicklungen in diesem Bereich anzupassen. Daher sollten das Kompetenzzentrum, das Netzwerk und die Gemeinschaft hinreichend flexibel sein, damit die erforderliche Fähigkeit, auf solche Entwicklungen zu reagieren, vorhanden ist. Sie sollten Projekte unterstützen, mit denen Einrichtungen ermöglicht wird, ihre Fähigkeiten stetig auszubauen und damit sowohl die eigene Abwehrfähigkeit als auch die der Union zu stärken.

(32) Das Kompetenzzentrum sollte die Gemeinschaft unterstützen. Das Kompetenzzentrum sollte die für Cybersicherheit relevanten Teile von „Horizont Europa" und des Programms „Digitales Europa" in Übereinstimmung mit dem mehrjährigen Arbeitsprogramm des Kompetenzzentrums (im Folgenden „mehrjähriges Arbeitsprogramm"), dem jährlichen Arbeitsprogramm sowie dem Strategieplanungsprozess im Rahmen von „Horizont Europa" umsetzen, indem Finanzhilfen und andere Formen von Finanzierungen vergeben werden, vor allem nach einer wettbewerbsorientierten Aufforderung zur Einreichung von Vorschlägen. Das Kompetenzzentrum sollte auch die Weitergabe von Fachwissen im Netzwerk und in der Gemeinschaft erleichtern und sollte gemeinsame Investitionen der Union, der Mitgliedstaaten oder der Industrie unterstützen. Besonderes Augenmerk sollte auf die Unterstützung von KMU im Bereich der Cybersicherheit und Maßnahmen zur Schließung von Qualifikationslücken gerichtet werden.

(33) Die für die Projektvorbereitung geleistete technische Hilfe sollte in uneingeschränkt objektiver und transparenter Weise erfolgen, mit der sichergestellt wird, dass alle potenziellen Begünstigten die gleichen Informationen erhalten und mit der Interessenkonflikte vermieden werden.

(34) Das Kompetenzzentrum sollte die langfristige strategische Zusammenarbeit und Koordinierung der Tätigkeiten der Gemeinschaft anregen und unterstützen, was eine große, offene, interdisziplinäre und vielfältige Gruppe von im Bereich Cybersicherheitstechnologie tätigen europäischen Interessenträger einbeziehen würde. Die Gemeinschaft sollte Forschungseinrichtungen, Branchen sowie den öffentlichen Sektor umfassen. Die Gemeinschaft sollte — insbesondere über die strategische Beratungsgruppe — einen Beitrag zu den Tätigkeiten des Kompetenzzentrums, dem mehrjährigen Arbeitsprogramm und dem jährlichen Arbeitsprogramm leisten. Die Gemeinschaft sollte auch von den Tätigkeiten des Kompetenzzentrums und des Netzwerks zum Aufbau von Gemeinschaften profitieren; darüber hinaus sollte sie aber im Hinblick auf Aufforderungen zur Einreichung von Vorschlägen oder Ausschreibungen nicht bevorzugt werden. Die Gemeinschaft sollte sich aus kollektiven Einrichtungen und Organisationen zusammensetzen. Damit das gesamte Fachwissen auf dem Gebiet der Cybersicherheit in der Union genutzt werden kann, sollten das Kompetenzzentrum und seine Gremien in der Lage sein, gleichzeitig auch auf das Fachwissen natürlicher Personen als Ad-hoc-Sachverständige zurückzugreifen.

(35) Das Kompetenzzentrum sollte mit der ENISA zusammenarbeiten und Synergien mit dieser Agentur sicherstellen und dem Kompetenzzentrum sachdienliche Hinweise von der ENISA geben, wenn es um die Festlegung der Finanzierungsprioritäten geht.

(36) Um den Erfordernissen sowohl der Anbieter- als auch der Nachfrageseite im Bereich Cybersicherheit gerecht zu werden, sollte sich die Aufgabe des Kompetenzzentrums, Branchen Fachwissen und technische Hilfe im Bereich der Cybersicherheit bereitzustellen, auf IKT-Produkte, -Prozesse und -Dienste sowie auf alle anderen technischen Produkte und Prozesse beziehen, in die Cybersicherheit einzubinden ist. Auf Antrag sollte auch der öffentliche Sektor vom Kompetenzzentrum unterstützt werden können.

(37) Um ein tragfähiges Cybersicherheitsumfeld zu etablieren, muss bei der Entwicklung, der Wartung, dem Betrieb und der Aktualisierung von Infrastrukturen, Produkten und Diensten grundsätzlich die konzeptionsintegrierte Sicherheit greifen, indem insbesondere modernste sichere Entwicklungsmethoden, angemessene Sicherheitstests und Sicherheitsprüfungen unterstützt, unverzüglich Aktualisierungen zur Behebung bekannter Schwachstellen oder Gefahren bereitgestellt und, soweit möglich, Dritte dazu befähigt werden, über das jeweilige Wartungsende des Produkts hinaus Aktualisierungen zu erstellen und bereitzustellen. Die konzeptionsintegrierte Sicherheit des IKT-Produkts, -Dienstes oder -Prozesses sollte während seiner gesamten Lebensdauer über dessen Konzeption und durch Entwicklungsprozesse sichergestellt werden, die ständig weiterentwickelt werden, um das Risiko von Schäden durch eine böswillige Nutzung zu verringern.

(38) Während das Kompetenzzentrum und das Netzwerk sich um stärkere Synergien und Abstimmung zwischen dem zivilen und dem Verteidigungssektor im Bereich der Cybersicherheit bemühen sollten, sollten die unter diese Verordnung fallenden, im Rahmen von „Horizont Europa" finanzierten Projekte im Einklang mit der Verordnung (EU) 2021/695 durchgeführt werden, in der festgelegt ist, dass der Schwerpunkt bei Forschungs- und Innovationstätigkeiten im Rahmen von „Horizont Europa" ausschließlich auf zivilen Anwendungen liegen muss.

(39) Diese Verordnung findet in erster Linie auf zivile Angelegenheiten Anwendung, jedoch können die Tätigkeiten der Mitgliedstaaten im Rahmen dieser Verordnung den Besonderheiten der Mitgliedstaaten Rechnung tragen, wenn die Cybersicherheitspolitik durch Behörden verfolgt wird, die sowohl zivile als auch militärische Aufgaben wahrnehmen und sollten darauf ausgerichtet sein, Komplementarität zu erreichen und Überschneidungen mit verteidigungsbezogenen Finanzierungsinstrumenten zu vermeiden.

(40) Diese Verordnung sollte die Haftung und die Transparenz des Kompetenzzentrums und jener Unternehmen, die Finanzmittel erhalten, im Einklang mit den einschlägigen Programmverordnungen gewährleisten.

(41) Die Umsetzung von Realisierungsprojekten, die insbesondere auf Unionsebene oder über gemeinsame Auftragsvergabe realisierte Infrastrukturen und Fähigkeiten betreffen, könnte in verschiedene Umsetzungsphasen unterteilt werden, etwa in getrennte Ausschreibungen für Hardware-Design und Software-Architektur, ihre Einrichtung sowie ihren Betrieb und ihre Wartung, wobei Unternehmen jeweils nur an einer der Phasen teilnehmen dürften und gegebenenfalls verlangen könnte, dass die Begünstigten, die an einer oder mehreren dieser Phasen beteiligt sind, bestimmte für Europa geltende Anforderungen in Bezug auf Eigentum oder Kontrolle erfüllen.

(42) Angesichts ihres Fachwissens im Bereich der Cybersicherheit und ihres Mandats als Bezugspunkt der Organe, Einrichtungen und sonstigen Stellen der Union sowie anderen maßgeblichen Interessenträgern der Union für Beratung und Fachwissen auf dem Gebiet der Cybersicherheit und angesichts der von ihr im Zusammenhang mit ihren Aufgaben gesammelten Beiträge sollte sich die ENISA aktiv an den Tätigkeiten des Kompetenzzentrums, einschließlich der Entwicklung der Agenda, beteiligen, wobei jedoch — insbesondere durch die Mitwirkung der ENISA als ständige Beobachterin im Verwaltungsrat des Kompetenzzentrums — Doppelarbeit vermieden werden sollte. Bezüglich der Aufstellung der Agenda, des jährlichen Arbeitsprogramms und des mehrjährigen Arbeitsprogramms sollten der Exekutivdirektor des Kompetenzzentrums und der Verwaltungsrat sämtliche von der ENISA durchgeführten strategischen Beratungen und bereitgestellten Beiträge im Einklang mit der vom Verwaltungsrat festgelegten Geschäftsordnung berücksichtigen.

(43) Erhalten die nationalen Koordinierungszentren und die Einrichtungen, die Teil der Gemeinschaft sind, einen Finanzbeitrag aus dem Unionshaushalt, so sollten sie öffentlich machen, dass ihre jeweiligen Tätigkeiten im Rahmen der vorliegenden Verordnung durchgeführt werden.

(44) Die Kosten für die Einrichtung des Kompetenzzentrums sowie für die Verwaltungs- und Koordinierungstätigkeiten des Kompetenzzentrums sollten von der Union sowie — im Verhältnis zum freiwilligen Beitrag der Mitgliedstaaten zu gemeinsamen Maßnahmen — von den Mitgliedstaaten finanziert werden. Um eine Doppelfinanzierung zu vermeiden, sollten in diese Tätigkeiten nicht gleichzeitig auch Mittel aus anderen Unionsprogrammen fließen.

(45) Der Verwaltungsrat, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzen sollte, sollte die allgemeine Ausrichtung der Tätigkeit des Kompetenzzentrums festlegen und dafür sorgen, dass das Kompetenzzentrums seine Aufgaben im Einklang mit dieser Verordnung wahrnimmt. Der Verwaltungsrat sollte die Agenda annehmen.

(46) Dem Verwaltungsrat sollten über die erforderlichen Befugnisse übertragen werden, um den Haushaltsplan des Kompetenzzentrums zu erstellen. Er sollte die Ausführung des Haushaltsplans überprüfen, eine angemessene Finanzordnung annehmen sowie transparente Verfahren für die Entscheidungsfindung des Kompetenzzentrums festlegen, einschließlich für die Annahme des jährlichen Arbeitsprogramm und des mehrjährigen Arbeitsprogramms, die die Agenda widerspiegeln. Der Verwaltungsrat sollte sich auch eine Geschäftsordnung geben, den Exekutivdirektor ernennen und über die Verlängerung oder die Beendigung der Amtszeit des Exekutivdirektors beschließen.

(47) Der Verwaltungsrat sollte die strategischen Tätigkeiten und Umsetzungstätigkeiten des Kompetenzzentrums beaufsichtigen und dafür sorgen, dass diese Tätigkeiten aufeinander abgestimmt sind. Das Kompetenzzentrum sollte in seinem jährlichen Bericht einen besonderen Schwerpunkt auf die strategischen Ziele legen, die es verwirklicht hat, und erforderlichenfalls Maßnahmen vorschlagen, um die Verwirklichung dieser strategischen Ziele weiter zu verbessern.

(48) Damit das Kompetenzzentrum seine Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten die Kommission und die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und Erfahrung in den Funktionsbereichen verfügen. Die Kommission und die Mitgliedstaaten sollten sich auch darum bemühen, die Fluktuation bei ihren jeweiligen Vertretern im Verwaltungsrat zu verringern, um die Kontinuität seiner Arbeit sicherzustellen.

(49) Angesichts des besonderen Status und der Zuständigkeit des Kompetenzzentrums für die Ausführung der Unionsmittel, insbesondere der Mittel aus „Horizont Europa“ und dem Programm „Digitales Europa“, sollte die Kommission im Verwaltungsrat bei Beschlüssen im Zusammenhang mit Unionsmitteln über 26 % aller Stimmen verfügen, um den Unionsmehrwert dieser Beschlüsse zu maximieren und gleichzeitig die Rechtmäßigkeit dieser Beschlüsse und deren Übereinstimmung mit den Prioritäten der Union zu gewährleisten.

(50) Damit das Kompetenzzentrum reibungslos funktioniert, ist es erforderlich, dass sein Exekutivdirektor in transparenter Weise aufgrund seiner Verdienste, seiner nachgewiesenen Verwaltungs- und Managementfähigkeiten und seiner einschlägigen Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit ernannt wird und seine Aufgaben völlig unabhängig wahrnimmt.

(51) Das Kompetenzzentrum sollte über eine strategische Beratungsgruppe als Beratungsgremium verfügen. Die strategische Beratungsgruppe sollte auf der Grundlage eines regelmäßigen Dialogs zwischen dem Kompetenzzentrum und der Gemeinschaft, die aus Vertretern von Privatsektor, Verbraucherorganisationen, Wissenschaft und sonstigen Interessenträgern bestehen sollte, Empfehlungen abgeben. Die strategische Beratungsgruppe sollte sich auf für die Interessenträger relevante Fragen konzentrieren und sie dem Verwaltungsrat und dem Exekutivdirektor zur Kenntnis bringen. Die Aufgaben der strategischen Beratungsgruppe sollten Empfehlungen zur Agenda, zum jährlichen Arbeitsprogramm und zum mehrjährigen Arbeitsprogramm einschließen. Die Vertretung der verschiedenen Interessenträger in der strategischen Beratungsgruppe sollte ausgewogen sein, unter besonderer Berücksichtigung von Vertretern von KMU, damit eine angemessene Vertretung der Interessenträger in der Arbeit des Kompetenzzentrums gewährleistet ist.

(52) Bei den Beiträgen der Mitgliedstaaten zu den Ressourcen des Kompetenzzentrums könnte es sich um Finanzbeiträge oder Beiträge in Form von Sachleistungen handeln. Finanzbeiträge könnten beispielsweise aus einer Finanzhilfe bestehen, die ein Mitgliedstaat einem Begünstigten in diesem Mitgliedstaat gewährt und die die finanzielle Unterstützung der Union für ein Projekt im Rahmen des jährlichen Arbeitsprogramms ergänzt. Allerdings würden Beiträge in Form von Sachleistungen typischerweise geleistet werden, wenn eine Einrichtung eines Mitgliedstaats selbst Begünstigte einer finanziellen Unterstützung durch die Union ist. Wenn zum Beispiel die Union die Tätigkeit eines nationalen Koordinierungszentrums zu 50 % subventioniert, würden die verbleibenden Kosten der Tätigkeit als Beitrag in Form von Sachleistungen verbucht. Ein anderes Beispiel wäre wie folgt: Wenn eine Einrichtung eines Mitgliedstaats finanzielle Unterstützung der Union für die Schaffung oder die Aufrüstung einer Infrastruktur erhält, die im Einklang mit dem jährlichen Arbeitsprogramm von den Interessenträgern gemeinsam genutzt werden soll, würden die damit verbundenen nicht subventionierten Kosten als Beiträge in Form von Sachleistungen verbucht.

(53) Gemäß den einschlägigen Bestimmungen der Delegierten Verordnung (EU) 2019/715 über Interessenkonflikte sollte das Kompetenzzentrum Vorschriften zur Vermeidung, Ermittlung und Beseitigung sowie zur Handhabung von Interessenkonflikten bezüglich seiner Mitglieder, Gremien und Mitarbeiter, des Verwaltungsrates sowie der strategischen Beratungsgruppe und der Gemeinschaft haben. Die Mitgliedstaaten sollten dafür Sorge tragen, dass Interessenkonflikte mit Blick auf die nationalen Koordinierungszentren im Einklang mit dem nationalen Recht vermieden, ermittelt und beseitigt werden. Das Kompetenzzentrum sollte das einschlägige Unionsrecht in Bezug auf den Zugang der Öffentlichkeit zu Dokumenten gemäß der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([9]) anwenden. Die Verarbeitung personenbezogener Daten durch das Kompetenzzentrum sollte der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([10]) unterliegen. Das Kompetenzzentrum sollte die für die Unionsorgane geltenden Bestimmungen des Unionsrechts über den Umgang mit Informationen, insbesondere den Umgang mit sensiblen Informationen und Verschlusssachen der EU, sowie die entsprechenden nationalen Rechtsvorschriften befolgen.

(54) Die finanziellen Interessen der Union und der Mitgliedstaaten sollten während des gesamten Ausgabenzyklus durch angemessene Maßnahmen geschützt werden; dazu gehören unter anderem Maßnahmen zur Prävention, Aufdeckung und Untersuchung von Unregelmäßigkeiten, die Rückforderung entgangener, zu Unrecht gezahlter oder nicht widmungsgemäß verwendeter Mittel und gegebenenfalls verwaltungsrechtliche und finanzielle Sanktionen gemäß der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates ([11]) (im Folgenden „Haushaltsordnung“).

(55) Das Kompetenzzentrum sollte seine Geschäftstätigkeit in offener und transparenter Weise ausüben. Es sollte alle relevanten Informationen fristgerecht übermitteln und seine Tätigkeiten bekannt machen, unter anderem auch durch an die Öffentlichkeit gerichtete Informations- und Verbreitungsmaßnahmen. Die Geschäftsordnungen des Verwaltungsrats des Kompetenzzentrums und der strategischen Beratungsgruppe sollten öffentlich zugänglich gemacht werden.

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

([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).

([11]) 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).

(56) Der Interne Prüfer der Kommission sollte gegenüber dem Kompetenzzentrum die gleichen Befugnisse ausüben wie gegenüber der Kommission.

(57) Die Kommission, der Rechnungshof und das Europäische Amt für Betrugsbekämpfung sollten Zugang zu allen Informationen und Räumlichkeiten des Kompetenzzentrums erhalten, die für die Durchführung von Rechnungsprüfungen und Untersuchungen in Bezug auf die vom Kompetenzzentrum unterzeichneten Finanzhilfen, Aufträge und Vereinbarungen erforderlich sind.

(58) Da die Ziele dieser Verordnung — nämlich die Stärkung der Wettbewerbsfähigkeit und der Kapazitäten der Union, die Wahrung und Weiterentwicklung der technischen und industriellen Kapazitäten der Union im Bereich der Cybersicherheitsforschung, die Steigerung der Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union und die Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Branchen der Union — von den Mitgliedstaaten allein nicht ausreichend verwirklicht werden können, da die vorhandenen begrenzten Ressourcen weit verstreut und umfangreiche Investitionen erforderlich sind, sondern vielmehr besser auf Unionsebene zu verwirklichen sind, da es darum geht, unnötige Doppelarbeit bei diesen Anstrengungen zu vermeiden, die kritische Investitionsmasse zu erreichen und sicherzustellen, dass die öffentlichen Mittel optimal genutzt werden und ein hohes Maß an Cybersicherheit in allen Mitgliedstaaten gefördert wird, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen und Grundsätze des Kompetenzzentrums und des Netzwerks

Artikel 1

Gegenstand und Anwendungsbereich

(1) Mit dieser Verordnung werden das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (im Folgenden „Kompetenzzentrum“) sowie das Netzwerk nationaler Koordinierungszentren (im Folgenden „Netzwerk“) eingerichtet. Diese Verordnung legt Bestimmungen für die Benennung nationaler Koordinierungszentren sowie Bestimmungen für die Einrichtung der Kompetenzgemeinschaft für Cybersicherheit (im Folgenden „Gemeinschaft“) fest.

(2) Das Kompetenzzentrum nimmt eine tragende Rolle bei der Umsetzung der Cybersicherheitskomponente des Programms „Digitales Europa“, insbesondere im Hinblick auf Maßnahmen im Zusammenhang mit Artikel 6 der Verordnung (EU) 2021/694, ein und trägt zur Umsetzung von „Horizont Europa“, insbesondere in Bezug auf Anhang I Pfeiler II Abschnitt 3.1.3 des Beschlusses (EU) 2021/764 des Rates ([12]) bei.

(3) Die Mitgliedstaaten tragen gemeinsam zur Arbeit des Kompetenzzentrums und des Netzwerks bei.

(4) Von dieser Verordnung unberührt bleiben die Zuständigkeiten der Mitgliedstaaten in Bezug auf die öffentliche Sicherheit, die Verteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Cybersicherheit“ alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;

2. „Netz- und Informationssystem“ ein Netz- und Informationssystem im Sinne des Artikels 4 Nummer 1 der Richtlinie (EU) 2016/1148;

3. „Cybersicherheitsprodukte, -dienste und -prozesse“ kommerzielle und nicht kommerzielle IKT-Produkte, -Dienste oder -Prozesse, die dem besonderen Zweck dienen, Netz- und Informationssysteme zu schützen oder die Vertraulichkeit, Integrität und Zugänglichkeit von Daten, die in Netz- und Informationssystemen verarbeitet oder gespeichert werden, sowie die Cybersicherheit der Nutzer solcher Systeme und anderer von Cyberbedrohungen betroffener Personen zu gewährleisten;

4. „Cyberbedrohung“ einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte;

([12]) Beschluss (EU) 2021/764 des Rates vom 10. Mai 2021 zur Einrichtung des spezifischen Programms zur Durchführung von „Horizont Europa“, dem Rahmenprogramm für Forschung und Innovation, und zur Aufhebung des Beschlusses 2013/743/EU (ABl. L 167 I vom 12.5.2021, S. 1).

5. „gemeinsame Maßnahme“ eine im jährlichen Arbeitsprogramm enthaltene Maßnahme, die finanzielle Unterstützung von „Horizont Europa“, dem Programm „Digitales Europa“ oder anderen Programmen der Union sowie finanzielle Unterstützung oder Unterstützung in Form von Sachleistungen von einem oder mehreren Mitgliedstaaten erhält und die im Wege von Projekten durchgeführt wird, an denen Begünstigte beteiligt sind, die in den Mitgliedstaaten niedergelassen sind und die finanzielle Unterstützung oder Unterstützung in Form von Sachleistungen von diesen Mitgliedstaaten erhalten;

6. „Beitrag in Form von Sachleistungen“ den nationalen Koordinierungszentren und anderen öffentlichen Einrichtungen bei der Beteiligung an im Rahmen dieser Verordnung finanzierten Projekten entstehende förderfähige Kosten, die nicht durch einen Beitrag der Union oder durch Finanzbeiträge der Mitgliedstaaten finanziert werden;

7. „Europäisches Digitales Innovationszentrum“ ein Europäisches Digitales Innovationszentrum im Sinne des Artikels 2 Buchstabe e der Verordnung (EU) 2021/694;

8. „Agenda“ eine umfassende und nachhaltige Strategie für Industrie, Technologie und Forschung im Bereich der Cybersicherheit, in der strategische Empfehlungen für die Entwicklung und das Wachstum des europäischen Sektors für Industrie, Technologie und Forschung im Bereich der Cybersicherheit sowie strategische Prioritäten für die Tätigkeiten des Kompetenzzentrums dargelegt sind und die hinsichtlich der Beschlüsse über die jährlichen Arbeitsprogramme nicht verbindlich ist;

9. „technische Hilfe“ die Unterstützung durch das Kompetenzzentrum für die nationalen Koordinierungszentren oder für die Gemeinschaft bei der Wahrnehmung ihrer Aufgaben durch Bereitstellung von Wissen oder Erleichterung des Zugangs zu Fachwissen in Bezug auf Industrie, Technologie und Forschung im Bereich der Cybersicherheit, Ermöglichung der Vernetzung, Sensibilisierung und Förderung der Zusammenarbeit, oder die Unterstützung durch das Kompetenzzentrum gemeinsam mit den nationalen Koordinierungszentren für die Interessenträger in Bezug auf die Vorbereitung von Projekten im Zusammenhang mit dem Auftrag des Kompetenzzentrums und des Netzwerks sowie den Zielen des Kompetenzzentrums.

Artikel 3

Auftrag des Kompetenzzentrums und des Netzwerks

(1) Der Auftrag des Kompetenzzentrums und des Netzwerks ist es, die Union zu unterstützen bei

a) der Stärkung ihrer Führungsrolle und strategischen Autonomie im Bereich der Cybersicherheit durch die Wahrung und Weiterentwicklung der forschungsbezogenen, wissenschaftlichen, gesellschaftsbezogenen, technologischen und industriellen Kapazitäten und Fähigkeiten der Union im Bereich der Cybersicherheit, die nötig sind, um das Vertrauen und die Sicherheit, einschließlich der Vertraulichkeit, Integrität und Zugänglichkeit von Daten, in den digitalen Binnenmarkt und auf diesem Markt zu steigern;

b) der Förderung der technologischen Kapazitäten, Fähigkeiten und Kompetenzen in der Union im Zusammenhang mit der Abwehrfähigkeit und Zuverlässigkeit der Infrastruktur der Netz- und Informationssysteme, darunter der kritischen Infrastruktur und der in der Union gängigen Hard- und Software; und

c) der Steigerung der globalen Wettbewerbsfähigkeit der Cybersicherheitsbranche der Union, der Gewährleistung hoher Cybersicherheitsstandards in der gesamten Union und der Verwandlung der Cybersicherheit in einen Wettbewerbsvorteil für andere Wirtschaftszweige der Union.

(2) Das Kompetenzzentrum und das Netzwerk nehmen ihre Aufgaben in Zusammenarbeit mit der ENISA und der Gemeinschaft, je nachdem, was angemessen ist, wahr.

(3) Das Kompetenzzentrum verwendet, im Einklang mit den Gesetzgebungsakten zur Einrichtung der betreffenden Programme, insbesondere „Horizont Europa“ und dem Programm „Digitales Europa“, die einschlägigen Finanzmittel der Union in einer Weise, dass ein Beitrag zu dem in Absatz 1 dargelegten Auftrag geleistet wird.

Artikel 4

Ziele des Kompetenzzentrums

(1) Das Kompetenzzentrum hat das allgemeine Ziel, die Forschung, Innovation und Realisierung im Bereich der Cybersicherheit zu fördern, um den in Artikel 3 festgelegten Auftrag zu erfüllen.

(2) Das Kompetenzzentrum hat folgende spezifische Ziele:

a) die Kapazitäten, die Fähigkeiten, das Wissen und die Infrastruktur im Bereich der Cybersicherheit zugunsten der Wirtschaft, insbesondere von KMU, der Forschungsgemeinschaften, des öffentlichen Sektors und der Zivilgesellschaft, zu verbessern, sofern angemessen,

b) die Abwehrfähigkeit im Bereich der Cybersicherheit, die Übernahme bewährter Verfahren im Bereich der Cybersicherheit, den Grundsatz der konzeptionsintegrierten Sicherheit und die Zertifizierung der Sicherheit digitaler Produkte und Dienste auf eine Art zu fördern, die die Maßnahmen anderer öffentlicher Einrichtungen ergänzt,

c) zu einem starken europäischen Cybersicherheitsökosystem, in dem alle einschlägigen Interessenträger zusammengeführt werden, beizutragen.

(3) Das Kompetenzzentrum verwirklicht die in Absatz 2 genannten spezifischen Ziele, indem es:

a) strategische Empfehlungen für Forschung, Innovation und Realisierung im Bereich der Cybersicherheit im Einklang mit dem Unionsrecht ausarbeitet und strategische Prioritäten für die Tätigkeiten des Kompetenzzentrums festlegt;

b) Maßnahmen im Rahmen der einschlägigen Finanzierungsprogramme der Union im Einklang mit den einschlägigen Arbeitsprogrammen und der Gesetzgebungsakte der Union zur Einrichtung dieser Finanzierungsprogramme durchführt;

c) die Zusammenarbeit und die Abstimmung zwischen den nationalen Koordinierungszentren sowie mit und innerhalb der Gemeinschaft fördert und

d) soweit dies sachdienlich und angemessen ist, IKT-Infrastrukturen und -Dienste entsprechend den in Artikel 5 Absatz 3 Buchstabe b aufgeführten jeweiligen Arbeitsprogrammen zu erwerben, wenn dies zur Erfüllung der in Artikel 5 genannten Aufgaben erforderlich ist.

Artikel 5

Aufgaben des Kompetenzzentrums

(1) Zur Erfüllung seines Auftrags und seiner Ziele übernimmt das Kompetenzzentrum folgende Aufgaben:

a) strategische Aufgaben und

b) Umsetzungsaufgaben.

(2) Die in Absatz 1 Buchstabe a genannten strategischen Aufgaben bestehen aus:

a) der Erarbeitung der Agenda und der Überwachung ihrer Umsetzung;

b) über die Agenda und das mehrjährige Arbeitsprogramm, unter Vermeidung von Überschneidungen mit den Tätigkeiten der ENISA und unter Berücksichtigung der Notwendigkeit von Synergien zwischen Cybersicherheit und anderen Teilen von „Horizont Europa“ und des Programms „Digitales Europa“:

   i) die Festlegung von Prioritäten für die Arbeit des Kompetenzzentrums in folgenden Bereichen:

      1. auf den gesamten Innovationszyklus ausgerichtete Ausweitung der Forschung und Innovation im Bereich der Cybersicherheit und die Realisierung dieser Forschung und Innovation;

      2. Entwicklung von Kapazitäten, Fähigkeiten und Infrastrukturen für Industrie, Technologie und Forschung im Bereich der Cybersicherheit;

      3. Verbesserung von Cybersicherheits- und Technologiekenntnissen und -kompetenzen in Industrie, Technologie und Forschung und auf allen relevanten Bildungsebenen bei gleichzeitiger Förderung eines ausgewogenen Geschlechterverhältnisses;

      4. Realisierung von Cybersicherheitsprodukten, -diensten und -verfahren;

      5. Unterstützung der Aufnahme von Cybersicherheitsprodukten, -diensten und -verfahren, die zur Erfüllung der Aufgaben gemäß Artikel 3 beitragen, am Markt;

      6. Unterstützung der Einführung und Integration modernster Cybersicherheitsprodukte, -dienste und -verfahren durch Behörden auf deren Ersuchen, durch nachfragende Branchen und durch andere Nutzer;

   ii) die Unterstützung der Cybersicherheitsbranche, insbesondere von KMU, um die Exzellenz, Kapazität und Wettbewerbsfähigkeit der Union im Hinblick auf Cybersicherheit zu stärken, auch durch Erschließung potenzieller Märkte und Realisierungsmöglichkeiten, und um Investoren zu gewinnen; und

   iii) Unterstützung und technische Hilfe für im Bereich der Cybersicherheit tätige Start-up-Unternehmen, KMU, Kleinstunternehmen, Verbände, Sachverständige und Civic-Technologie-Projekte;

c) die Gewährleistung von Synergien zwischen und Zusammenarbeit mit einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union, insbesondere der ENISA, unter Vermeidung jeglicher Doppelarbeit in Bezug auf die Tätigkeiten dieser Organe, Einrichtungen und sonstigen Stellen der Union;

d) die Koordinierung der nationalen Koordinierungszentren durch das Netzwerk und die Gewährleistung eines regelmäßigen Austauschs von Fachwissen;

e) die fachkundige Beratung von Mitgliedstaaten, auf deren Ersuchen, zu Industrie, Technologie und Forschung im Bereich der Cybersicherheit, einschließlich der Vergabe öffentlicher Aufträge und der Realisierung von Technologien;

f) die Förderung der Zusammenarbeit und des Austauschs von Fachwissen zwischen allen einschlägigen Interessenträgern, insbesondere den Mitgliedern der Gemeinschaft;

g) die Teilnahme an Unions-, nationalen und internationalen Konferenzen, Messen und Foren, die einen Bezug zu dem Auftrag, den Zielen und den Aufgaben des Kompetenzzentrums haben, um Ansichten und einschlägige bewährte Verfahren mit anderen Teilnehmern auszutauschen;

h) die Ermöglichung der Nutzung der Ergebnisse von Forschungs- und Innovationsprojekten bei Maßnahmen im Zusammenhang mit der Entwicklung von Cybersicherheitsprodukten, -diensten und -verfahren, wobei angestrebt wird, Fragmentierung und Doppelarbeit zu vermeiden und bewährte Verfahren in Bezug auf Cybersicherheitsprodukte, -dienste und -verfahren nachzubilden, insbesondere solche, die von KMU entwickelt wurden, und solche, die auf quelloffener Software beruhen;

(3) Die Umsetzungsaufgaben gemäß Absatz 1 Buchstabe b bestehen aus:

a) der Koordinierung und Verwaltung der Arbeit des Netzwerks und der Gemeinschaft zur Erfüllung des in Artikel 3 festgelegten Auftrags, insbesondere durch Unterstützung von im Bereich der Cybersicherheit tätigen Start-up-Unternehmen, KMU, Kleinstunternehmen, Verbänden und Civic-Technology-Projekten in der Union und der Erleichterung ihres Zugangs zu Fachwissen, Finanzierung, Investitionen und Märkten;

b) der Aufstellung und Durchführung des jährlichen Arbeitsprogramms im Einklang mit der Agenda und dem mehrjährigen Arbeitsprogramm in Bezug auf die die Cybersicherheit betreffenden Teile:

   i) des Programms „Digitales Europa“, insbesondere den Maßnahmen im Zusammenhang mit Artikel 6 der Verordnung (EU) 2021/694,

   ii) gemeinsamer Maßnahmen, die gemäß den die Cybersicherheit betreffenden Bestimmungen von „Horizont Europa“, insbesondere in Bezug auf Anhang I Pfeiler II Abschnitt 3.1.3 des Beschlusses (EU) 2021/764 Unterstützung erhalten, im Einklang mit dem mehrjährigen Arbeitsprogramm und dem strategischen Planungsprozess im Rahmen von „Horizont Europa“, und

   iii) anderer Programme, wenn diese in Gesetzgebungsakten der Union vorgesehen sind;

c) gegebenenfalls Unterstützung der Verwirklichung des spezifischen Ziels 4 „fortgeschrittene digitale Kompetenzen“ gemäß Artikel 7 der Verordnung (EU) 2021/694 in Zusammenarbeit mit den Europäischen Digitalen Innovationszentren;

d) fachkundiger Beratung der Kommission zu Industrie, Technologie und Forschung im Bereich der Cybersicherheit, wenn die Kommission die Entwürfe der Arbeitsprogramme gemäß Artikel 13 des Beschlusses (EU) 2021/764 erstellt;

e) der Durchführung oder Ermöglichung der Realisierung von IKT-Infrastrukturen sowie der Erleichterung der Beschaffung einer solchen Infrastruktur im Dienst der Gesellschaft, der Wirtschaft und des öffentlichen Sektors auf Ersuchen der Mitgliedstaaten, der Forschungsgemeinschaften und der Betreiber wesentlicher Dienste unter anderem durch Beiträge der Mitgliedstaaten und Finanzierungsmittel der Union für gemeinsame Maßnahmen im Einklang mit der Agenda, dem jährlichen Arbeitsprogramm und dem mehrjährigen Arbeitsprogramm.;

f) der Aufklärung über den Auftrag des Kompetenzzentrums und des Netzwerks sowie über die Ziele und Aufgaben des Kompetenzzentrums;

g) unbeschadet des zivilen Charakters der über „Horizont Europa“ zu finanzierenden Projekte und im Einklang mit den Verordnungen (EU) 2021/695 und (EU) 2021/694 die Verstärkung der Synergien und der Koordinierung zwischen dem zivilen und dem Verteidigungssektor im Bereich der Cybersicherheit, durch die Förderung des Austauschs von:

   i) Wissen und Informationen über Technologien und Anwendungen mit doppeltem Verwendungszweck,

   ii) Ergebnissen, Anforderungen und bewährten Verfahren, und

   iii) Informationen über die Prioritäten der einschlägigen Programme der Union.

(4) Das Kompetenzzentrum führt die in Absatz 1 genannten Aufgaben in enger Zusammenarbeit mit dem Netzwerk aus.

(5) Gemäß Artikel 6 der Verordnung (EU) 2021/695 und vorbehaltlich einer Beitragsvereinbarung gemäß Artikel 2 Nummer 18 der Haushaltsordnung kann das Kompetenzzentrum mit der Durchführung der die Cybersicherheit betreffenden Teile im Rahmen von „Horizont Europa", die nicht durch die Mitgliedstaaten kofinanzierten werden, insbesondere des Anhangs I Pfeiler II Abschnitt 3.1.3 des Beschlusses (EU) 2021/764, betraut werden.

Artikel 6

Benennung der nationalen Koordinierungszentren

(1) Bis zum 29. Dezember 2021 benennt jeder Mitgliedstaat eine Einrichtung, die die in Absatz 5 festgelegten Kriterien erfüllt, die als nationales Koordinierungszentrum für die Zwecke dieser Verordnung dienen soll. Jeder Mitgliedstaat notifiziert dem Verwaltungsrat diese Einrichtung unverzüglich. Bei dieser Einrichtung kann es sich um eine in dem jeweiligen Mitgliedstaat bereits bestehende Einrichtung handeln.

Die in Unterabsatz 1 dieses Absatzes genannte Frist wird um den Zeitraum verlängert, in dem die Kommission die in Absatz 2 genannte Stellungnahme abzugeben hat.

(2) Ein Mitgliedstaat kann die Kommission jederzeit um eine Stellungnahme dazu ersuchen, ob die Einrichtung, die er als nationales Koordinierungszentrum benannt hat oder zu benennen beabsichtigt, über die notwendigen Kapazitäten zur Mittelverwaltung verfügt, um den Auftrag und die Ziele gemäß dieser Verordnung erfüllen zu können. Die Kommission gibt dem betreffenden Mitgliedstaat ihre Stellungnahme innerhalb von drei Monaten nach dem Ersuchen des Mitgliedstaats ab.

(3) Auf der Grundlage der Notifizierung einer Einrichtung durch einen Mitgliedstaat gemäß Absatz 1 nimmt der Verwaltungsrat diese Einrichtung spätestens drei Monate nach der Notifizierung in die Liste der nationalen Koordinierungszentren auf. Das Kompetenzzentrum veröffentlicht die Liste der ernannten nationalen Koordinierungszentren.

(4) Ein Mitgliedstaat kann jederzeit eine neue Einrichtung als nationales Koordinierungszentrum für die Zwecke dieser Verordnung benennen. Die Absätze 1, 2 und 3 gelten für die Benennung jeder neuen Einrichtung.

(5) Das nationale Koordinierungszentrum muss eine öffentliche Einrichtung oder eine Einrichtung mit mehrheitlicher Beteiligung des Mitgliedstaats sein, die nach nationalem Recht, einschließlich durch Befugnisübertragung, Aufgaben der öffentlichen Verwaltung wahrnimmt und die Kapazität hat, das Kompetenzzentrum und das Netzwerk bei der Erfüllung ihres Auftrags gemäß Artikel 3 dieser Verordnung zu unterstützen. Es muss entweder über Fachwissen in Forschung und Technologie auf dem Gebiet der Cybersicherheit verfügen oder direkten Zugang dazu haben. Es muss die Kapazität haben, sich wirksam mit der Industrie, dem öffentlichen Sektor, Wissenschaft und Forschung, den Bürgern sowie den nach der Richtlinie (EU) 2016/1148 benannten Behörden auszutauschen und abzustimmen.

(6) Ein nationales Koordinierungszentrum können jederzeit seine Anerkennung als eine Einrichtung beantragen, die über die notwendigen Kapazitäten zur Mittelverwaltung verfügt, um den Auftrag und die Ziele gemäß dieser Verordnung im Einklang mit den Verordnungen (EU) 2021/695 und (EU) 2021/694 zu erfüllen. Innerhalb von drei Monaten nach einem solchen Antrags bewertet die Kommission, ob das betreffende nationale Koordinierungszentrum über diese Kapazitäten verfügt, und trifft eine Entscheidung.

Hat die Kommission einem Mitgliedstaat nach dem Verfahren des Absatzes 2 eine befürwortende Stellungnahme übermittelt, so gilt diese Stellungnahme als Entscheidung, mit der anerkannt wird, dass die betreffende Einrichtung über die notwendigen Kapazitäten für die Zwecke des vorliegenden Absatzes verfügt.

Spätestens bis zum 29. August 2021 gibt die Kommission nach Anhörung des Verwaltungsrats Leitlinien in Bezug auf die Bewertung nach Unterabsatz 1 heraus, einschließlich einer Präzisierung der Bedingungen für die Anerkennung und der Modalitäten für die Durchführung von Stellungnahmen und Bewertungen.

Vor Abgabe der Stellungnahme gemäß Absatz 2 und der Entscheidung gemäß Unterabsatz 1 des vorliegenden Absatzes berücksichtigt die Kommission etwaige von dem antragstellenden nationalen Koordinierungszentrum bereitgestellten Informationen und Unterlagen.

Jede Entscheidung, ein nationales Koordinierungszentrum nicht anzuerkennen, weil es nicht über die notwendigen Kapazitäten zur Mittelverwaltung verfügt, um den Auftrag und die Ziele gemäß dieser Verordnung zu erfüllen, muss hinreichend begründet werden, wobei die Anforderungen anzugeben sind, die das antragstellende nationale Koordinierungszentrum noch nicht erfüllt hat, welche die Entscheidung, die Anerkennung abzulehnen, rechtfertigen. Jedes nationale Koordinierungszentrum, dessen Antrag zur Anerkennung abgelehnt wurde, kann seinen Antrag mit zusätzlichen Informationen jederzeit erneut einreichen.

Die Mitgliedstaaten unterrichten die Kommission über Änderungen bei den nationalen Koordinierungszentren, wie beispielsweise der Zusammensetzung des nationalen Koordinierungszentrums, der Rechtsform des nationalen Koordinierungszentrums oder anderen relevanten Aspekten, die sich auf ihre Kapazitäten zur Verwaltung von Mitteln zur Erfüllung des Auftrags und der Ziele gemäß dieser Verordnung auswirken. Erhält die Kommission solche Informationen, kann sie die Entscheidung über die Anerkennung oder Ablehnung der Anerkennung der Tatsache, dass ein nationales Koordinierungszentrum über die notwendigen Kapazitäten zur Mittelverwaltung verfügt, entsprechend überprüfen.

(7) Dem Netzwerk gehören alle nationalen Koordinierungszentren an, die dem Verwaltungsrat von den Mitgliedstaaten notifiziert wurden.

Artikel 7

Aufgaben der nationalen Koordinierungszentren

(1) Die nationalen Koordinierungszentren haben folgende Aufgaben:

a) sie dienen als auf nationaler Ebene angesiedelte Anlaufstellen für die Gemeinschaft zur Unterstützung des Kompetenzzentrums bei der Erfüllung seines Auftrags und seiner Ziele, insbesondere bei der Koordinierung der Gemeinschaft durch Koordinierung der Mitglieder der Gemeinschaft in ihren Mitgliedstaaten;

b) sie stellen Fachwissen für die strategischen Aufgaben gemäß Artikel 5 Absatz 2 bereit und unterstützen aktiv bei diesen Aufgaben, unter Berücksichtigung der einschlägigen nationalen und regionalen Herausforderungen für die Cybersicherheit in verschiedenen Sektoren;

c) sie fördern und erleichtern die Beteiligung der Zivilgesellschaft, der Industrie, insbesondere von Start-up-Unternehmen und KMU, von Wissenschaft und Forschung und anderer Interessenträger auf der nationalen Ebene an grenzübergreifenden Projekten und Cybersicherheitsmaßnahmen, die im Rahmen der einschlägigen Programme der Union finanziert werden, und ermutigen diese zur Teilnahme;

d) sie stellen technische Hilfe für Interessenträger bereit, indem sie diese in der Antragsphase bei Projekten, die das Kompetenzzentrum im Rahmen seines Auftrags und seiner Ziele verwaltet, unterstützen, wobei die Regeln der wirtschaftlichen Haushaltsführung, insbesondere in Bezug auf Interessenkonflikte, uneingeschränkt einzuhalten sind;

e) sie bemühen sich um die Schaffung von Synergien mit einschlägigen Tätigkeiten auf nationaler, regionaler und lokaler Ebene, wie etwa der nationalen Forschungs-, Entwicklungs- und Innovationspolitik im Bereich der Cybersicherheit, insbesondere der Politikbereiche, die in den nationalen Cybersicherheitsstrategien aufgeführt sind;

f) sie führen spezifische Maßnahmen durch, für die das Kompetenzzentrum Finanzhilfen gewährt hat, unter anderem durch die finanzielle Unterstützung Dritter gemäß Artikel 204 der Haushaltsordnung unter den in den betreffenden Finanzhilfevereinbarungen festgelegten Bedingungen;

g) sie arbeiten mit den Behörden der Mitgliedstaaten im Hinblick auf einen möglichen Beitrag zur Förderung und Verbreitung von Schulungsprogrammen im Bereich Cybersicherheit zusammen, unbeschadet der Zuständigkeiten der Mitgliedstaaten für Bildung und unter Berücksichtigung der einschlägigen Aufgaben der ENISA;

h) sie fördern und verbreiten die einschlägigen Ergebnisse der Arbeit des Netzwerks, der Gemeinschaft und des Kompetenzzentrums auf nationaler, regionaler oder lokaler Ebene;

i) sie prüfen die Anträge von Einrichtungen, die in demselben Mitgliedstaat wie das nationale Koordinierungszentrum niedergelassen sind, auf Aufnahme in die Gemeinschaft;

j) sie unterstützen und fördern die Beteiligung einschlägiger Einrichtungen an den Tätigkeiten des Kompetenzzentrums, des Netzwerks und der Gemeinschaft und überwachen gegebenenfalls den Umfang der Beteiligung an der Forschung, Entwicklung und Realisierung im Bereich der Cybersicherheit und der Höhe der in diesem Zusammenhang gewährten öffentlichen Finanzhilfen.

(2) Für die Zwecke von Absatz 1 Buchstabe f des vorliegenden Artikels kann die finanzielle Unterstützung Dritter in jeder in Artikel 125 der Haushaltsordnung genannten Form des Beitrags der Union, auch in Form von Pauschalbeträgen, gewährt werden.

(3) Die nationalen Koordinierungszentren können auf der Grundlage der Entscheidung gemäß Artikel 6 Absatz 6 der vorliegenden Verordnung im Einklang mit Artikel 195 Absatz 1 Buchstabe d der Haushaltsordnung für die Wahrnehmung der im vorliegenden Artikel festgelegten Aufgaben eine Finanzhilfe der Union erhalten.

(4) Die nationalen Koordinierungszentren arbeiten gegebenenfalls über das Netzwerk zusammen.

Artikel 8

Die Kompetenzgemeinschaft für Cybersicherheit

(1) Die Gemeinschaft leistet einen Beitrag zu dem in Artikel 3 festgelegten Auftrag des Kompetenzzentrums und des Netzwerks und fördert, teilt und verbreitet Fachwissen auf dem Gebiet der Cybersicherheit in der gesamten Union.

(2) Die Gemeinschaft besteht aus Einrichtungen der Industrie, einschließlich KMU, Wissenschafts- und Forschungseinrichtungen, anderen einschlägigen Organisationen der Zivilgesellschaft sowie gegebenenfalls europäischen Normungsorganisationen und öffentlichen und anderen Einrichtungen, die sich mit operativen und technischen Fragen der Cybersicherheit befassen, und gegebenenfalls aus Interessenträgern aus Sektoren, die ein Interesse an Cybersicherheit haben und mit Herausforderungen in Bezug auf die Cybersicherheit konfrontiert sind. Die Gemeinschaft bringt die wichtigsten Interessenträger im Hinblick auf die technologischen, industriellen, forschungsbezogenen und wissenschaftlichen Kapazitäten im Bereich der Cybersicherheit in der Union zusammen. Sie bezieht die nationalen Koordinierungszentren, gegebenenfalls die Europäischen Digitalen Innovationszentren sowie die Organe, Einrichtungen und sonstigen Stellen der Union, die über einschlägiges Fachwissen verfügen, wie etwa die ENISA, in ihre Arbeit ein.

(3) Nur Einrichtungen, die in den Mitgliedstaaten niedergelassen sind, können als Mitglieder der Gemeinschaft registriert werden. Sie müssen nachweisen, dass sie einen Beitrag zum Auftrag leisten können, und müssen über Fachwissen auf dem Gebiet der Cybersicherheit in mindestens einem der folgenden Bereiche verfügen:

a) Wissenschaft, Forschung oder Innovation,

b) industrielle Entwicklung oder Produktentwicklung,

c) Schulung und Bildung,

d) Informationssicherheit oder Maßnahmen zur Reaktion auf Vorfälle,

e) Ethik,

f) formale und technische Normung und entsprechende Spezifikationen.

(4) Das Kompetenzzentrum registriert Einrichtungen auf deren Ersuchen als Mitglieder der Gemeinschaft, nachdem das nationale Koordinierungszentrum des Mitgliedstaats, in dem diese Einrichtungen niedergelassen sind, geprüft hat, ob diese Einrichtungen die Kriterien nach Absatz 3 des vorliegenden Artikels erfüllen. Bei dieser Prüfung werden auch alle einschlägigen nationalen Prüfungen berücksichtigt, die die nationalen zuständigen Behörden aus Sicherheitsgründen vorgenommen haben. Solche Registrierungen gelten unbefristet, können jedoch vom Kompetenzzentrum jederzeit widerrufen werden, wenn das einschlägige nationale Koordinierungszentrum der Auffassung ist, dass die betreffende Einrichtung die Kriterien nach Absatz 3 des vorliegenden Artikels nicht mehr erfüllt oder unter Artikel 136 der Haushaltsordnung fällt, oder wenn dies aus Gründen der Sicherheit gerechtfertigt ist. Wird die Mitgliedschaft in der Gemeinschaft aus Sicherheitsgründen widerrufen, so muss die Widerrufsentscheidung verhältnismäßig und begründet sein. Die nationalen Koordinierungszentren streben eine ausgewogene Vertretung der Interessenträger in der Gemeinschaft an und unterstützen aktiv die Beteiligung, insbesondere von KMU.

(5) Die nationalen Koordinierungszentren sind dazu angehalten, über das Netzwerk zusammenzuarbeiten, damit sie die Kriterien gemäß Absatz 3 und die Verfahren zur Prüfung und Registrierung von Einrichtungen gemäß Absatz 4 einheitlich anwenden.

(6) Das Kompetenzzentrum registriert einschlägige Organe, Einrichtungen und sonstige Stellen der Union als Mitglieder der Gemeinschaft, nachdem es geprüft hat, ob dieses Organ, diese Einrichtung oder sonstige Stelle der Union die Kriterien nach Absatz 3 des vorliegenden Artikels erfüllt. Solche Registrierungen gelten unbefristet, können jedoch vom Kompetenzzentrum jederzeit widerrufen werden, wenn es der Auffassung ist, dass das Organ, die Einrichtung oder sonstige Stelle der Union die Kriterien nach Absatz 3 des vorliegenden Artikels nicht mehr erfüllt oder unter Artikel 136 der Haushaltsordnung fällt.

(7) Die Vertreter der Organe, Einrichtungen und sonstigen Stellen der Union können sich an der Arbeit der Gemeinschaft beteiligen.

(8) Eine Einrichtung, die als Mitglied der Gemeinschaft registriert ist, benennt ihre Vertreter, damit ein effizienter Dialog sichergestellt ist. Diese Vertreter müssen über Fachwissen in Bezug auf Industrie, Technologie oder Forschung im Bereich der Cybersicherheit verfügen. Die Anforderungen können vom Verwaltungsrat weiter präzisiert werden, ohne den Einrichtungen bei der Benennung ihrer Vertreter übermäßige Beschränkungen aufzuerlegen.

(9) Die Gemeinschaft leistet im Einklang mit der Geschäftsordnung des Verwaltungsrats dem Exekutivdirektor und dem Verwaltungsrat durch ihre Arbeitsgruppen und insbesondere die strategische Beratungsgruppe strategische Beratung zu der Agenda, dem jährlichen Arbeitsprogramm und dem mehrjährigen Arbeitsprogramm.

Artikel 9

Aufgaben der Mitglieder der Gemeinschaft

Die Mitglieder der Gemeinschaft

a) unterstützen das Kompetenzzentrum bei der Erfüllung seines Auftrags und seiner Ziele und arbeiten hierzu eng mit dem Kompetenzzentrum und den nationalen Koordinierungszentren zusammen;

b) beteiligen sich gegebenenfalls an formellen oder informellen Tätigkeiten sowie an den in Artikel 13 Absatz 3 Buchstabe n genannten Arbeitsgruppen, um bestimmte, im jährlichen Arbeitsprogramm vorgesehene Tätigkeiten durchzuführen; und

c) unterstützen das Kompetenzzentrum und die nationalen Koordinierungszentren gegebenenfalls bei der Förderung bestimmter Projekte.

Artikel 10

Zusammenarbeit des Kompetenzzentrums mit anderen Organen, Einrichtungen und sonstigen Stellen der Union sowie mit internationalen Organisationen

(1) Um Kohärenz und Komplementarität sicherzustellen und gleichzeitig Doppelarbeit zu vermeiden, arbeitet das Kompetenzzentrum mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union zusammen, einschließlich der ENISA, des Europäischen Auswärtigen Dienstes, der Generaldirektion der Gemeinsamen Forschungsstelle der Kommission, der Europäischen Exekutivagentur für die Forschung, der Exekutivagentur des Europäischen Forschungsrats und der Europäischen Exekutivagentur für Gesundheit und Digitales, die mit dem Durchführungsbeschluss (EU) 2021/173 der Kommission ([13]) eingerichtet wurden, der einschlägigen Europäischen Digitalen Innovationszentren, des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität bei der mit der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates ([14]) eingerichteten Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung, der Europäischen Verteidigungsagentur im Zusammenhang mit den Aufgaben gemäß Artikel 5 der vorliegenden Verordnung und anderer einschlägiger Einrichtungen der Union. Das Kompetenzzentrum kann gegebenenfalls auch mit internationalen Organisationen zusammenarbeiten.

(2) Die Zusammenarbeit gemäß Absatz 1 des vorliegenden Artikels kann im Rahmen von Arbeitsvereinbarungen stattfinden. Diese Vereinbarungen werden dem Verwaltungsrat zur Genehmigung vorgelegt. Der Austausch von Verschlusssachen erfolgt im Rahmen von gemäß Artikel 36 Absatz 3 geschlossenen Verwaltungsvereinbarungen.

KAPITEL II

Organisation des Kompetenzzentrums

Artikel 11

Zusammensetzung und Struktur

(1) Die Mitglieder des Kompetenzzentrums sind die Union, vertreten durch die Kommission, und die Mitgliedstaaten.

(2) Die Struktur des Kompetenzzentrums muss die Erfüllung der Ziele nach Artikel 4 und der Aufgaben nach Artikel 5 gewährleisten und umfasst

a) einen Verwaltungsrat;

b) einen Exekutivdirektor;

c) eine strategische Beratungsgruppe.

([13]) Durchführungsbeschluss (EU) 2021/173 der Kommission vom 12. Februar 2021 zur Einrichtung der Europäischen Exekutivagentur für Klima, Infrastruktur und Umwelt, der Europäischen Exekutivagentur für Gesundheit und Digitales, der Europäischen Exekutivagentur für die Forschung, der Europäischen Exekutivagentur für den Innovationsrat und für KMU, der Exekutivagentur des Europäischen Forschungsrats sowie der Europäischen Exekutivagentur für Bildung und Kultur und zur Aufhebung der Durchführungsbeschlüsse 2013/801/EU, 2013/771/EU, 2013/778/EU, 2013/779/EU, 2013/776/EU und 2013/770/EU (ABl. L 50 vom 15.2.2021, S. 9).

([14]) Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

Abschnitt I

Verwaltungsrat

Artikel 12

Zusammensetzung des Verwaltungsrats

(1) Der Verwaltungsrat besteht aus je einem Vertreter pro Mitgliedstaat und zwei Kommissionsvertretern, die im Namen der Union handeln.

(2) Jedes Mitglied des Verwaltungsrats hat einen Stellvertreter. Der Stellvertreter vertritt das Mitglied im Fall seiner Abwesenheit.

(3) Die von den Mitgliedstaaten ernannten Mitglieder des Verwaltungsrats und deren Stellvertreter sind Bedienstete des öffentlichen Sektors ihres jeweiligen Mitgliedstaats und werden aufgrund ihrer Sachkenntnis auf dem Gebiet Forschung, Technologie und Industrie im Bereich Cybersicherheit, ihrer Fähigkeit, zur Gewährleistung der Koordinierung der Maßnahmen und Standpunkte mit ihrem jeweiligen nationalen Koordinierungszentrum oder ihrer einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen ernannt. Die Kommission ernennt ihre Mitglieder des Verwaltungsrats und deren Stellvertreter aufgrund ihrer Sachkenntnis auf dem Gebiet Cybersicherheit und Technologie oder ihrer einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen sowie ihrer Fähigkeit zur Gewährleistung von Koordinierung, Synergien und — soweit möglich — gemeinsamen Initiativen zwischen verschiedenen sektoralen und horizontalen Strategien der Union im Zusammenhang mit Cybersicherheit. Die Kommission und die Mitgliedstaaten bemühen sich, die Fluktuation bei ihren Vertretern im Verwaltungsrat gering zu halten, um die Kontinuität der Arbeit des Verwaltungsrats sicherzustellen. Die Kommission und die Mitgliedstaaten setzen sich für eine ausgewogene Vertretung von Frauen und Männern im Verwaltungsrat ein.

(4) Die Amtszeit der Mitglieder des Verwaltungsrats und ihrer Stellvertreter beträgt vier Jahre. Sie kann verlängert werden.

(5) Die Mitglieder des Verwaltungsrats stellen in unabhängiger und transparenter Weise sicher, dass der Auftrag, die Ziele, die Identität und die Eigenständigkeit des Kompetenzzentrums gewahrt werden und dass dessen Maßnahmen mit jenem Auftrag und jenen Zielen übereinstimmen.

(6) Der Verwaltungsrat kann gegebenenfalls Beobachter einladen, die an den Sitzungen des Verwaltungsrats teilnehmen, darunter Vertreter der einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitglieder der Gemeinschaft.

(7) Ein Vertreter der ENISA ist ständiger Beobachter im Verwaltungsrat. Der Verwaltungsrat kann einen Vertreter der strategischen Beratungsgruppe einladen, an seinen Sitzungen teilzunehmen.

(8) Der Exekutivdirektor nimmt an den Sitzungen des Verwaltungsrats teil, hat jedoch kein Stimmrecht.

Artikel 13

Aufgaben des Verwaltungsrats

(1) Der Verwaltungsrat trägt die Gesamtverantwortung für die strategische Ausrichtung und die Geschäfte des Kompetenzzentrums, beaufsichtigt die Durchführung seiner Tätigkeiten und ist zuständig für alle Aufgaben, die nicht ausdrücklich dem Exekutivdirektor übertragen wurden.

(2) Der Verwaltungsrat gibt sich eine Geschäftsordnung. Diese Geschäftsordnung beinhaltet spezielle Verfahren zur Ermittlung und Vermeidung von Interessenkonflikten und gewährleistet die Vertraulichkeit sensibler Informationen.

(3) Der Verwaltungsrat trifft die erforderlichen strategischen Entscheidungen, insbesondere im Hinblick auf:

a) die Ausarbeitung und Annahme der Agenda und die Überwachung ihrer Durchführung;

b) die Annahme — unter Berücksichtigung der politischen Prioritäten der Union und der Agenda — des mehrjährigen Arbeitsprogramms, in dem die gemeinsamen Prioritäten für Industrie, Technologie und Forschung auf der Grundlage der von den Mitgliedstaaten in Zusammenarbeit mit der Gemeinschaft ermittelten Bedürfnisse enthalten sind, auf die sich die finanzielle Unterstützung seitens der Union konzentrieren muss, einschließlich der Schlüsseltechnologien und -bereiche für die Entwicklung der eigenen Fähigkeiten der Union im Bereich der Cybersicherheit;

c) die Annahme des jährlichen Arbeitsprogramms für die Verwendung der einschlägigen Mittel der Union, insbesondere für die Umsetzung der die Cybersicherheit betreffenden Teile von „Horizont Europa“, soweit sie von den Mitgliedstaaten freiwillig kofinanziert werden, und des Programms „Digitales Europa“ im Einklang mit dem mehrjährigen Arbeitsprogramm des Kompetenzzentrums und dem Strategieplanungsprozess im Rahmen von „Horizont Europa“;

d) die Annahme des Jahresabschlusses und der Bilanz sowie des jährlichen Tätigkeitsberichts des Kompetenzzentrums auf der Grundlage eines Vorschlags des Exekutivdirektors;

e) die Annahme der eigenen Finanzordnung des Kompetenzzentrums gemäß Artikel 70 der Haushaltsordnung;

f) die Zuweisung von Mitteln aus dem Haushaltsplan der Union für Themenbereiche mit gemeinsamen Maßnahmen von Union und Mitgliedstaaten als Teil des jährlichen Arbeitsprogramms;

g) die Beschreibung der in Buchstabe f des vorliegenden Unterabsatzes genannten gemeinsamen Maßnahmen und die Festlegung der Bedingungen für deren Durchführung solcher gemeinsamer Maßnahmen im Rahmen des jährlichen Arbeitsprogramms und im Einklang mit den in Buchstabe f genannten Beschlüssen und gemäß den Verordnungen (EU) 2021/695 und (EU) 2021/694;

h) die Annahme eines Verfahrens zur Ernennung des Exekutivdirektors sowie die Ernennung und Abberufung des Exekutivdirektors, die Verlängerung seiner Amtszeit, die Vorgabe von Leitlinien für den Exekutivdirektor und die Beaufsichtigung der Leistung des Exekutivdirektors;

i) die Annahme von Leitlinien zur Prüfung und Registrierung von Einrichtungen als Mitglieder der Gemeinschaft;

j) die Annahme der in Artikel 10 Absatz 2 genannten Arbeitsvereinbarungen;

k) die Ernennung des Rechnungsführers;

l) die Annahme des jährlichen Haushaltsplans des Kompetenzzentrums, einschließlich des entsprechenden Stellenplans mit Angabe der Zahl der Planstellen auf Zeit nach Funktions- und Besoldungsgruppe, mit der Zahl der Vertragsbediensteten und abgeordneten nationalen Sachverständigen in Vollzeitäquivalenten;

m) die Annahme von Transparenzvorschriften für das Kompetenzzentrum und von Vorschriften zur Vermeidung von und zum Umgang mit Interessenkonflikten — auch in Bezug auf die Mitglieder des Verwaltungsrates — gemäß Artikel 42 der Delegierten Verordnung (EU) 2019/715;

n) die Einrichtung von Arbeitsgruppen innerhalb der Gemeinschaft, gegebenenfalls unter Berücksichtigung der Empfehlungen der strategischen Beratungsgruppe;

o) die Ernennung der Mitglieder der strategischen Beratungsgruppe;

p) die Annahme von Vorschriften über die Kostenerstattung für Mitglieder der strategischen Beratungsgruppe;

q) die Einrichtung eines Überwachungsmechanismus, um sicherzustellen, dass die Verwendung der entsprechenden vom Kompetenzzentrum verwalteten Mittel im Einklang mit der Agenda, dem Auftrag, dem mehrjährigen Arbeitsprogramm sowie den Vorschriften der Programme, aus denen die jeweilige Finanzierung stammt, erfolgt;

r) die Gewährleistung eines regelmäßigen Dialogs und die Einrichtung eines wirksamen Mechanismus für die Zusammenarbeit mit der Gemeinschaft;

s) die Festlegung der Kommunikationspolitik des Kompetenzzentrums auf Grundlage einer Empfehlung des Exekutivdirektors;

t) gegebenenfalls die Festlegung von Durchführungsbestimmungen zum Statut der Beamten der Europäischen Union und die Beschäftigungsbedingungen für die sonstigen Bediensteten der Union gemäß der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates ([15]) (im Folgenden „Statut der Beamten“ und „Beschäftigungsbedingungen“) nach Artikel 30 Absatz 3 der vorliegenden Verordnung;

u) gegebenenfalls die Festlegung von Bestimmungen über die Abstellung nationaler Sachverständiger zum Kompetenzzentrum und über den Einsatz von Praktikanten nach Artikel 31 Absatz 2;

v) die Annahme von Sicherheitsvorschriften für das Kompetenzzentrum;

w) die Annahme einer Betrugs- und Korruptionsbekämpfungsstrategie, die den diesbezüglichen Betrugs- und Korruptionsrisiken entspricht, sowie die Annahme von umfassenden Maßnahmen — im Einklang mit den geltenden Rechtsvorschriften der Union — zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, unter Berücksichtigung einer Kosten-Nutzen-Analyse der durchzuführenden Maßnahmen;

x) erforderlichenfalls die Festlegung der Methode zur Berechnung des freiwilligen Finanzbeitrags der beitragenden Mitgliedstaaten und ihres freiwilligen Beitrags in Form von Sachleistungen im Einklang mit den Verordnungen (EU) 2021/695 und (EU) 2021/694 oder anderer anwendbarer Gesetzgebung;

([15]) ABl. L 56 vom 4.3.1968, S. 1.

y) die Gewährleistung von Kohärenz und Synergien mit den nicht vom Kompetenzzentrum verwalteten Teilen der Programme „Digitales Europa“ und von „Horizont Europa“ sowie mit anderen Unionsprogrammen im Zusammenhang mit dem jährlichen Arbeitsprogramm und dem mehrjährigen Arbeitsprogramm;

z) die Annahme des jährlichen Berichts über die Verwirklichung der strategischen Ziele und Prioritäten des Kompetenzzentrums, erforderlichenfalls mit einer Empfehlung für eine bessere Verwirklichung dieser Ziele und Prioritäten.

Sofern im Jahresarbeitsprogramm gemeinsame Maßnahmen vorgesehen sind, enthält es Informationen über die freiwilligen Beiträge der Mitgliedstaaten zu gemeinsamen Maßnahmen. Gegebenenfalls wird in Vorschlägen, insbesondere im Vorschlag für das jährliche Arbeitsprogramm, bewertet, ob es notwendig ist, die Sicherheitsvorschriften gemäß Artikel 33 der vorliegenden Verordnung, einschließlich des Sicherheitsselbstbewertungsverfahrens gemäß Artikel 20 der Verordnung (EU) 2021/695 anzuwenden;

(4) Bezüglich der in Absatz 3 Buchstaben a, b und c festgelegten Entscheidungen haben der Exekutivdirektor und der Verwaltungsrat im Einklang mit der vom Verwaltungsrat festgelegten Geschäftsordnung einschlägige strategische Beratung durch die und Beiträge der ENISA zu berücksichtigen.

(5) Der Verwaltungsrat ist dafür verantwortlich, sicherzustellen, dass adäquate Folgemaßnahmen zu den Empfehlungen, die im Durchführungsbericht und in der Bewertung, die in Artikel 38 Absatz 2 und Absatz 4 genannt sind, durchgeführt werden.

Artikel 14

Vorsitz und Sitzungen des Verwaltungsrats

(1) Der Verwaltungsrat wählt aus dem Kreis seiner Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden für einen Zeitraum von jeweils drei Jahren. Die Amtszeit des Vorsitzenden und des stellvertretenden Vorsitzenden kann einmal auf Beschluss des Verwaltungsrats verlängert werden. Endet jedoch die Mitgliedschaft des Vorsitzenden oder des stellvertretenden Vorsitzenden im Verwaltungsrat während ihrer Amtszeit, so endet auch ihre Amtszeit automatisch zu diesem Zeitpunkt. Der stellvertretende Vorsitzende tritt im Fall der Verhinderung des Vorsitzenden von Amts wegen an dessen Stelle. Der Vorsitzende nimmt an den Abstimmungen teil.

(2) Der Verwaltungsrat hält mindestens dreimal jährlich ordentliche Sitzungen ab. Außerordentliche Sitzungen können auf Antrag der Kommission, auf Antrag eines Drittels aller Mitglieder des Verwaltungsrats, auf Antrag des Vorsitzenden oder auf Antrag des Exekutivdirektors in Wahrnehmung seiner Aufgaben einberufen werden.

(3) Der Exekutivdirektor beteiligt sich an den Beratungen des Verwaltungsrats, sofern der Verwaltungsrat nichts anderes beschließt, verfügt jedoch über kein Stimmrecht.

(4) Der Verwaltungsrat kann im Einzelfall andere Personen einladen, um an den Sitzungen als Beobachter teilzunehmen.

(5) Der Vorsitzende kann Vertreter der Gemeinschaft einladen, an den Sitzungen des Verwaltungsrats teilzunehmen; sie besitzen jedoch kein Stimmrecht.

(6) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter können sich nach Maßgabe der Geschäftsordnung des Verwaltungsrats in den Sitzungen von Beratern oder Sachverständigen unterstützen lassen.

(7) Die Sekretariatsgeschäfte des Verwaltungsrats werden vom Kompetenzzentrum wahrgenommen.

Artikel 15

Abstimmungsregeln des Verwaltungsrats

(1) Der Verwaltungsrat verfolgt bei seinen Beratungen einen konsensorientierten Ansatz. Eine Abstimmung findet statt, wenn die Mitglieder des Verwaltungsrats keinen Konsens erzielen konnten.

(2) Kann der Verwaltungsrat keinen Konsens bei einer Angelegenheit erzielen, so fasst er seine Beschlüsse mit einer Mehrheit von mindestens 75 % der Stimmen aller Mitglieder, wobei die Vertreter der Kommission zu diesem Zweck ein einziges Mitglied darstellen. Ein abwesendes Mitglied des Verwaltungsrats kann sein Stimmrecht auf seinen Stellvertreter oder — bei Abwesenheit seines Stellvertreters — auf ein anderes Mitglied übertragen. Ein Mitglied des Verwaltungsrats darf höchstens ein anderes Mitglied vertreten.

(3) Beschlüsse des Verwaltungsrats zu den gemeinsamen Maßnahmen und deren Verwaltung gemäß Artikel 13 Absatz 3 Buchstaben f und g werden wie folgt gefasst:

a) Beschlüsse über die Zuweisung von Mitteln aus dem Haushaltsplan der Union für gemeinsame Maßnahmen gemäß Artikel 13 Absatz 3 Buchstabe f sowie Beschlüsse über die Aufnahme der betreffenden gemeinsamen Maßnahmen in das jährliche Arbeitsprogramm werden gemäß Absatz 2 des vorliegenden Artikels gefasst.

b) Beschlüsse im Zusammenhang mit der Beschreibung der gemeinsamen Maßnahmen und zur Festlegung der Bedingungen für deren Durchführung gemäß Artikel 13 Absatz 3 Buchstabe g werden von den teilnehmenden Mitgliedstaaten und der Kommission gefasst, wobei die Stimmrechte der Mitglieder im Verhältnis zu dem entsprechenden Beitrag stehen, den sie gemäß der nach Artikel 13 Absatz 3 Buchstabe x festgelegten Methode zu der betreffenden gemeinsamen Maßnahme geleistet haben.

(4) Bei Beschlüssen, die gemäß Artikel 13 Absatz 3 Buchstaben b, c, d, e, f, k, l, p, q, t, u, w, x und y gefasst werden, verfügt die Kommission über 26 % aller Stimmen im Verwaltungsrat.

(5) Bei anderen als den in Absatz 3 Buchstabe b und in Absatz 4 genannten Beschlüssen verfügen jeder Mitgliedstaat und die Union über jeweils eine Stimme. Die Stimme der Union wird gemeinsam von den beiden Vertretern der Kommission abgegeben.

(6) Der Vorsitzende nimmt an der Abstimmung teil.

Abschnitt II

Exekutivdirektor

Artikel 16

Ernennung und Abberufung des Exekutivdirektors und Verlängerung seiner Amtszeit

(1) Der Exekutivdirektor ist eine Person mit Fachwissen und hohem Ansehen auf den Gebieten, auf denen das Kompetenzzentrum tätig ist.

(2) Der Exekutivdirektor wird als Zeitbediensteter des Kompetenzzentrums nach Artikel 2 Buchstabe a der Beschäftigungsbedingungen eingestellt.

(3) Der Exekutivdirektor wird vom Verwaltungsrat auf der Grundlage einer Liste von Bewerbern ernannt, die die Kommission im Anschluss an ein offenes, transparentes und diskriminierungsfreies Auswahlverfahren vorschlägt.

(4) Für den Abschluss des Vertrags mit dem Exekutivdirektor wird das Kompetenzzentrum durch den Vorsitzenden des Verwaltungsrats vertreten.

(5) Die Amtszeit des Exekutivdirektors beträgt vier Jahre. Vor dem Ende dieses Zeitraums nimmt die Kommission eine Bewertung vor, bei der die Leistung des Exekutivdirektors und die künftigen Aufgaben und Herausforderungen des Kompetenzzentrums berücksichtigt werden.

(6) Der Verwaltungsrat kann auf einen Vorschlag der Kommission, der die Bewertung nach Absatz 5 berücksichtigt, die Amtszeit des Exekutivdirektors einmal um höchstens vier Jahre verlängern.

(7) Ein Exekutivdirektor, dessen Amtszeit verlängert wurde, darf nicht an einem anderen Auswahlverfahren für dieselbe Stelle teilnehmen.

(8) Der Exekutivdirektor kann nur durch einen Beschluss des Verwaltungsrats auf Vorschlag der Kommission oder von mindestens 50 % der Mitgliedstaaten seines Amtes enthoben werden.

Artikel 17

Aufgaben des Exekutivdirektors

(1) Der Exekutivdirektor ist für den Betrieb und die laufende Geschäftsführung des Kompetenzzentrums verantwortlich und ist dessen gesetzlicher Vertreter. Der Exekutivdirektor ist gegenüber dem Verwaltungsrat rechenschaftspflichtig und nimmt seine Aufgaben im Rahmen der ihm übertragenen Befugnisse völlig unabhängig wahr. Der Exekutivdirektor wird vom Personal des Kompetenzzentrums unterstützt.

(2) Der Exekutivdirektor erfüllt mindestens folgende Aufgaben in unabhängiger Weise:

a) Durchführung der vom Verwaltungsrat gefassten Beschlüsse;

b) Unterstützung des Verwaltungsrats bei seiner Arbeit, Wahrnehmung der Sekretariatsgeschäfte für seine Sitzungen und Bereitstellung aller zur Wahrnehmung seiner Aufgaben erforderlichen Informationen;

c) Ausarbeitung und Vorlage des Entwurfs der Agenda sowie — im Einklang mit der Agenda — des Entwurfs des mehrjährigen Arbeitsprogramms und des Entwurfs des jährlichen Arbeitsprogramms des Kompetenzzentrums zur Annahme durch den Verwaltungsrat, einschließlich Angaben zum Umfang der Aufforderungen zur Einreichung von Vorschlägen, der Aufforderungen zur Interessenbekundung und der Ausschreibungen, die für die Durchführung des jährlichen Arbeitsprogramms erforderlich sind, sowie der entsprechenden von den Mitgliedstaaten und der Kommission vorgelegten Ausgabenvoranschläge; dies geschieht nach Anhörung des Verwaltungsrats und der Kommission und unter Berücksichtigung der Beiträge der nationalen Koordinierungszentren und der Gemeinschaft;

d) Ausarbeitung und Vorlage des Entwurfs des jährlichen Haushaltsplans zur Annahme durch den Verwaltungsrat, einschließlich des entsprechenden Stellenplans gemäß Artikel 13 Absatz 3 Buchstabe l mit Angabe der Zahl der Planstellen auf Zeit je Besoldungs- und Funktionsgruppe sowie der Zahl der Vertragsbediensteten und abgeordneten nationalen Sachverständigen, ausgedrückt in Vollzeitäquivalenten;

e) Durchführung des jährlichen Arbeitsprogramms und des mehrjährigen Arbeitsprogramms und Berichterstattung darüber an den Verwaltungsrat;

f) Ausarbeitung des Entwurfs des jährlichen Tätigkeitsberichts des Kompetenzzentrums mit den Angaben über die entsprechenden Ausgaben und die Durchführung der Agenda und des mehrjährigen Arbeitsprogramms; erforderlichenfalls werden diesem Bericht Vorschläge für eine weitere Verbesserung der Verwirklichung oder für die Neuformulierung der strategischen Ziele und Prioritäten beigefügt;

g) Gewährleistung der Durchführung wirksamer Überwachungs- und Bewertungsverfahren in Bezug auf die Leistung des Kompetenzzentrums;

h) Ausarbeitung eines Aktionsplans mit Folgemaßnahmen zu den Schlussfolgerungen des Durchführungsberichts und der Bewertung, die in Artikel 38 Absatz 2 und Absatz 4 genannt sind, und alle zwei Jahre Übermittlung von Fortschrittsberichten an das Europäische Parlament und die Kommission;

i) Ausarbeitung und Abschluss von Vereinbarungen mit den nationalen Koordinierungszentren;

j) Wahrnehmung der Zuständigkeit für Verwaltungs-, Finanz- und Personalangelegenheiten, einschließlich der Ausführung des Haushaltsplans des Kompetenzzentrums, wobei die Beratung durch die einschlägige interne Auditstelle im Einklang mit den Beschlüssen gemäß Artikel 13 Absatz 3 Buchstaben e, l, t, u, v und w gebührend zu berücksichtigen ist;

k) Genehmigung und Verwaltung der Einleitung von Aufforderungen zur Einreichung von Vorschlägen entsprechend dem jährlichen Arbeitsprogramm und Verwaltung der sich daraus ergebenden Finanzhilfevereinbarungen und -beschlüsse;

l) Genehmigung der Liste der Maßnahmen, die auf der Grundlage einer von einer unabhängigen Sachverständigengruppe erstellten Rangliste für eine Finanzierung ausgewählt wurden;

m) Genehmigung und Verwaltung der Einleitung von Ausschreibungen entsprechend dem jährlichen Arbeitsprogramm und Verwaltung der sich daraus ergebenden Verträge;

n) Genehmigung der Angebote, die für eine Finanzierung ausgewählt wurden;

o) Vorlage des Entwurfs des Jahresabschlusses und der Bilanz bei der einschlägigen internen Auditstelle und anschließend beim Verwaltungsrat;

p) Gewährleistung der Durchführung von Risikobewertungen und eines Risikomanagements;

q) Unterzeichnung einzelner Finanzhilfevereinbarungen, Beschlüsse und Verträge;

r) Unterzeichnung der Verträge über öffentliche Aufträge;

s) Ausarbeitung eines Aktionsplans mit Folgemaßnahmen zu den Schlussfolgerungen interner oder externer Prüfberichte sowie der Untersuchungen des mit dem Beschluss 1999/352/EG, EGKS, Euratom der Kommission ([16]) errichteten Europäischen Amtes für Betrugsbekämpfung (OLAF) und alle zwei Jahre Berichterstattung über die erzielten Fortschritte an die Kommission sowie regelmäßig an den Verwaltungsrat;

t) Ausarbeitung des Entwurfs der für das Kompetenzzentrum geltenden Finanzordnung;

u) Einrichtung eines wirksamen und effizienten internen Kontrollsystems und Sicherstellung seines ordnungsgemäßen Funktionierens sowie Meldung bedeutsamer diesbezüglicher Änderungen an den Verwaltungsrat;

([16]) Beschluss 1999/352/EG, EGKS, Euratom der Kommission vom 28. April 1999 zur Errichtung des Europäischen Amtes für Betrugsbekämpfung (OLAF) (ABl. L 136 vom 31.5.1999, S. 20).

v) Gewährleistung einer wirksamen Kommunikation mit den Organen der Union und auf Ersuchen Berichterstattung an das Europäische Parlament und den Rat;

w) Ergreifung sonstiger Maßnahmen, die zur Beurteilung der Erfüllung des Auftrags und der Ziele des Kompetenzzentrums erforderlich sind;

x) Ausführung der ihm vom Verwaltungsrat übertragenen sonstigen Aufgaben.

Abschnitt III

Strategische Beratungsgruppe

Artikel 18

Zusammensetzung der strategischen Beratungsgruppe

(1) Die strategische Beratungsgruppe besteht aus höchstens 20 Mitgliedern. Die Mitglieder werden vom Verwaltungsrat auf Vorschlag des Exekutivdirektors aus dem Kreis der Vertreter der Mitglieder der Gemeinschaft, bei denen es sich nicht um Vertreter von Organen, Einrichtungen und sonstigen Stellen der Union handelt, ernannt. Es kommen nur Vertreter von Mitgliedern infrage, die nicht von einem Drittland oder einer Einrichtung mit Sitz in einem Drittland kontrolliert werden. Die Ernennung erfolgt nach Maßgabe eines offenen, transparenten und diskriminierungsfreien Verfahrens. Der Verwaltungsrat verfolgt bei der Zusammensetzung der strategischen Beratungsgruppe das Ziel, im Hinblick auf die Vertretung in der Gemeinschaft ein ausgewogenes Verhältnis zwischen wissenschaftlichen, wirtschaftlichen und zivilgesellschaftlichen Einrichtungen, nachfrage- und angebotsseitigen Branchen, großen Unternehmen und KMU, sowie ein ausgewogenes Verhältnis in Bezug auf geographische Herkunft und Geschlecht, zu erreichen. Bei der Zusammensetzung der strategischen Beratungsgruppe wird auch das Ziel verfolgt, im Interesse des Zusammenhalts der Union und aller Mitgliedstaaten im Bereich der Cybersicherheit bei Forschung, Industrie und Technologie ein intrasektorales Gleichgewicht zu erreichen. Die strategische Beratungsgruppe setzt sich so zusammen, dass ein umfassender, kontinuierlicher und ständiger Dialog zwischen der Gemeinschaft und dem Kompetenzzentrum ermöglicht wird.

(2) Die Mitglieder der strategischen Beratungsgruppe verfügen über Fachwissen in Bezug auf Forschung und industrielle Entwicklung sowie Angebot, Umsetzung bzw. Realisierung gewerblicher Dienstleistungen oder entsprechender Produkte im Bereich der Cybersicherheit. Die Anforderungen in Bezug auf solches Fachwissen werden vom Verwaltungsrat genauer festgelegt.

(3) Die Verfahren für die Ernennung der Mitglieder der strategischen Beratungsgruppe und die Arbeitsweise der strategischen Beratungsgruppe werden in der Geschäftsordnung des Verwaltungsrats festgelegt und veröffentlicht.

(4) Die Amtszeit der Mitglieder der strategischen Beratungsgruppe beträgt zwei Jahre. Sie kann einmal verlängert werden.

(5) Vertreter der Kommission und anderer Organe, Einrichtungen und sonstigen Stellen der Union, insbesondere der ENISA, können von der strategischen Beratungsgruppe dazu eingeladen werden, sich an ihrer Arbeit zu beteiligen und diese zu unterstützen. Die strategische Beratungsgruppe kann im Einzelfall gegebenenfalls zusätzliche Vertreter der Gemeinschaft als Beobachter, Berater oder Sachverständige einladen, um der Entwicklungsdynamik im Bereich der Cybersicherheit Rechnung zu tragen. Die Mitglieder des Verwaltungsrats können als Beobachter an den Sitzungen der strategischen Beratungsgruppe teilnehmen.

Artikel 19

Arbeitsweise der strategischen Beratungsgruppe

(1) Die strategische Beratungsgruppe tritt mindestens dreimal im Jahr zusammen.

(2) Die strategische Beratungsgruppe berät den Verwaltungsrat bei der Einrichtung von Arbeitsgruppen innerhalb der Gemeinschaft gemäß Artikel 13 Absatz 3 Buchstabe n zu bestimmten Fragen, die für die Arbeit des Kompetenzzentrums von Bedeutung sind, sofern diese direkt mit den in Artikel 20 genannten Aufgaben und Zuständigkeiten zusammenhängen. Falls erforderlich unterliegen diese Arbeitsgruppen der Gesamtkoordinierung durch ein Mitglied oder mehrere Mitglieder der strategischen Beratungsgruppe.

(3) Die strategische Beratungsgruppe wählt ihren Vorsitzenden mit einfacher Mehrheit ihrer Mitglieder.

(4) Die Sekretariatsgeschäfte der strategischen Beratungsgruppe werden vom Exekutivdirektor und dem Personal des Kompetenzzentrums unter Verwendung der vorhandenen Ressourcen und unter gebührender Berücksichtigung der Arbeitsbelastung des Kompetenzzentrums wahrgenommen. Die für die Unterstützung der strategischen Beratungsgruppe zugewiesenen Mittel werden im Entwurf des jährlichen Haushaltsplans ausgewiesen.

(5) Die strategische Beratungsgruppe gibt sich mit einfacher Mehrheit ihrer Mitglieder eine Geschäftsordnung.

Artikel 20

Aufgaben der strategischen Beratungsgruppe

Die strategische Beratungsgruppe berät das Kompetenzzentrum regelmäßig bei der Durchführung seiner Tätigkeiten und sorgt für die Kommunikation mit der Gemeinschaft und anderen einschlägigen Interessenträgern. Die strategische Beratungsgruppe

a) unterstützt den Exekutivdirektor und den Verwaltungsrat innerhalb der vom Verwaltungsrat festgelegten Fristen und gegebenenfalls unter Berücksichtigung der Beiträge der Gemeinschaft und der in Artikel 13 Absatz 3 Buchstabe n genannten Arbeitsgruppen durch ständig aktualisierte strategische Beratung und Beiträge zur Agenda, zum jährlichen Arbeitsprogramm und zum mehrjährigen Arbeitsprogramm;

b) berät den Verwaltungsrat bezüglich der Einrichtung von Arbeitsgruppen innerhalb der Gemeinschaft gemäß Artikel 13 Absatz 3 Buchstabe n zu spezifischen Fragen, die für die Arbeit des Kompetenzzentrums von Belang sind;

c) beschließt und organisiert öffentliche Konsultationen, die vom Verwaltungsrat zu genehmigen sind und an denen alle öffentlichen und privaten Akteure teilnehmen können, die ein Interesse im Bereich der Cybersicherheit haben, um Beiträge für die in Buchstabe a genannte strategische Beratung zu sammeln.

KAPITEL III

Finanzbestimmungen

Artikel 21

Finanzbeiträge der Union und der Mitgliedstaaten

(1) Das Kompetenzzentrum wird von der Union und gemeinsame Maßnahmen werden von der Union und durch freiwillige Beiträge der Mitgliedstaaten finanziert.

(2) Die Verwaltungs- und Betriebskosten bei gemeinsamen Maßnahmen werden von der Union und den Mitgliedstaaten, die zu den gemeinsamen Maßnahmen beitragen, im Einklang mit den Verordnungen (EU) 2021/695 und (EU) 2021/694 getragen.

(3) Der Beitrag der Union zur Deckung der Verwaltungs- und Betriebskosten des Kompetenzzentrums besteht aus

a) höchstens 1 649 566 000 EUR aus dem Programm „Digitales Europa", davon höchstens 32 000 000 EUR für Verwaltungskosten;

b) einem Betrag aus „Horizont Europa" — auch für Verwaltungskosten — für gemeinsame Maßnahmen, der dem Betrag der von den Mitgliedstaaten gemäß Absatz 7 des vorliegenden Artikels geleisteten Beiträge entspricht, jedoch nicht den Betrag übersteigt, der in dem gemäß Artikel 6 Absatz 6 der Verordnung (EU) 2021/695 durchzuführenden strategischen Planungsprozess von „Horizont Europa", im jährlichen Arbeitsprogramm oder im mehrjährigen Arbeitsprogramm festgelegt ist;

c) einem Betrag aus den anderen einschlägigen Programmen der Union, sofern er für die Durchführung der Aufgaben oder die Verwirklichung der Ziele des Kompetenzzentrums erforderlich ist, vorbehaltlich der gemäß den Rechtsakten der Union zur Aufstellung dieser Programme gefassten Beschlüsse.

(4) Der Höchstbeitrag der Union wird aus den Mitteln des Gesamthaushaltsplans der Union für das Programm „Digitales Europa", das mit dem Beschluss (EU) 2021/764 festgelegte Spezifische Programm zur Durchführung von „Horizont Europa" und andere Programme und Projekte, die in das Tätigkeitsfeld des Kompetenzzentrums oder des Netzwerks fallen, bereitgestellt.

(5) Das Kompetenzzentrum führt die Cybersicherheitsmaßnahmen im Rahmen des Programms „Digitales Europa" und von „Horizont Europa" im Einklang mit Artikel 62 Absatz 1 Unterabsatz 1 Buchstabe c Ziffer iv der Haushaltsordnung durch.

(6) Beiträge aus anderen als den in den Absätzen 3 und 4 aufgeführten Unionsprogrammen, die Teil der Kofinanzierung seitens der Union für ein von einem der Mitgliedstaaten durchgeführtes Programm sind, werden bei der Berechnung des Höchstbetrags des Finanzbeitrags der Union gemäß den genannten Absätzen nicht angerechnet.

(7) Die Mitgliedstaaten beteiligen sich durch Finanzbeiträge und/oder Beiträge in Form von Sachleistungen freiwillig an gemeinsamen Maßnahmen. Beteiligt sich ein Mitgliedstaat an einer gemeinsamen Maßnahme, so deckt der Finanzbeitrag dieses Mitgliedstaats die Verwaltungskosten im Verhältnis zu seinem Beitrag zu dieser gemeinsamen Maßnahme. Die Verwaltungskosten gemeinsamer Maßnahmen werden durch Finanzbeiträge gedeckt. Die Betriebskosten bei gemeinsamen Maßnahmen können gemäß „Horizont Europa" und dem Programm „Digitales Europa" durch einen Finanzbeitrag oder als Beitrag in Form von Sachleistungen gedeckt werden. Beiträge eines Mitgliedstaats können als Unterstützung erfolgen, die der jeweilige Mitgliedstaat im Rahmen einer gemeinsamen Maßnahme Begünstigten leistet, die in dem betreffenden

Mitgliedstaat niedergelassen sind. Beiträge der Mitgliedstaaten in Form von Sachleistungen bestehen aus den den nationalen Koordinierungszentren und anderen öffentlichen Einrichtungen bei der Beteiligung an im Rahmen dieser Verordnung finanzierten Projekten entstehenden förderfähigen Kosten abzüglich eines etwaigen Beitrags der Union zu diesen Kosten. Bei im Rahmen von „Horizont Europa" finanzierten Projekten werden die förderfähigen Kosten im Einklang mit Artikel 36 der Verordnung (EU) 2021/695 berechnet. Bei im Rahmen des Programms „Digitales Europa" finanzierten Projekten werden die förderfähigen Kosten im Einklang mit der Haushaltsordnung berechnet.

Der veranschlagte Gesamtbetrag der freiwilligen Beiträge der Mitgliedstaaten zu gemeinsamen Maßnahmen im Rahmen von „Horizont Europa" — einschließlich der Finanzbeiträge für Verwaltungskosten — wird im Hinblick auf die Berücksichtigung in dem gemäß Artikel 6 Absatz 6 der Verordnung (EU) 2021/695 durchzuführenden strategischen Planungsprozess unter Mitwirkung des Verwaltungsrats festgelegt. Für Maßnahmen im Rahmen des Programms „Digitales Europa" können die Mitgliedstaaten unbeschadet des Artikels 15 der Verordnung (EU) 2021/694 einen Beitrag zu den über das Programm „Digitales Europa" kofinanzierten Kosten des Kompetenzzentrums leisten, der unter den in Absatz 3 Buchstabe a des vorliegenden Artikels angegebenen Beträgen liegt.

(8) Nationale Kofinanzierungen von durch andere Programme der Union als „Horizont Europa" und dem Programm „Digitales Europa" unterstützten Maßnahmen durch die Mitgliedstaaten gelten als nationale Beiträge der Mitgliedstaaten, soweit diese Beiträge Teil gemeinsamer Maßnahmen sind und in das Arbeitsprogramm des Kompetenzzentrums aufgenommen wurden.

(9) Für die Zwecke der Bewertung der Beiträge nach Absatz 3 des vorliegenden Artikels und Artikel 22 Absatz 2 Buchstabe b werden Kosten nach den üblichen Kostenrechnungsverfahren des betreffenden Mitgliedstaats, den geltenden Rechnungslegungsgrundsätzen des betreffenden Mitgliedstaats und den relevanten internationalen Rechnungslegungsstandards bestimmt. Kosten werden von einem unabhängigen externen Rechnungsprüfer zertifiziert, der von dem betreffenden Mitgliedstaat benannt wird. Die Bewertungsmethode kann vom Kompetenzzentrum überprüft werden, falls hinsichtlich der Zertifizierung Unklarheiten bestehen.

(10) Falls ein Mitgliedstaat seinen Verpflichtungen zur Leistung seiner Finanzbeiträge oder Beiträge in Form von Sachleistungen in Bezug auf gemeinsame Maßnahmen nicht nachgekommen ist, informiert der Exekutivdirektor den betreffenden Mitgliedstaat schriftlich über dessen Versäumnis und setzt ihm eine angemessene Frist für die Beseitigung dieses Versäumnisses. Wird das Versäumnis nicht innerhalb dieser Frist beseitigt, so beruft der Exekutivdirektor eine Sitzung des Verwaltungsrats ein, in der darüber entschieden wird, ob dem säumigen beteiligten Mitgliedstaat das Stimmrecht zu entziehen ist oder ob andere Maßnahmen zu treffen sind, bis dieser Mitgliedstaat seinen Verpflichtungen nachgekommen ist. Das Stimmrecht des säumigen Mitgliedstaats in Bezug auf gemeinsame Maßnahmen wird ausgesetzt, bis er seine Verpflichtungen erfüllt hat.

(11) Die Kommission kann den Finanzbeitrag der Union zu gemeinsamen Maßnahmen aufkündigen, anteilsmäßig kürzen oder aussetzen, wenn die beitragenden Mitgliedstaaten die in Absatz 3 Buchstabe b genannten Beiträge nicht, nur teilweise oder verspätet leisten. Die Kündigung, Kürzung oder Aussetzung des Finanzbeitrags der Union durch die Kommission richtet sich nach dem Betrag und dem Zeitraum, in dem der Mitgliedstaat seine Beiträge nicht, nur zum Teil oder verspätet geleistet hat.

(12) Die beitragenden Mitgliedstaaten melden jährlich bis zum 31. Januar dem Verwaltungsrat die Höhe der in Absatz 7 genannten Beiträge für gemeinsame Maßnahmen mit der Union, die im vorangegangenen Haushaltsjahr geleistet wurden.

Artikel 22

Kosten und Mittelausstattung des Kompetenzzentrums

(1) Die Verwaltungskosten des Kompetenzzentrums werden grundsätzlich durch Finanzbeiträge von der Union gedeckt, die jährlich geleistet werden. Zusätzliche Finanzbeiträge werden von den beitragenden Mitgliedstaaten im Verhältnis zu ihren freiwilligen Beiträgen zu gemeinsamen Maßnahmen geleistet. Wird ein Teil des Beitrags zu den Verwaltungskosten nicht in Anspruch genommen, so kann er zur Deckung von Betriebskosten des Kompetenzzentrums bereitgestellt werden.

(2) Die Betriebskosten des Kompetenzzentrums werden gedeckt durch

a) den Finanzbeitrag der Union,

b) freiwillige Finanzbeiträge oder Beiträge in Form von Sachleistungen der beitragenden Mitgliedstaaten bei gemeinsamen Maßnahmen.

(3) Die in den Haushalt des Kompetenzzentrums eingestellten Mittel setzen sich aus den folgenden Beiträgen zusammen:

a) den Finanzbeiträgen der Union zu Betriebs- und Verwaltungskosten;

b) den freiwilligen Finanzbeiträgen der beitragenden Mitgliedstaaten zu Verwaltungskosten bei gemeinsamen Maßnahmen;

c) den freiwilligen Finanzbeiträgen der beitragenden Mitgliedstaaten zu Betriebskosten bei gemeinsamen Maßnahmen;

d) etwaigen Einnahmen des Kompetenzzentrums;

e) sämtlichen sonstigen Finanzbeiträgen, Mitteln oder Einnahmen.

(4) Zinserträge aus den von den beitragenden Mitgliedstaaten an das Kompetenzzentrum gezahlten Beiträgen gelten als Einnahmen des Kompetenzzentrums.

(5) Alle Mittel des Kompetenzzentrums und seine Tätigkeiten dienen dazu, die festgelegten Ziele zu verwirklichen.

(6) Das Kompetenzzentrum ist Eigentümer aller Vermögenswerte, die es selbst erwirtschaftet hat oder die ihm zum Zweck der Verwirklichung seiner Ziele übertragen wurden. Unbeschadet der geltenden Vorschriften für das jeweilige Förderprogramm wird über das Eigentum an den im Rahmen gemeinsamer Maßnahmen erwirtschafteten oder erworbenen Vermögenswerten gemäß Artikel 15 Absatz 3 Buchstabe b entschieden.

(7) Sofern sich das Kompetenzzentrum nicht in Abwicklung befindet, bleiben etwaige Einnahmeüberschüsse im Eigentum des Kompetenzzentrums und werden nicht an die beitragenden Mitglieder des Kompetenzzentrums ausgezahlt.

(8) Das Kompetenzzentrum arbeitet eng mit anderen Organen, Einrichtungen und sonstigen Stellen der Union zusammen, wobei deren jeweilige Mandate gebührend zu berücksichtigen sind und es nicht zu Überschneidungen mit den bestehenden Kooperationsmechanismen kommen darf, damit Synergien mit diesen genutzt und, sofern möglich und angemessen, damit die Verwaltungskosten gesenkt werden können.

Artikel 23

Finanzielle Verpflichtungen

Die finanziellen Verpflichtungen des Kompetenzzentrums dürfen den Betrag der ihm zur Verfügung stehenden oder seinem Haushalt von seinen Mitgliedern zugewiesenen Finanzmittel nicht übersteigen.

Artikel 24

Haushaltsjahr

Das Haushaltsjahr beginnt am 1. Januar und endet am 31. Dezember.

Artikel 25

Aufstellung des Haushaltsplans

(1) Der Exekutivdirektor erstellt jedes Jahr den Entwurf des Voranschlags der Einnahmen und Ausgaben des Kompetenzzentrums für das folgende Haushaltsjahr und legt ihn dem Verwaltungsrat zusammen mit dem Entwurf des Stellenplans gemäß Artikel 13 Absatz 3 Buchstabe l vor. Einnahmen und Ausgaben müssen ausgeglichen sein. Die Ausgaben des Kompetenzzentrums umfassen die Personal-, Verwaltungs-, Infrastruktur- und Betriebsausgaben. Die Verwaltungsausgaben sind auf ein Mindestmaß zu beschränken, einschließlich durch Umschichtung von Personal oder Planstellen.

(2) Der Verwaltungsrat erstellt jedes Jahr auf der Grundlage des nach Absatz 1 erstellten Entwurfs des Voranschlags der Einnahmen und Ausgaben einen Voranschlag der Einnahmen und Ausgaben des Kompetenzzentrums für das folgende Haushaltsjahr.

(3) Der Verwaltungsrat übermittelt der Kommission jedes Jahr bis zum 31. Januar den in Absatz 2 des vorliegenden Artikels genannten Voranschlag, der Teil des Entwurfs des einheitlichen Programmplanungsdokuments gemäß Artikel 32 Absatz 1 der delegierten Verordnung (EU) 2019/715 ist.

(4) Die Kommission setzt auf der Grundlage des in Absatz 2 des vorliegenden Artikels genannten Voranschlags die von ihr für erforderlich erachteten Mittelansätze für den Stellenplan gemäß Artikel 13 Absatz 3 Buchstabe l der vorliegenden Verordnung und den Betrag des Zuschusses aus dem Gesamthaushaltsplan in den Haushaltsplanentwurf der Union ein, den sie nach den Artikeln 313 und 314 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) dem Europäischen Parlament und dem Rat vorlegt.

(5) Das Europäische Parlament und der Rat bewilligen die Mittel für den Beitrag für das Kompetenzzentrum.

(6) Der Stellenplan gemäß Artikel 13 Absatz 3 Buchstabe l wird vom Europäischen Parlament und vom Rat angenommen.

(7) Der Haushaltsplan des Kompetenzzentrums wird zusammen mit dem jährlichen Arbeitsprogramm und dem mehrjährigen Arbeitsprogramm vom Verwaltungsrat angenommen. Er wird endgültig, sobald der Gesamthaushaltsplan der Union endgültig festgestellt ist. Gegebenenfalls nimmt der Verwaltungsrat eine Anpassung des Haushaltsplans des Kompetenzzentrums und des jährlichen Arbeitsprogramms entsprechend dem Gesamthaushaltsplan der Union vor.

Artikel 26

Rechnungslegung des Kompetenzzentrums und Entlastung

Die vorläufige und endgültige Rechnungslegung des Kompetenzzentrums sowie die Entlastung entsprechen den Regeln und dem Zeitplan der Haushaltsordnung und der Finanzordnung des Kompetenzzentrums.

Artikel 27

Tätigkeitsberichte und Finanzberichterstattung

(1) Der Exekutivdirektor erstattet dem Verwaltungsrat jährlich Bericht über die Erfüllung seiner Pflichten gemäß der Finanzordnung des Kompetenzzentrums.

(2) Binnen zwei Monaten nach Ende jedes Haushaltsjahres legt der Exekutivdirektor dem Verwaltungsrat einen jährlichen Tätigkeitsbericht über die Fortschritte des Kompetenzzentrums im vorangegangenen Kalenderjahr zur Billigung vor; darin wird insbesondere auf das für jenes Jahr geltende jährliche Arbeitsprogramm und auf die Verwirklichung seiner strategischen Ziele und Prioritäten Bezug genommen. Dieser Bericht enthält Informationen über folgende Aspekte:

a) durchgeführte operative Maßnahmen mit den entsprechenden Ausgaben;

b) die eingereichten Maßnahmen mit einer Aufschlüsselung nach Art der Teilnehmer — einschließlich KMU — und nach Mitgliedstaat;

c) die für eine Finanzierung ausgewählten Maßnahmen mit einer Aufschlüsselung nach Art der Teilnehmer, einschließlich KMU, und nach Mitgliedstaat unter Angabe des vom Kompetenzzentrum für die einzelnen Teilnehmer und Maßnahmen zur Verfügung gestellten Beitrags;

d) die Erfüllung des Auftrags und der Ziele gemäß dieser Verordnung sowie Vorschläge für weitere Arbeiten, die zur Erfüllung dieses Auftrags und dieser Ziele erforderlich sind;

e) die Kohärenz der Umsetzungsaufgaben mit der Agenda und dem mehrjährigen Arbeitsprogramm.

(3) Der jährliche Tätigkeitsbericht wird nach seiner Genehmigung durch den Verwaltungsrat veröffentlicht.

Artikel 28

Finanzordnung

Das Kompetenzzentrum beschließt eine eigene Finanzordnung gemäß Artikel 70 der Haushaltsordnung.

Artikel 29

Schutz der finanziellen Interessen der Union

(1) Das Kompetenzzentrum gewährleistet bei der Durchführung der nach dieser Verordnung finanzierten Maßnahmen den Schutz der finanziellen Interessen der Union durch geeignete Präventivmaßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch regelmäßige und wirksame Kontrollen und — bei Feststellung von Unregelmäßigkeiten — durch Rückforderung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch wirksame, verhältnismäßige und abschreckende verwaltungsrechtliche Sanktionen.

(2) Das Kompetenzzentrum gewährt Bediensteten der Kommission und sonstigen von der Kommission ermächtigten Personen sowie dem Europäischen Rechnungshof Zugang zu den Standorten und Räumlichkeiten des Kompetenzzentrums sowie zu allen Informationen, einschließlich Informationen in elektronischer Form, die für die Durchführung der Rechnungsprüfungen erforderlich sind.

(3) Das OLAF kann gemäß den Bestimmungen und Verfahren der Verordnung (Euratom, EG) Nr. 2185/96 des Rates ([17]) und der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates ([18]) Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob es im Zusammenhang mit Finanzhilfevereinbarungen oder Verträgen, die gemäß dieser Verordnung direkt oder indirekt finanziert werden, zu Betrug, Korruption oder anderen rechtswidrigen Handlungen zum Nachteil der finanziellen Interessen der Union gekommen ist.

(4) Unbeschadet der Absätze 1, 2 und 3 ist in Verträgen und Finanzhilfevereinbarungen, die sich aus der Durchführung dieser Verordnung ergeben, der Kommission, dem Kompetenzzentrum, dem Rechnungshof und OLAF ausdrücklich die Befugnis zu erteilen, entsprechend ihren Zuständigkeiten derartige Rechnungsprüfungen und Untersuchungen durchzuführen. Wenn die Durchführung einer Maßnahme ganz oder teilweise weitervergeben oder weiterdelegiert wird oder wenn sie die Vergabe eines öffentlichen Auftrags oder finanzieller Unterstützung an einen Dritten erfordert, müssen der Vertrag bzw. die Finanzhilfevereinbarung die Pflicht des Auftragnehmers oder des Begünstigten einschließen, von beteiligten Dritten die ausdrückliche Anerkennung dieser Befugnisse der Kommission, des Kompetenzzentrums, des Rechnungshofs und des OLAF zu verlangen.

KAPITEL IV

Personal des Kompetenzzentrums

Artikel 30

Personal

(1) Für das Personal des Kompetenzzentrums gelten das Statut der Beamten und die Beschäftigungsbedingungen sowie die im gegenseitigen Einvernehmen der Organe der Union erlassenen Regelungen zur Durchführung des Statuts der Beamten und der Beschäftigungsbedingungen.

(2) Der Verwaltungsrat übt in Bezug auf das Personal des Kompetenzzentrums die Befugnisse aus, die der Anstellungsbehörde durch das Statut der Beamten und der zum Abschluss von Dienstverträgen befugten Behörde durch die Beschäftigungsbedingungen übertragen wurden (im Folgenden „Befugnisse der Anstellungsbehörde").

(3) Der Verwaltungsrat erlässt gemäß Artikel 110 des Statuts der Beamten einen Beschluss auf der Grundlage von Artikel 2 Absatz 1 des Statuts der Beamten und Artikel 6 der Beschäftigungsbedingungen, durch den dem Exekutivdirektor die entsprechenden Befugnisse der Anstellungsbehörde übertragen und die Bedingungen festgelegt werden, unter denen diese Befugnisübertragung ausgesetzt werden kann. Der Exekutivdirektor kann diese Befugnisse weiterübertragen.

(4) Ist dies in außergewöhnlichen Fällen erforderlich, so kann der Verwaltungsrat die Übertragung der Befugnisse der Anstellungsbehörde auf den Exekutivdirektor sowie jegliche weitere Übertragung durch Letzteren durch einen Beschluss vorübergehend aussetzen. In solchen Fällen übt der Verwaltungsrat die Befugnisse der Anstellungsbehörde selbst aus oder überträgt sie einem seiner Mitglieder oder einem anderen Bediensteten des Kompetenzzentrums als dem Exekutivdirektor.

(5) Der Verwaltungsrat erlässt im Einklang mit Artikel 110 des Statuts der Beamten Durchführungsbestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen.

(6) Die Personalstärke wird durch den in Artikel 13 Absatz 3 Buchstabe l genannten Stellenplan unter Angabe der Zahl der Planstellen auf Zeit nach Funktions- und Besoldungsgruppe und der Zahl der Vertragsbediensteten (in Vollzeitäquivalenten) in Übereinstimmung mit dem jährlichen Haushaltsplan des Kompetenzzentrums festgelegt.

(7) Der Personalbedarf des Kompetenzzentrums wird in erster Linie durch eine Umschichtung von Personal oder Planstellen von Organen, Einrichtungen und sonstigen Stellen der Union und durch die Einstellung von zusätzlichem Personal gedeckt. Das Personal des Kompetenzzentrums kann aus Bediensteten auf Zeit und Vertragsbediensteten bestehen.

([17]) Verordnung (Euratom, EG) Nr. 2185/96 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Europäischen Gemeinschaften vor Betrug und anderen Unregelmäßigkeiten (ABl. L 292 vom 15.11.1996, S. 2).

([18]) Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1).

(8) Sämtliche Personalausgaben trägt das Kompetenzzentrum.

Artikel 31

Abgeordnete nationale Sachverständige und sonstige Bedienstete

(1) Das Kompetenzzentrum kann auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht vom Kompetenzzentrum selbst beschäftigt wird.

(2) Der Verwaltungsrat beschließt im Einvernehmen mit der Kommission eine Regelung für die Abordnung nationaler Sachverständiger zum Kompetenzzentrum.

Artikel 32

Vorrechte und Befreiungen

Das dem EUV und dem AEUV beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union findet auf das Kompetenzzentrum und sein Personal Anwendung.

KAPITEL V

Gemeinsame Bestimmungen

Artikel 33

Sicherheitsvorschriften

(1) Artikel 12 der Verordnung (EU) 2021/694 gilt für die Teilnahme an allen vom Kompetenzzentrum finanzierten Maßnahmen.

(2) Für aus „Horizont Europa" finanzierte Maßnahmen gelten die folgenden besonderen Sicherheitsvorschriften:

a) für die Zwecke von Artikel 38 Absatz 1 der Verordnung (EU) 2021/695 kann die Gewährung nicht ausschließlicher Lizenzen, wenn dies im jährlichen Arbeitsprogramm vorgesehen ist, auf Dritte beschränkt werden, die in einem Mitgliedstaat niedergelassen sind oder als niedergelassen gelten und von diesem Mitgliedstaat oder von Staatsangehörigen dieses Mitgliedstaats geführt werden;

b) für die Zwecke von Artikel 40 Absatz 4 Unterabsatz 1 Buchstabe b der Verordnung (EU) 2021/695 kann gegen die Übertragung von Eigentumsrechten an den Ergebnissen oder gegen die Gewährung einer ausschließlichen Lizenz zur Nutzung der Ergebnisse Einspruch erhoben werden, wenn die Übertragung oder Lizenzierung an einen Rechtsträger erfolgen soll, der zwar seinen Sitz in einem assoziierten Land oder in der Union hat, aber aus Drittländern geführt wird;

c) für die Zwecke von Artikel 41 Absatz 7 Unterabsatz 1 Buchstabe a der Verordnung (EU) 2021/695 kann die Gewährung von Zugangsrechten im Sinne von Artikel 2 Nummer 9 der genannten Verordnung, wenn dies im jährlichen Arbeitsprogramm vorgesehen ist, auf Rechtsträger beschränkt werden, die in einem Mitgliedstaat niedergelassen sind oder als niedergelassen gelten und von diesem Mitgliedstaat oder von Staatsangehörigen dieses Mitgliedstaats geführt werden.

Artikel 34

Transparenz

(1) Das Kompetenzzentrum führt seine Tätigkeiten mit einem hohen Maß an Transparenz aus.

(2) Das Kompetenzzentrum stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise rechtzeitig angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere über die Ergebnisse seiner Arbeit, erhalten. Ferner veröffentlicht es die nach Artikel 43 abgegebenen Interessenerklärungen. Diese Anforderungen gelten auch für die nationalen Koordinierungszentren, die Gemeinschaft und die strategische Beratungsgruppe im Einklang mit einschlägigem Recht.

(3) Der Verwaltungsrat kann auf Vorschlag des Exekutivdirektors gestatten, dass interessierte Kreise als Beobachter an bestimmten Arbeiten des Kompetenzzentrums teilnehmen.

(4) Das Kompetenzzentrum legt in der Geschäftsordnung des Verwaltungsrats des Kompetenzzentrums und der strategischen Beratungsgruppe die praktischen Einzelheiten für die Anwendung der Transparenzvorschriften nach den Absätzen 1 und 2 des vorliegenden Artikels fest. Bei Maßnahmen, die aus „Horizont Europa" finanziert werden, tragen diese Vorschriften und Einzelheiten den Bestimmungen der Verordnung (EU) 2021/695 Rechnung.

Artikel 35

Ausgewogenes Geschlechterverhältnis

Bei der Durchführung dieser Verordnung wählen die Kommission, die Mitgliedstaaten und anderen institutionellen und privatwirtschaftlichen Interessensträger im Zusammenhang mit der Benennung von Kandidaten oder dem Vorschlag von Vertretern nach Möglichkeit aus mehreren Kandidaten Vertreter aus und strebt dabei die Sicherstellung eines ausgewogenen Geschlechterverhältnisses an.

Artikel 36

Sicherheitsvorschriften für den Schutz von Verschlusssachen und nicht als Verschlusssache eingestuften vertraulichen Informationen

(1) Nach Genehmigung durch die Kommission nimmt der Verwaltungsrat die Sicherheitsvorschriften des Kompetenzzentrums an. Diese Sicherheitsvorschriften wenden dabei die in den Beschlüssen (EU, Euratom) 2015/443 ([19]) und (EU, Euratom) 2015/444 ([20]) der Kommission enthaltenen Grundsätze und Regeln an.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal des Kompetenzzentrums unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 AEUV.

(3) Das Kompetenzzentrum kann die Maßnahmen treffen, die notwendig sind, um den Austausch von Informationen, die für seine Aufgaben von Belang sind, mit der Kommission und den Mitgliedstaaten sowie gegebenenfalls mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union zu erleichtern. Alle zu diesem Zweck getroffenen Verwaltungsvereinbarungen über den Austausch von EU-Verschlusssachen oder, falls keine solche Vereinbarungen vorliegen, jede Ad-hoc-Weitergabe von EU-Verschlusssachen in Ausnahmefällen bedarf der vorherigen Genehmigung durch die Kommission.

Artikel 37

Zugang zu Unterlagen

(1) Die Verordnung (EG) Nr. 1049/2001 findet auf die Dokumente des Kompetenzzentrums Anwendung.

(2) Der Verwaltungsrat legt bis zum 29. Dezember 2021 Maßnahmen zur Durchführung der Verordnung (EG) Nr. 1049/2001 fest.

(3) Gegen Entscheidungen des Kompetenzzentrums nach Artikel 8 der Verordnung (EG) Nr. 1049/2001 kann nach Maßgabe von Artikel 228 AEUV Beschwerde beim Bürgerbeauftragten eingelegt oder nach Artikel 263 AEUV Klage beim Gerichtshof der Europäischen Union erhoben werden.

Artikel 38

Überwachung, Bewertung und Überprüfung

(1) Das Kompetenzzentrum stellt sicher, dass seine Tätigkeiten, einschließlich der über die nationalen Koordinierungszentren und das Netzwerk verwalteten Tätigkeiten, einer kontinuierlichen und systematischen Überwachung und regelmäßigen Bewertung unterzogen werden. Das Kompetenzzentrum stellt sicher, dass die Daten für die Überwachung der Durchführung und der Ergebnisse der in Artikel 4 Absatz 3 Buchstabe b genannten Finanzierungsprogramme der Union effizient, wirksam und zeitnah erhoben werden und erlegt den Empfängern von Unionsmitteln und den Mitgliedstaaten verhältnismäßige Vorgaben für die Berichterstattung auf. Die Schlussfolgerungen dieser Bewertung werden veröffentlicht.

(2) Sobald ausreichende Informationen über die Durchführung dieser Verordnung vorliegen, spätestens jedoch 30 Monate nach dem in Artikel 46 Absatz 4 bestimmten Zeitpunkt, erstellt die Kommission einen Durchführungsbericht zu den Tätigkeiten des Kompetenzzentrums und berücksichtigt dabei die zuvor eingereichten Beiträge des Verwaltungsrats, der nationalen Koordinierungszentren und der Gemeinschaft. Die Kommission übermittelt diesen Durchführungsbericht bis zum 30. Juni 2024 an das Europäische Parlament und den Rat. Das Kompetenzzentrum und die Mitgliedstaaten stellen der Kommission die für die Erstellung des Berichts erforderlichen Informationen zur Verfügung.

(3) Der in Absatz 2 genannte Durchführungsbericht umfasst Bewertungen

a) der Arbeitskapazität des Kompetenzzentrums hinsichtlich seines Auftrags, seiner Ziele, seines Mandats und seiner Aufgaben sowie der Zusammenarbeit und Koordinierung mit anderen Interessenträgern, insbesondere den nationalen Koordinierungszentren, der Gemeinschaft und der ENISA;

([19]) Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 41).

([20]) Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 72 vom 17.3.2015, S. 53).

b) der vom Kompetenzzentrum erzielten Ergebnisse im Hinblick auf seinen Auftrag, seine Ziele, sein Mandat und seine Aufgaben, wobei insbesondere die Effizienz des Kompetenzzentrums bei der Koordinierung der Unionsmittel und bei der Bündelung von Fachwissen bewertet werden;

c) der Kohärenz der Umsetzungsaufgaben mit der Agenda und dem mehrjährigen Arbeitsprogramm;

d) der Abstimmung und der Zusammenarbeit des Kompetenzzentrums mit den Programmausschüssen von „Horizont Europa" und des Programms „Digitales Europa", insbesondere im Hinblick auf die Steigerung von Kohärenz und Synergien mit der Agenda, dem jährlichen Arbeitsprogramm, dem mehrjährigen Arbeitsprogramm, „Horizont Europa" und dem Programm „Digitales Europa";

e) der gemeinsamen Maßnahmen.

(4) Nach Übermittlung des in Absatz 2 des vorliegenden Artikels genannten Durchführungsberichts führt die Kommission eine Bewertung des Kompetenzzentrums durch und berücksichtigt dabei die zuvor eingereichten Beiträge des Verwaltungsrats, der nationalen Koordinierungszentren und der Gemeinschaft. Diese Bewertung nimmt Bezug auf oder aktualisiert gegebenenfalls die in Absatz 3 des vorliegenden Artikels genannten Bewertungen und wird vor Ablauf des in Artikel 47 Absatz 1 festgelegten Zeitraums durchgeführt, damit rechtzeitig festgestellt werden kann, ob es angemessen ist, das Mandat des Kompetenzzentrums über diesen Zeitraum hinaus zu verlängern. Bei dieser Bewertung werden rechtliche und administrative Aspekte des Mandats des Kompetenzzentrums sowie das Potenzial, im Hinblick auf andere Organe, Einrichtungen und sonstige Stellen der Union Synergien zu bewirken und Fragmentierung zu vermeiden, beurteilt.

Ist die Kommission der Ansicht, dass das Fortbestehen des Kompetenzzentrums vor dem Hintergrund seines Auftrags, seiner Ziele, seines Mandats und seiner Aufgaben gerechtfertigt ist, so kann sie einen Gesetzgebungsvorschlag zur Verlängerung der in Artikel 47 festgelegten Bestehensdauer des Kompetenzzentrums vorlegen.

(5) Auf der Grundlage der Schlussfolgerungen aus dem Durchführungsbericht nach Absatz 2 kann die Kommission geeignete Maßnahmen ergreifen.

(6) Die Überwachung, Bewertung, stufenweise Beendigung und Erneuerung des Beitrags aus „Horizont Europa" erfolgen nach Maßgabe der Artikel 10, 50 und 52 der Verordnung (EU) 2021/695 und der vereinbarten Durchführungsmodalitäten.

(7) Die Überwachung, Berichterstattung und Bewertung hinsichtlich des Beitrags aus dem Programm „Digitales Europa" erfolgen nach Maßgabe der Artikel 24 und 25 der Verordnung (EU) 2021/694.

(8) Im Falle einer Abwicklung des Kompetenzzentrums nimmt die Kommission innerhalb von sechs Monaten nach der Abwicklung, spätestens jedoch zwei Jahre nach Einleitung des Abwicklungsverfahrens gemäß Artikel 47 eine abschließende Bewertung des Kompetenzzentrums vor. Die Ergebnisse dieser abschließenden Bewertung werden dem Europäischen Parlament und dem Rat übermittelt.

Artikel 39

Rechtspersönlichkeit des Kompetenzzentrums

(1) Das Kompetenzzentrum besitzt Rechtspersönlichkeit.

(2) Das Kompetenzzentrum verfügt in jedem Mitgliedstaat über die weitestgehende Rechts- und Geschäftsfähigkeit, die Rechtspersonen nach dessen Recht zuerkannt wird. Es kann insbesondere bewegliches und unbewegliches Vermögen erwerben und veräußern und ist vor Gericht parteifähig.

Artikel 40

Haftung des Kompetenzzentrums

(1) Die vertragliche Haftung des Kompetenzzentrums bestimmt sich nach dem für die betreffende Vereinbarung bzw. den betreffenden Beschluss oder Vertrag geltenden Recht.

(2) Im Bereich der außervertraglichen Haftung leistet das Kompetenzzentrum für die von seinem Personal in Wahrnehmung seiner Aufgaben verursachten Schäden Schadenersatz nach den allgemeinen Rechtsgrundsätzen, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.

(3) Etwaige Schadenersatzzahlungen des Kompetenzzentrums aufgrund der Haftung gemäß den Absätzen 1 und 2 sowie die damit zusammenhängenden Kosten und Ausgaben gelten als Ausgaben des Kompetenzzentrums und werden aus seinen Mitteln geleistet.

(4) Für die Erfüllung seiner Verpflichtungen haftet ausschließlich das Kompetenzzentrum.

Artikel 41

Zuständigkeit des Gerichtshofs der Europäischen Union und anwendbares Recht

(1) Der Gerichtshof der Europäischen Union ist zuständig

a) für Entscheidungen aufgrund von Schiedsklauseln in vom Kompetenzzentrum gefassten Beschlüssen oder in vom Kompetenzzentrum geschlossenen Vereinbarungen oder Verträgen;

b) für Schadenersatzstreitigkeiten aufgrund eines durch das Personal des Kompetenzzentrums in Wahrnehmung seiner Aufgaben verursachten Schadens;

c) für alle Streitsachen zwischen dem Kompetenzzentrum und seinem Personal im Rahmen und unter den Bedingungen des Statuts der Beamten.

(2) In Angelegenheiten, die nicht durch diese Verordnung oder sonstige Rechtsakte der Union geregelt sind, gilt das Recht des Mitgliedstaats, in dem das Kompetenzzentrum seinen Sitz hat.

Artikel 42

Haftung der Union und der Mitgliedstaaten und Versicherung

(1) Die finanzielle Haftung der Union und der Mitgliedstaaten für die Schulden des Kompetenzzentrums ist auf deren bereits zu den Verwaltungsausgaben geleistete Finanzbeiträge beschränkt.

(2) Das Kompetenzzentrum schließt angemessene Versicherungsverträge und erhält diese aufrecht.

Artikel 43

Interessenkonflikt

Der Verwaltungsrat nimmt in Bezug auf seine Mitglieder, seine Gremien und sein Personal, einschließlich des Exekutivdirektors, Regeln zur Vermeidung, Ermittlung und Beseitigung von Interessenkonflikten an. In diesen Regeln sind Bestimmungen vorzusehen, durch die im Einklang mit der Haushaltsordnung Interessenkonflikte bei den Vertretern der Mitglieder, die einen Sitz im Verwaltungsrat sowie in der ständigen Beratungsgruppe haben, vermieden werden, einschließlich Bestimmungen über Interessenerklärungen. Die nationalen Koordinierungszentren unterliegen im Zusammenhang mit Interessenkonflikten dem nationalen Recht.

Artikel 44

Schutz personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch das Kompetenzzentrum unterliegt der Verordnung (EU) 2018/1725.

(2) Der Verwaltungsrat beschließt Durchführungsbestimmungen nach Artikel 45 Absatz 3 der Verordnung (EU) 2018/1725. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der genannten Verordnung durch das Kompetenzzentrum erforderlich sind, festlegen.

Artikel 45

Unterstützung seitens des Aufnahmemitgliedstaat

Zwischen dem Kompetenzzentrum und dem Aufnahmemitgliedstaat, in dem es seinen Sitz hat, kann eine Verwaltungsvereinbarung über die Vorrechte und Befreiungen und die sonstige Unterstützung des Kompetenzzentrums seitens dieses Mitgliedstaats geschlossen werden.

KAPITEL VI

Schlussbestimmungen

Artikel 46

Erste Maßnahmen

(1) Die Kommission ist für die Einrichtung und die Aufnahme der Tätigkeit des Kompetenzzentrums verantwortlich, bis dieses über die operativen Kapazitäten zur Ausführung seines eigenen Haushaltsplans verfügt. Die Kommission führt im Einklang mit dem Unionsrecht alle notwendigen Maßnahmen unter Einbeziehung der zuständigen Gremien des Kompetenzzentrums durch.

(2) Für die Zwecke von Absatz 1 des vorliegenden Artikels kann die Kommission einen Interims-Exekutivdirektor benennen, bis der Exekutivdirektor nach seiner Ernennung durch den Verwaltungsrat gemäß Artikel 16 die Amtsgeschäfte aufnimmt. Der Interims-Exekutivdirektor nimmt die Aufgaben des Exekutivdirektors wahr und kann von einer begrenzten Zahl von Bediensteten der Kommission unterstützt werden. Die Kommission kann hierzu eine begrenzte Zahl ihrer Bediensteten übergangsweise an das Kompetenzzentrum abordnen.

(3) Der Interims-Exekutivdirektor kann alle Zahlungen genehmigen, für die im Jahreshaushaltsplan des Kompetenzzentrums Mittel zur Verfügung stehen, nachdem Verwaltungsrats ihn beschlossen hat, und Vereinbarungen und Verträge, einschließlich Arbeitsverträge, schließen und Beschlüsse fassen, nachdem der Stellenplan gemäß Artikel 13 Absatz 3 Buchstabe l angenommen wurde.

(4) Der Interims-Exekutivdirektor bestimmt im Einvernehmen mit dem Exekutivdirektor und vorbehaltlich der Genehmigung des Verwaltungsrats den Tag, ab dem das Kompetenzzentrum über die Kapazität zur Ausführung seines eigenen Haushaltsplans verfügen muss. Ab diesem Tag nimmt die Kommission für die Tätigkeiten des Kompetenzzentrums keine Mittelbindungen mehr vor und führt keine Zahlungen mehr aus.

Artikel 47

Bestehensdauer

(1) Das Kompetenzzentrum wird für den Zeitraum vom 28. Juni 2021 bis zum 31. Dezember 2029 eingerichtet.

(2) Wird das Mandat des Kompetenzzentrums nicht gemäß Artikel 38 Absatz 4 verlängert, wird nach Ende des in Absatz 1 des vorliegenden Artikels genannten Zeitraums automatisch das Abwicklungsverfahren eingeleitet.

(3) Zur Abwicklung des Kompetenzzentrums ernennt der Verwaltungsrat einen oder mehrere Abwicklungsbeauftragte, die seinen Beschlüssen nachkommen.

(4) Bei der Abwicklung des Kompetenzzentrums werden seine Vermögenswerte zur Deckung seiner Verbindlichkeiten und der Kosten seiner Abwicklung verwendet. Etwaige Überschüsse werden proportional zu ihren Finanzbeiträgen auf die Union und die beitragenden Mitgliedstaaten umgelegt, die zum Zeitpunkt der Abwicklung am Kompetenzzentrum beteiligt sind. Etwaige auf die Union umgelegte Überschüsse fließen in den Unionshaushalt zurück.

Artikel 48

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 20. Mai 2021.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Die Präsidentin*
D.M. SASSOLI	A.P. ZACARIAS