EUROPÄISCHE
KOMMISSION

Brüssel, den 22.2.2018
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“)

(Text von Bedeutung für den EWR)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Die Europäische Union hat bereits eine Reihe von Maßnahmen zur Erhöhung der Abwehrfähigkeit und zur Verbesserung ihrer Abwehrbereitschaft im Bereich der Cybersicherheit getroffen. In der ersten EU-Cybersicherheitsstrategie[1] aus dem Jahr 2013 wurden strategische Ziele und konkrete Maßnahmen festgelegt, um die Abwehrfähigkeit zu verbessern, die Cyberkriminalität zu verringern, ein politisches Konzept und Fähigkeiten für die Cyberabwehr auszuarbeiten, industrielle und technische Ressourcen zu entwickeln und eine kohärente internationale Cyberraumpolitik für die EU auszuarbeiten. Seither gab es in diesem Bereich wichtige Entwicklungen, insbesondere das zweite Mandat für die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)[2] und die Verabschiedung der **Richtlinie über die Sicherheit von Netz- und Informationssystemen**[3] (im Folgenden die „NIS-Richtlinie"), die die Grundlage für den vorliegenden Vorschlag bilden.

Außerdem hat die Europäische Kommission im **Jahr 2016 eine Mitteilung „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche"**[4] **verabschiedet**, in der weitere Maßnahmen angekündigt wurden, um die Zusammenarbeit und die Weitergabe von Wissen und Informationen zu intensivieren und um die Abwehrfähigkeit und die Abwehrbereitschaft der EU zu stärken, wobei auch die Möglichkeit massiver Sicherheitsvorfälle und einer gesamteuropäischen Cybersicherheitskrise berücksichtigt wurde. In diesem Zusammenhang kündigte die Kommission an, dass sie die **Bewertung** und **Überprüfung** der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates über die ENISA und zur Aufhebung der Verordnung (EG) Nr. 460/2004 (im Folgenden die „ENISA-Verordnung") vorziehen würde. Das Bewertungsverfahren könne zu einer Reform der Agentur und zu einer Stärkung ihrer Fähigkeiten und Kapazitäten, die Mitgliedstaaten auf nachhaltige Weise zu unterstützen, führen. Die Agentur würde daher eine stärkere operative und zentrale Funktion bei der Verwirklichung der Abwehrfähigkeit gegenüber Cyberangriffen erhalten, und in ihrem neuen Mandat würden die in der NIS-Richtlinie begründeten neuen Zuständigkeiten der Agentur anerkannt werden.

Die NIS-Richtlinie ist ein erster wesentlicher Schritt zur Förderung einer Kultur des Risikomanagements, da durch sie Sicherheitsanforderungen eingeführt wurden, zu deren Einhaltung die zentralen Wirtschaftsakteure, insbesondere Betreiber wesentlicher Dienste (Betreiber wesentlicher Dienste - BWD) und Anbieter bestimmter wichtiger digitaler Dienste (Anbieter digitaler Dienste - ADD) rechtlich verpflichtet sind. Da Sicherheitsanforderungen für die Wahrung der Vorteile der fortschreitenden Digitalisierung der Gesellschaft als

---

1 Gemeinsame Mitteilung der Europäischen Kommission und des Europäischen Auswärtigen Dienstes: Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum - JOIN(2013).

2 Verordnung (EU) Nr. 526/3013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004.

3 Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

4 Mitteilung der Kommission – Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche, COM(2016) 410 final.

wesentlich angesehen werden und die Verbreitung von vernetzten Geräten (Internet der Dinge (IoT) rasch fortschreitet, wurde in der Mitteilung von 2016 auch die Idee vorgebracht, einen Rahmen für die Zertifizierung der Sicherheit von IKT-Produkten und -Diensten festzulegen, um das Vertrauen in den digitalen Binnenmarkt und seine Sicherheit zu stärken. Mit Blick auf die vermehrte Nutzung von Technologien, die ein hohes Maß an Cybersicherheit erfordern, z. B. vernetzte und selbstfahrende Autos, elektronische Gesundheitssysteme oder industrielle Automatisierungssteuerungssysteme (Industrial Automation Control Systems – IACS), erhält die IKT-Cybersicherheitszertifizierung eine besondere Relevanz.

Die genannten politischen Maßnahmen und Ankündigungen wurden in den **Schlussfolgerungen des Rates** von 2016 erneut bekräftigt, in denen festgestellt wurde, dass „Cyberbedrohungen und Angriffsflächen für Cyberattacken sich weiterentwickeln und zunehmen, weshalb insbesondere zur Bewältigung schwerwiegender grenzüberschreitender Cybervorfälle eine ständige und noch engere Zusammenarbeit erforderlich ist". In den Schlussfolgerungen wurde erneut bekräftigt, dass „die ENISA-Verordnung eines der Kernelemente der Widerstandsfähigkeit gegenüber Cyberangriffen in der EU"[5] ist, und die Kommission wurde aufgefordert, weitere Schritte zu unternehmen, um die Frage der Zertifizierung auf europäischer Ebene anzugehen.

Die Einführung eines Zertifizierungssystems würde die Schaffung eines geeigneten Governance-Systems auf EU-Ebene voraussetzen, zu dem auch die Fachkompetenz einer unabhängigen EU-Agentur beitragen könnte. Diesbezüglich wird die ENISA im vorliegenden Vorschlag als die sich dafür anbietende EU-Einrichtung mit Kompetenz in Cybersicherheitsfragen genannt, die eine solche Rolle übernehmen sollte, um die zuständigen nationalen Stellen im Bereich der Zertifizierung zusammenzuführen und ihre Arbeit zu koordinieren.

In ihrer **Mitteilung zur Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt vom Mai 2017** hat die Kommission weiter ausgeführt, dass sie bis September 2017 das ENISA-Mandat überprüfen würde. Im Rahmen der Überprüfung sollte ihre Rolle im veränderten Cybersicherheitsökosystem festgelegt und sollten Maßnahmen für die Normierung, Zertifizierung und Kennzeichnung der Cybersicherheit entwickelt werden, um die Cybersicherheit von IKT-basierten Systemen, einschließlich vernetzter Objekte, zu verbessern[6]. In den **Schlussfolgerungen des Europäischen Rates** vom Juni 2017[7] wurde die Absicht der Kommission begrüßt, die Cybersicherheitsstrategie im September zu überprüfen und vor Jahresende weitere gezielte Maßnahmen vorzuschlagen.

Der Verordnungsvorschlag sieht ein umfassendes Bündel von Maßnahmen vor, die auf früheren Maßnahmen aufbauen und sich gegenseitig verstärkende Ziele fördern:

- Ausbau der **Kapazitäten und der Abwehrbereitschaft** der Mitgliedstaaten und Unternehmen
- Verbesserung der **Zusammenarbeit und der Koordinierung** zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU

---

5 Schlussfolgerungen des Rates zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche vom 15. November 2016.

6 Mitteilung der Kommission über die Halbzeitbewertung der Umsetzung der Strategie für einen digitalen Binnenmarkt, COM(2017) 228.

7 Tagung des Europäischen Rates (22. und 23. Juni 2017) – Schlussfolgerungen, EUCO 8/17.

- Ausbau der **Kapazitäten auf EU-Ebene, um die Maßnahmen der Mitgliedstaaten zu ergänzen**, insbesondere im Fall von grenzüberschreitenden Cyberkrisen
- Stärkere **Sensibilisierung** der Bürger und Unternehmen für Fragen der Cybersicherheit
- Verbesserung der allgemeinen **Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit**[8] von IKT-Produkten und -Diensten, um das Vertrauen in den digitalen Binnenmarkt und in digitale Innovationen zu stärken, und
- Vermeidung eines **Nebeneinanders unterschiedlicher Zertifizierungssysteme** in der EU sowie der damit verbundene Anforderungen und Bewertungskriterien in den einzelnen Mitgliedstaaten und Sektoren.

Im folgenden Teil der Begründung werden die Gründe für die Initiative im Hinblick auf die für die ENISA vorgeschlagenen Maßnahmen und die Zertifizierung der Cybersicherheit ausführlicher erläutert.

[8] Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit bedeutet, dass den Nutzern ausreichende Informationen über die Cybersicherheitseigenschaften bereitgestellt werden, um das Sicherheitsniveau eines bestimmten IKT-Produkts, eines bestimmten IKT-Dienstes oder eines bestimmten IKT-Verfahrens objektiv feststellen zu können.

ENISA

Die ENISA fungiert als ein Kompetenzzentrum für die Verbesserung der Netz- und Informationssicherheit in der Union und zur Unterstützung des Kapazitätsaufbaus der Mitgliedstaaten.

Die ENISA wurde 2004[9] gegründet, um einen Beitrag zum übergeordneten Ziel der Gewährleistung einer hohen und effektiven Netz- und Informationssicherheit innerhalb der EU zu leisten. Im Jahr 2013 wurde mit der Verordnung (EU) Nr. 526/2013 das neue Mandat der Agentur für einen Zeitraum von sieben Jahren bis 2020 festgelegt. Die Agentur ist in Griechenland angesiedelt, wobei sich ihr Verwaltungssitz in Heraklion (Kreta) befindet und das Kerngeschäft von Athen aus betrieben wird.

Bei der ENISA handelt es sich um eine kleine Agentur, die im Vergleich zu allen anderen Agenturen der EU über geringe Haushaltsmittel und wenig Mitarbeiter verfügt. Ihr Mandat ist befristet.

Die ENISA unterstützt die europäischen Organe, die Mitgliedstaaten und die Wirtschaft dabei, **Netz- und Informationssicherheitsprobleme anzugehen, zu bewältigen und insbesondere zu verhindern**. Dies geschieht durch eine Reihe von Aktivitäten in fünf Bereichen, die in ihrer Strategie[10] benannt wurden:

- Fachkompetenz: Bereitstellung von Informationen und Fachwissen zu zentralen Fragen der Netz- und Informationssicherheit
- Politik: Unterstützung der Politikgestaltung und -umsetzung in der Union
- Kapazitäten: Unterstützung des Aufbaus von Kapazitäten in der Union (z. B. durch Fortbildungen, Empfehlungen, Sensibilisierungsmaßnahmen)
- Fachkreise: Förderung der Fachkreise im Bereich der Netz- und Informationssicherheit (z. B. Unterstützung der Computer-Notfallteams (Computer Emergency Response Teams, CERTs), Koordinierung europaweiter Cyberübungen)
- Schaffung von Möglichkeiten (z. B. Zusammenarbeit mit den Interessenträgern, internationale Beziehungen).

Bei den Verhandlungen über die NIS-Richtlinie beschlossen die gesetzgebenden EU-Organe, der ENISA wichtige Aufgaben bei der Durchführung dieser Richtlinie zuzuweisen. Insbesondere stellt die Agentur das Sekretariat des CSIRTs-Netzes (das eingerichtet wurde, um eine schnelle und wirksame operative Zusammenarbeit zwischen den Mitgliedstaaten bei bestimmten Cybersicherheitsvorfällen sowie den Austausch von Informationen über Risiken zu fördern), und sie wird auch herangezogen, um die Kooperationsgruppe für die strategische Zusammenarbeit bei der Wahrnehmung ihrer Aufgaben zu unterstützen. In der NIS-Richtlinie ist ferner geregelt, dass die ENISA die Mitgliedstaaten und die Kommission mit Fachkompetenz, als Berater und als Mittler für den Austausch bewährter Verfahren unterstützen muss.

---

9 Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit,, ABl. L 77 vom 13.3.2004, S. 1.

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

Im Einklang mit der ENISA-Verordnung hat die Kommission eine Bewertung der Agentur vorgenommen, zu der eine unabhängige Studie sowie eine öffentliche Konsultation gehören. Im Rahmen der Bewertung wurden die Relevanz, Wirkung, Wirksamkeit, Effizienz und Kohärenz sowie der EU-Mehrwert der Agentur im Hinblick auf ihre Leistungen, Führung, interne Organisationsstruktur und Arbeitsmethoden im Zeitraum 2013-2016 beurteilt.

Die Gesamtleistung der ENISA wurde von der Mehrheit der Teilnehmer[11] an der öffentlichen Konsultation (74 %) positiv bewertet. Darüber hinaus vertrat die Mehrheit der Befragten die Auffassung, dass die ENISA ihre einzelnen Ziele erreicht (für jedes der Ziele waren mindestens 63 % dieser Meinung). Die Dienste und Produkte der ENISA werden von fast der Hälfte der Befragten (46 %) regelmäßig (monatlich oder häufiger) genutzt und wegen ihrer Qualität (62 %) geschätzt ebenso wie deshalb, weil sie von einer Einrichtung auf EU-Ebene (83 %) stammen.

Allerdings ist die große Mehrheit (88 %) der Teilnehmer der Auffassung, dass die derzeit auf EU-Ebene verfügbaren Instrumente und Mechanismen für die Bewältigung der gegenwärtigen Herausforderungen im Bereich der Cybersicherheit nicht ausreichen oder nur zum Teil geeignet sind. Die Befragten gaben mit großer Mehrheit (98 %) an, dass eine EU-Einrichtung diesen Bedarf decken sollte, und 99 % der Teilnehmer meinten, die ENISA sei die dafür richtige Organisation. Darüber hinaus äußerten 67,5 % der Konsultationsteilnehmer die Ansicht, dass die ENISA eine Rolle bei der Festlegung eines harmonisierten Rahmens für die Sicherheitszertifizierung von IT-Produkten und -Diensten spielen könnte.

Die Gesamtbewertung (der nicht nur die öffentliche Konsultation, sondern auch eine Reihe von Einzelbefragungen, zusätzliche gezielte Umfragen und Workshops zugrunde lagen) kam zu folgenden Schlussfolgerungen:

- Die Ziele der ENISA sind nach wie vor relevant. Vor dem Hintergrund schneller technologischer Entwicklungen und der sich ändernden Bedrohungen und angesichts der zunehmenden weltweiten Cybersicherheitsrisiken besteht in der EU eindeutig der Bedarf, hochrangiges Fachwissen über Fragen der Cybersicherheit zu fördern und weiter zu stärken. In den Mitgliedstaaten müssen Kapazitäten aufgebaut werden, um Bedrohungen verstehen und abwehren zu können, und die Interessenträger müssen über alle Themenbereiche und Einrichtungen hinweg zusammenarbeiten.
- Trotz ihrer geringen Haushaltsmittelausstattung war die Agentur bei der Nutzung ihrer Ressourcen und bei der Wahrnehmung ihrer Aufgaben operativ effizient. Die Aufteilung zwischen Athen und Heraklion hat jedoch auch zusätzliche Verwaltungskosten entstehen lassen.
- Was die Wirksamkeit betrifft, hat die ENISA ihre Ziele teilweise erreicht. Indem sie den Aufbau von Kapazitäten in den 28 Mitgliedstaaten[12] angeboten, die

[11] 90 Teilnehmer aus 19 Mitgliedstaaten antworteten auf die Konsultation (88 Antworten und zwei Positionspapiere), darunter waren auch nationale Behörden aus 15 Mitgliedstaaten und acht Dachverbände, die eine beträchtliche Anzahl von europäischen Unternehmen vertraten.

[12] Die Teilnehmer an der öffentlichen Konsultation wurden gebeten, sich dazu zu äußern, welches ihrer Ansicht nach die wesentlichen Leistungen der ENISA im Zeitraum 2013-2016 waren. Befragte aus allen Gruppen (insgesamt 55 Befragte, einschließlich 13 von nationalen Behörden, 20 aus der Privatwirtschaft und 22 unter der Rubrik „sonstige“) nannten als wichtigste Leistungen der ENISA die folgenden: 1) Die Koordinierung der CyberEurope-Übungen; 2) die Unterstützung der CERTs/CSIRTs durch Fortbildungen und Workshops zur Förderung der Koordinierung und des Austausches; 3) ENISA-Veröffentlichungen (Leitlinien und Empfehlungen, Berichte zur Bedrohungslage, Strategien für die Berichterstattung über Sicherheitsvorfälle und für das Krisenmanagement usw.), die als nützlich

Zusammenarbeit zwischen den Mitgliedstaaten und den Interessenträgern im Bereich der Netz- und Informationssicherheit verbessert, Fachwissen bereitgestellt, Fachkreise aufgebaut und die Entwicklung von politischen Strategien unterstützt hat, hat die Agentur erfolgreich zur Verbesserung der Netz- und Informationssicherheit in Europa beigetragen. Insgesamt hat sich die ENISA mit Sorgfalt auf die Umsetzung ihres Arbeitsprogramms konzentriert und als vertrauenswürdiger Partner ihrer Interessenträger in einem Bereich gehandelt, dessen große grenzüberschreitende Relevanz erst vor Kurzem anerkannt wurde.

- Der ENISA ist es auf dem weiten Feld der Netz- und Informationssicherheit zumindest bis zu einem gewissen Grad gelungen, Wirkung zu erzielen, doch sie hat es nicht vermocht, einen starken Markennamen zu entwickeln und als *das* Kompetenzzentrum in Europa anerkannt zu werden. Erklären lässt sich dies durch das weit gefasste Mandat der ENISA, die nicht mit entsprechend ausreichenden Ressourcen ausgestattet war. Zudem ist die ENISA die einzige EU-Agentur mit einem befristeten Mandat, wodurch sie in der Entwicklung langfristiger Zielvorstellungen und in der nachhaltigen Unterstützung ihrer Interessenträger eingeschränkt wird. Dies steht auch im Widerspruch zu den Bestimmungen der NIS-Richtlinie, durch die die ENISA mit unbefristeten Aufgaben betraut wird. Schließlich wurde in der Bewertung festgestellt, dass sich diese begrenzte Wirksamkeit zum Teil mit der stärkeren Inanspruchnahme von externem Fachwissen als von internem Fachwissen und mit den Schwierigkeiten bei der Einstellung und Bindung von Fachkräften erklären lässt.
- Nicht zuletzt wurde in der Bewertung festgestellt, dass der Mehrwert der Agentur in erster Linie in ihrer Fähigkeit liegt, die Zusammenarbeit vor allem zwischen den Mitgliedstaaten und insbesondere mit einschlägigen Fachkreisen der Netz- und Informationssicherheit (insbesondere zwischen den CSIRTs), zu stärken. Auf EU-Ebene gibt es keinen anderen Akteur, der die Zusammenarbeit eines solchen breiten Spektrums an Interessenträgern im Bereich der Netz- und Informationssicherheit unterstützt. Da die ENISA jedoch für ihre Aktivitäten strikte Prioritäten festsetzen muss, ist ihr Arbeitsprogramm vor allem auf die Bedürfnisse der Mitgliedstaaten ausgerichtet. Die Folge davon ist, dass sie den Bedürfnissen der übrigen Interessenträger, insbesondere der Industrie, nicht ausreichend Rechnung trägt. Außerdem führte dies dazu, dass die Agentur darum bemüht war, den Bedürfnissen ihrer zentralen Interessenträger gerecht zu werden, wodurch sie daran gehindert wurde, eine größere Wirkung zu erzielen. Der Mehrwert der Agentur war daher je nach den verschiedenen Bedürfnissen ihrer Interessenträger und je nachdem, inwieweit die Agentur in der Lage war, darauf zu reagieren, unterschiedlich (z. B. große/kleine Mitgliedstaaten, Mitgliedstaaten/Industrie).

Zusammenfassend ließen die Ergebnisse der Konsultationen der Interessenträger und der Bewertung den Schluss zu, dass die Ressourcen und das Mandat der ENISA angepasst werden müssen, damit sie eine angemessene Rolle bei der Bewältigung der derzeitigen und künftigen Herausforderungen spielen kann.

---

erachtet wurden, um die nationalen Sicherheitsrahmen auszuarbeiten und zu aktualisieren, und weil sie politischen Entscheidungsträgern und Cyberpraktikern als Referenz dienen; 4) die Unterstützung bei der Bekanntmachung der NIS-Richtlinie; 5) die Bemühungen zur Sensibilisierung für die Cybersicherheit durch den „Monat der Cybersicherheit“.

Angesichts dieser Ergebnisse sieht der vorliegende Vorschlag eine Überarbeitung des aktuellen Mandats der ENISA sowie neue Aufgaben und Funktionen für die Agentur vor, um die Mitgliedstaaten, die EU-Organe und die Bemühungen anderer Interessenträger wirksam und effizient zu unterstützen, damit ein sicherer Cyberraum in der Europäischen Union gewährleistet wird. Durch das vorgeschlagene neue Mandat soll die Agentur eine stärkere Rolle spielen und stärker im Mittelpunkt stehen, insbesondere indem sie auch den Mitgliedstaaten bei der Umsetzung der NIS-Richtlinie und bei der Bekämpfung besonderer Gefahren (operative Kapazität) aktiver hilft und indem sie zu einem Kompetenzzentrum wird, das die Mitgliedstaaten und die Kommission bei der Cybersicherheitszertifizierung unterstützt. Im vorliegenden Vorschlag ist Folgendes vorgesehen:

- Die ENISA würde ein ständiges Mandat und damit eine stabile Grundlage für die Zukunft erhalten. Das neue Mandat, die Ziele und Aufgaben sollen dennoch regelmäßig überprüft werden.
- Das vorgeschlagene Mandat präzisiert die Rolle der ENISA als EU-Cybersicherheitsagentur und als Referenz im EU Cybersicherheitsökosystem und sieht vor, dass die Agentur in enger Zusammenarbeit mit allen anderen einschlägigen Stellen eines solchen Ökosystems handelt.
- Die Organisation und die Führung der Agentur, die im Rahmen der Bewertung positiv beurteilt wurden, würden moderat geändert werden, insbesondere um sicherzustellen, dass sich die Bedürfnisse der breiteren Kreise der Interessenträger besser in der Arbeit der Agentur widerspiegeln.
- Der vorgeschlagene Zuständigkeitsbereich des Mandats ist genau abgegrenzt, wobei die Bereiche gestärkt werden, in denen die Agentur einen eindeutigen Mehrwert unter Beweis gestellt hat, und neue Bereiche hinzugefügt werden, in denen Unterstützung im Hinblick auf die neuen politischen Prioritäten und Instrumente benötigt wird, insbesondere im Hinblick auf die NIS-Richtlinie, die Überprüfung der EU-Cybersicherheitsstrategie, den angekündigten EU-Konzeptentwurf für Cybersicherheit für die Zusammenarbeit bei Cyberkrisen und die IKT-Sicherheitszertifizierung.
    - **Entwicklung und Umsetzung der EU-Politik:** Die ENISA würde damit beauftragt werden, proaktiv zur Entwicklung der Politik im Bereich der Netz- und Informationssicherheit und zu anderen politischen Initiativen mit Cybersicherheitselementen in verschiedenen Sektoren (z. B. Energie, Verkehr, Finanzen) beizutragen. Zu diesem Zweck würde sie eine ausgeprägte Beratungsfunktion haben, die sie durch unabhängige Stellungnahmen sowie Vorarbeiten für die Entwicklung und Aktualisierung der Politik und des Rechts wahrnehmen könnte. Die ENISA würde auch die EU-Politik und das EU-Recht in den Bereichen elektronische Kommunikation, elektronische Identität und Vertrauensdienste unterstützen, um ein höheres Cybersicherheitsniveau zu fördern. In der Umsetzungsphase, vor allem im Zusammenhang mit der NIS-Kooperationsgruppe, würde die ENISA die Mitgliedstaaten dabei unterstützen, für die Umsetzung der NIS-Richtlinie einen Ansatz zu finden, der grenz- und sektorenübergreifend sowie mit anderen einschlägigen Strategien und Rechtsvorschriften kohärent ist. Im Interesse einer regelmäßigen Überprüfung der Strategien und Rechtsvorschriften im Bereich der Cybersicherheit würde die ENISA auch regelmäßig über den Stand der Umsetzung des EU-Rechtsrahmens Bericht erstatten.

- **Aufbau von Kapazitäten:** Die ENISA würde einen Beitrag zur Verbesserung der Fähigkeiten und Fachkompetenzen der EU-Behörden sowie der nationalen Behörden leisten, was auch die Reaktion auf Sicherheitsvorfälle und die Überwachung der cybersicherheitsbezogenen Regulierungsmaßnahmen einschließt. Außerdem müsste die Agentur zum Aufbau von Informationsaustausch- und -analysezentren (ISAC) in verschiedenen Sektoren beitragen, indem sie bewährte Verfahren bereitstellt, die verfügbaren Instrumente und Verfahren erläutert und sich in geeigneter Weise mit Regulierungsfragen im Zusammenhang mit dem Informationsaustausch befasst.

- **Wissen und Information, Sensibilisierung:** Die ENISA würde zum „Informationsdrehkreuz" der EU werden. Dies würde die Förderung und den Austausch bewährter Verfahren und Initiativen in der gesamten EU durch die Zusammenführung von Informationen zur Cybersicherheit umfassen, die von den Organen, Einrichtungen und sonstigen Stellen der EU und der Einzelstaaten stammen. Die Agentur würde auch zum Thema „Sicherheit kritischer Infrastrukturen" Beratungsleistungen, Orientierungshilfen und bewährte Verfahren zur Verfügung stellen. Ferner würde die ENISA nach signifikanten grenzüberschreitenden Cybersicherheitsvorfällen Berichte erstellen, um Unternehmen und Bürgern in der EU Orientierungshilfen zu geben. Zu diesem Arbeitsschwerpunkt würde auch die regelmäßige Durchführung von Sensibilisierungsmaßnahmen in Abstimmung mit den Behörden der Mitgliedstaaten gehören.

- **Marktbezogene Aufgaben (Normung, Cybersicherheitszertifizierung):** Die ENISA würde eine Reihe von Aufgaben wahrnehmen, die speziell den Binnenmarkt unterstützen und eine Cybersicherheits-„Marktbeobachtungsstelle" umfassen; dazu würde sie einschlägige Trends auf dem Cybersicherheitsmarkt analysieren, um Angebot und Nachfrage besser aufeinander abzustimmen, und die Entwicklung der EU-Politik in den Bereichen IKT-Normung und IKT-Cybersicherheitszertifizierung unterstützen. Speziell im Bereich der Normung würde sie die Ausarbeitung und Einführung von Cybersicherheitsnormen fördern. Zudem würde die ENISA Aufgaben wahrnehmen, die im Zusammenhang mit dem künftigen Zertifizierungsrahmen geplant sind (siehe folgenden Abschnitt).

- **Forschung und Innovation:** Die ENISA würde ihre Fachkompetenz durch die Beratung der EU und der nationalen Behörden bei der Festsetzung von Prioritäten in der Forschung und Entwicklung einbringen, auch im Rahmen der vertraglichen öffentlich-privaten Partnerschaft zur Cybersicherheit. Die Beratungsleistung der ENISA würde in das neue Europäische Forschungs- und Kompetenzzentrum für Cybersicherheit im Rahmen des nächsten mehrjährigen Finanzrahmens einfließen. Auf Anfrage der Kommission wäre die ENISA ebenfalls an der Umsetzung von EU-Förderprogrammen für Forschung und Innovation beteiligt.

- **Operative Zusammenarbeit und Krisenmanagement:** Diesem Arbeitsschwerpunkt sollte Folgendes zugrunde liegen: die Stärkung der bestehenden präventiven operativen Fähigkeiten, insbesondere der Ausbau der europaweiten Übungen zur Cybersicherheit (CyberEurope) dadurch, dass sie jährlich abgehalten werden, und eine unterstützende Rolle bei der operativen

Zusammenarbeit durch die Wahrnehmung der Sekretariatsgeschäfte des CSIRTs-Netzes (gemäß der NIS-Richtlinie), indem u. a. sichergestellt wird, dass die IT-Infrastruktur und die Kommunikationskanäle des CSIRTs-Netzes gut funktionieren. In diesem Zusammenhang wäre eine strukturierte Zusammenarbeit mit dem CERT-EU, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und anderen maßgeblichen EU-Einrichtungen erforderlich. Zudem sollte eine strukturierte Zusammenarbeit mit dem CERT-EU in enger räumlicher Nähe die Erbringung technischer Hilfe im Falle signifikanter Sicherheitsvorfälle und die Unterstützung der Analyse von Sicherheitsvorfällen ermöglichen. Anfragende Mitgliedstaaten würden bei der Bewältigung von Sicherheitsvorfällen sowie bei der Analyse von Anfälligkeiten, Artefakten und Sicherheitsvorfällen unterstützt werden, damit sie ihre eigenen Präventions- und Reaktionsfähigkeiten stärken können.

- Die ENISA würde auch bei dem **EU-Konzeptentwurf für Cybersicherheit**, der als Teil des Pakets vorgelegt wurde, und bei der Ausarbeitung der Empfehlung der Kommission an die Mitgliedstaaten für eine koordinierte Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen großen Ausmaßes auf EU-Ebene eine Rolle spielen[13]. Die ENISA würde die Zusammenarbeit zwischen den einzelnen Mitgliedstaaten bei der Reaktion auf Notfälle durch die Analyse und Aggregierung der nationalen Lageberichte auf der Grundlage der Informationen, die der Agentur von den Mitgliedstaaten und anderen Einrichtungen auf freiwilliger Basis zur Verfügung gestellt werden, erleichtern.

- **Zertifizierung der Cybersicherheit von IKT-Produkten und -Diensten**

Um Vertrauen und Sicherheit herzustellen und zu wahren, müssen bei IKT-Produkten und -Diensten Sicherheitsmerkmale unmittelbar in der Frühphase ihrer technischen Konzeption und Entwicklung eingebaut werden („security by design“ – eingebaute Sicherheit). Außerdem müssen Kunden und Nutzer feststellen können, welche Vertrauenswürdigkeitsstufe die von ihnen beschafften oder gekauften Produkte und Dienste haben.

Die Zertifizierung, die in der förmlichen Evaluierung von Produkten, Diensten und Prozessen durch eine unabhängige und akkreditierte Stelle anhand bestimmter definierter Kriterien und Normen und in der Ausstellung einer Bescheinigung besteht, aus der die Übereinstimmung mit ihnen hervorgeht, spielt eine wichtige Rolle dabei, das Vertrauen in Produkte und Dienste zu stärken und ihre Sicherheit zu erhöhen. Auch wenn Sicherheitsevaluierungen ziemlich technisch sind, so dient die Zertifizierung doch dazu, Käufer und Nutzer über die Sicherheitseigenschaften der IKT-Produkte und -Dienste, die sie kaufen oder verwenden, zu informieren und etwaige diesbezügliche Bedenken auszuräumen. Wie vorstehend ausgeführt, ist dies besonders relevant für neue Systeme, die die digitale Technik ausgiebig nutzen und ein hohes Maß an Sicherheit erfordern, wie z. B. vernetzte und selbstfahrende Autos,

[13] Der Konzeptentwurf wird Anwendung finden auf Cybersicherheitsvorfälle, die so große Störungen hervorrufen, dass der betroffene Mitgliedstaat sie allein nicht bewältigen kann, oder die so weitreichende und beträchtliche Auswirkungen von technischer oder politischer Tragweite auf zwei oder mehr Mitgliedstaaten oder EU-Organe haben, dass rasch koordinierte Maßnahmen zu treffen sind und auf Unionsebene politisch reagiert werden muss.

elektronische Gesundheitsdienste, industrielle Automatisierungssteuerungssysteme (Industrial Automation Control Systems – IACS)[14] und intelligente Netze.

Derzeit ist die Lage hinsichtlich der Cybersicherheitszertifizierung von IKT-Produkten und -Diensten in der EU sehr uneinheitlich. Es gibt eine Reihe internationaler Initiativen, z. B. die sogenannten *Common Criteria (CC) for Information Technology Security Evaluation* (ISO 15408) – eine internationale Norm für die Evaluierung der IT-Sicherheit. Sie beruht auf der Evaluierung durch Dritte und sieht sieben Vertrauenswürdigkeitsstufen (*Evaluation Assurance Levels, EAL*) vor. Die CC und die begleitende gemeinsame Methodik für die Evaluierung der Sicherheit von Informationstechnologien (*Methodology for Information Technology Security Evaluation, CEM*) bilden die technische Grundlage für ein internationales Abkommen über die Anerkennung der CC (*Common Criteria Recognition Arrangement, CCRA*), durch das sichergestellt wird, dass CC-Zertifikate von allen Unterzeichnern des CCRA anerkannt werden. Gemäß der aktuellen Fassung des CCRA werden jedoch nur Evaluierungen bis zur Stufe EAL 2 gegenseitig anerkannt. Außerdem haben nur 13 Mitgliedstaaten das Abkommen unterzeichnet.

Die Zertifizierungsbehörden von 12 Mitgliedstaaten haben ein Abkommen über die gegenseitige Anerkennung der Zertifikate geschlossen, die in Übereinstimmung mit dem Abkommen auf der Grundlage der CC ausgestellt wurden[15]. Darüber hinaus gibt es in den Mitgliedstaaten bereits mehrere IKT-Zertifizierungsinitiativen oder es werden solche gerade auf den Weg gebracht. Wenngleich diese Initiativen wichtig sind, bergen sie doch die Gefahr einer Marktfragmentierung und können Interoperabilitätsprobleme verursachen. Dies hat zur Folge, dass ein Unternehmen unter Umständen mehrere Zertifizierungsverfahren in verschiedenen Mitgliedstaaten durchlaufen muss, um sein Produkt auf mehreren Märkten anbieten zu können. So muss beispielsweise ein Hersteller intelligenter Stromzähler, der seine Produkte in drei Mitgliedstaaten, etwa in Deutschland, Frankreich und im Vereinigten Königreich, verkaufen möchte, derzeit die Anforderungen von drei verschiedenen Zertifizierungssystemen erfüllen. Diese Systeme sind das System *„Commercial Product Assurance“ (CPA)* im Vereinigten Königreich, das System *„Certification de Sécurité de Premier Niveau“ (CSPN)* in Frankreich und ein auf den CC beruhendes spezielles Schutzprofil in Deutschland.

Diese Situation führt zu höheren Kosten und bedeutet für Unternehmen, die in mehreren Mitgliedstaaten tätig sind, einen erheblichen Verwaltungsaufwand. Auch wenn die Zertifizierungskosten in Abhängigkeit von dem jeweiligen Produkt/Dienst, der angestrebten Vertrauenswürdigkeitsstufe und/oder anderen Komponenten sehr unterschiedlich sein können, sind sie für die Unternehmen in der Regel relativ hoch. Die Smart-Meter-Gateway-Zertifizierung durch das BSI kostet beispielsweise mehr als 1 Mio. EUR (höchste Prüf- und Vertrauenswürdigkeitsstufe, bei der nicht nur ein Produkt, sondern auch die gesamte umgebende Infrastruktur geprüft wird). Die Kosten für die Zertifizierung intelligenter Zähler

---

14 Die GD JRC hat einen Bericht veröffentlicht, in dem erste gemeinsame europäische Anforderungen vorgeschlagen und die Grundzüge der Cybersicherheitszertifizierung von IACS-Komponenten vorgestellt werden. Abrufbar unter: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

15 Der Gruppe Hoher Beamter für Informationssicherheit (SOG-IS) gehören 12 Mitgliedstaaten und Norwegen an; sie hat für eine begrenzte Anzahl von Produkten wie z. B. digitale Signaturen, digitale Fahrtenschreiber und Chipkarten einige Schutzprofile entwickelt. Die Teilnehmer arbeiten zusammen, um die Standardisierung von CC-Schutzprofilen abzustimmen, und koordinieren die Entwicklung von Schutzprofilen. In den nationalen öffentlichen Ausschreibungen verlangen die Mitgliedstaaten häufig eine SOG-IS-Zertifizierung.

im Vereinigten Königreich belaufen sich auf knapp 150 000 EUR. In Frankreich sind die Kosten mit denen im Vereinigten Königreich vergleichbar: ca. 150 000 EUR oder mehr.

Wichtige öffentliche und privaten Interessenträger haben festgestellt, dass ohne ein EU-weites Zertifizierungssystem für die Cybersicherheit Unternehmen in vielen Fällen in jedem einzelnen Mitgliedstaat eine Zertifizierung durchlaufen müssen, was zu einer Fragmentierung des Marktes führt. Besonders hervorzuheben ist, dass ohne EU-Harmonisierungsrechtsvorschriften für IKT-Produkte und -Dienste Unterschiede bei den Normen und Praktiken im Bereich der Cybersicherheitszertifizierung in den Mitgliedstaaten dazu führen können, dass in der EU in der Praxis 28 getrennte Sicherheitsmärkte mit jeweils eigenen technischen Anforderungen, Prüfverfahren und Cybersicherheitszertifizierungs-verfahren entstehen. Diese divergierenden nationalen Ansätze können, falls keine geeigneten Maßnahmen auf EU-Ebene ergriffen werden, einen erheblichen Rückschlag für die Verwirklichung des digitalen Binnenmarkts zur Folge haben und die damit verbundenen positiven Auswirkungen auf Wachstum und Beschäftigung verlangsamen oder gar nicht erst aufkommen lassen.

Ausgehend von den vorstehend genannten Entwicklungen wird mit der vorgeschlagenen Verordnung ein europäischer Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten („der **Rahmen**“) geschaffen und werden die wesentlichen Funktionen und Aufgaben der ENISA im Bereich der Cybersicherheitszertifizierung festgelegt. Der vorliegende Vorschlag enthält ein umfassendes Rahmenregelwerk für europäische Cybersicherheitszertifizierungssysteme. Mit ihm werden keine unmittelbar operativen Zertifizierungssysteme eingeführt, sondern es wird vielmehr ein System (ein Rahmen) für die Ausarbeitung spezifischer Zertifizierungssysteme für bestimmte IKT-Produkte/-Dienste (im Folgenden „europäische Systeme für die Cybersicherheitszertifizierung“) geschaffen. Dadurch, dass europäische Systeme für die Cybersicherheitszertifizierung im Einklang mit dem Rahmen geschaffen werden, werden die auf der Grundlage dieser Systeme ausgestellten Zertifikate in allen Mitgliedstaaten gültig sein und anerkannt werden; außerdem wird dadurch der derzeit bestehenden Marktfragmentierung entgegengewirkt.

Genereller Zweck eines europäischen Systems für die Cybersicherheitszertifizierung ist es, zu bescheinigen, dass IKT-Produkte und -Dienste, die gemäß diesem System zertifiziert wurden, bestimmte Cybersicherheitsanforderungen erfüllen. Dies würde z. B. den von ihnen gebotenen Schutz der Daten (unabhängig davon, ob diese gespeichert, übermittelt oder auf sonstige Weise verarbeitet werden) vor zufälligen oder unberechtigten Speicherungs-, Verarbeitungs-, Zugangs-, Offenlegungs- und Vernichtungsvorgängen und vor zufälligen Verlusten oder Veränderungen umfassen. EU-Systeme für die Cybersicherheitszertifizierung würden hinsichtlich der technischen Anforderungen, die die Produkte erfüllen müssen, und hinsichtlich der entsprechenden Evaluierungsverfahren auf vorhandene Normen zurückgreifen und die technischen Normen nicht selbst entwickeln[16]. Eine EU-weite Zertifizierung von Produkten wie Chipkarten, die derzeit anhand internationaler CC-Normen im Rahmen des (vorstehend beschriebenen) multilateralen SOG-IS-Systems geprüft werden, würde beispielsweise bedeuten, dass dieses System in der gesamten EU Gültigkeit erlangen würde.

In dem Vorschlag werden nicht nur bestimmte Sicherheitsziele umrissen, die bei der Konzipierung eines konkreten europäischen Systems für die Cybersicherheitszertifizierung zu

[16] Europäische Normen werden von europäischen Normungsorganisationen entwickelt, die von der Europäischen Kommission durch die Veröffentlichung im *Amtsblatt* bestätigt werden (siehe Verordnung (EU) Nr. 1025/2012).

berücksichtigen sind, sondern es wird auch der Mindestinhalt solcher Systeme beschrieben. Derartige Systeme müssen u. a. eine Reihe von bestimmten Elementen definieren, die den Umfang und Gegenstand der Cybersicherheitszertifizierung festlegen. Dazu zählen die Nennung der Kategorien der erfassten Produkte und Dienste, die detaillierte Festlegung der Cybersicherheitsanforderungen (z. B. durch Bezugnahme auf einschlägige Normen oder technische Spezifikationen), die spezifischen Evaluierungskriterien und -methoden sowie die Vertrauenswürdigkeitsstufe, die durch sie gewährleistet werden soll (d. h. niedrig, mittel oder hoch).

Europäische Systeme für die Cybersicherheitszertifizierung werden von der ENISA mit der Unterstützung und mit der fachlichen Beratung der Europäischen Gruppe für die Cybersicherheitszertifizierung (siehe unten) und in enger Zusammenarbeit mit ihr ausgearbeitet und von der Kommission durch Durchführungsrechtsakte verabschiedet werden. Wenn der Bedarf für ein Cybersicherheitszertifizierungssystem festgestellt wird, wird die Kommission die ENISA auffordern, ein System für bestimmte IKT-Produkte und -Dienste auszuarbeiten. Die Arbeiten der ENISA am System werden in enger Zusammenarbeit mit den in der Gruppe vertretenen nationalen Aufsichtsbehörden für die Zertifizierung erfolgen. Die Mitgliedstaaten und die Gruppe können der Kommission vorschlagen, dass die Kommission die ENISA zur Ausarbeitung eines besonderen Systems auffordert.

Die Zertifizierung kann ein sehr kostspieliger Prozess sein, was wiederum zu höheren Preisen für die Kunden und Verbraucher führen kann. Die Notwendigkeit einer Zertifizierung kann auch je nach spezifischem Kontext der Nutzung der Produkte und Dienste und in Abhängigkeit vom raschen technologischen Wandel erheblich variieren. Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte daher weiterhin auf freiwilliger Basis erfolgen, sofern in den Rechtsvorschriften der Union zur Festlegung von Anforderungen an die Sicherheit von IKT-Produkten und -Diensten nicht etwas anderes bestimmt ist.

Im Interesse der Harmonisierung und zur Vermeidung der Fragmentierung werden nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten, die Gegenstand eines europäischen Systems für die Cybersicherheitszertifizierung sind, ab dem im Durchführungsrechtsakt für die Annahme des Systems festgelegten Datum keine Anwendung mehr finden. Ferner sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten, die unter ein bestehendes europäisches System für die Cybersicherheitszertifizierung fallen, einführen.

Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet ist, werden die Hersteller von IKT-Produkten und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte oder Dienste bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. Die Konformitätsbewertungsstellen sollten von einer Akkreditierungsstelle akkreditiert werden, sofern sie bestimmten Anforderungen genügen. Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen werden die einer Konformitätsbewertungsstelle erteilte Akkreditierung widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

Im Vorschlag ist vorgesehen, dass die Überwachungs-, Aufsichts- und Durchsetzungsaufgaben den Mitgliedstaaten obliegen. Die Mitgliedstaaten müssen eine für die Zertifizierung zuständige Aufsichtsbehörde stellen. Aufgabe dieser Behörde wird die Aufsicht darüber sein, dass die in ihrem Hoheitsgebiet ansässigen

Konformitätsbewertungsstellen und die von diesen ausgestellten Zertifikate den Anforderungen genügen, die in dieser Verordnung und in den jeweiligen europäischen Cybersicherheitszertifizierungssystemen festgelegt sind. Die nationalen Aufsichtsbehörden für die Zertifizierung werden Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf die von Konformitätsbewertungsstellen in ihrem Hoheitsgebiet ausgestellten Zertifikate eingereicht werden, bearbeiten. Sie werden den Beschwerdegegenstand, soweit angemessen, untersuchen und den Beschwerdeführer über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist unterrichten. Darüber hinaus werden sie mit anderen Aufsichtsbehörden für die Zertifizierung und anderen öffentlichen Stellen zusammenarbeiten, z. B. indem sie Informationen über die etwaige Nichtkonformität von IKT-Produkten und -Diensten mit den Anforderungen dieser Verordnung oder mit bestimmten europäischen Systemen für die Cybersicherheitszertifizierung austauschen.

Und schließlich wird mit dem Vorschlag die Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) eingesetzt, die aus den nationalen Zertifizierungsaufsichtsbehörden aller Mitgliedstaaten besteht. Hauptaufgabe der Gruppe ist die Beratung der Kommission in Fragen der Cybersicherheitszertifizierungspolitik und die Zusammenarbeit mit der ENISA bei der Entwicklung vorläufiger europäischer Systeme für die Cybersicherheitszertifizierung. Die ENISA wird die Kommission dadurch unterstützen, dass sie das Sekretariat der Gruppe stellt, und sie wird ein aktualisiertes öffentliches Verzeichnis der Systeme führen, die gemäß dem europäischen Rahmen für die Cybersicherheitszertifizierung genehmigt wurden. Die ENISA würde auch Kontakte zu den Normungsgremien pflegen, um die Zweckmäßigkeit der in den genehmigten Systemen verwendeten Normen sicherzustellen und Bereiche zu benennen, in denen ein Normungsbedarf im Bereich der Cybersicherheit besteht.

Der europäische Rahmen für die Cybersicherheitszertifizierung (im Folgenden „der Rahmen“) wird Bürgern und Unternehmen mehrere Vorteile bieten. Besonders herauszustellen sind die folgenden:

- Mit der Einführung EU-weiter Systeme für die Cybersicherheitszertifizierung für bestimmte Produkte oder Dienste erhalten die Unternehmen eine „zentrale Anlaufstelle“ für die Zertifizierung der Cybersicherheit in der EU. Diese Unternehmen müssen ihr Produkt nur einmal zertifizieren lassen und erhalten ein in allen Mitgliedstaaten gültiges Zertifikat. Sie müssen ihre Produkte nicht von unterschiedlichen nationalen Zertifizierungsstellen erneut zertifizieren lassen. Dies wird die Kosten für die Unternehmen deutlich verringern, grenzüberschreitende Tätigkeiten erleichtern und letztlich eine Fragmentierung des Binnenmarkts für die jeweiligen Produkte verringern oder vermeiden.
- Mit dem Rahmen wird der Vorrang der europäischen Systeme für die Cybersicherheitszertifizierung vor den nationalen Systemen festgelegt: Nach dieser Regelung ersetzt ein verabschiedetes europäisches System für die Cybersicherheitszertifizierung alle bestehenden parallelen nationalen Systeme für dieselben IKT-Produkte oder -Dienste einer bestimmten Vertrauenswürdigkeitsstufe. Dies wird mehr Klarheit schaffen und den derzeitigen Wildwuchs sich überschneidender und möglicherweise widersprüchlicher nationaler Zertifizierungssysteme im Bereich der Cybersicherheit eindämmen.
- Ferner unterstützt und ergänzt der Vorschlag die Umsetzung der NIS-Richtlinie, indem sie Unternehmen, die der Richtlinie unterliegen, ein äußerst nützliches Werkzeug an die Hand gibt, um die Einhaltung der NIS-Anforderungen in der gesamten Europäischen Union nachzuweisen. Bei der Entwicklung neuer Systeme

für die Cybersicherheitszertifizierung werden die Kommission und die ENISA ein besonderes Augenmerk darauf legen, dass sich die NIS-Anforderungen in den Systemen für die Cybersicherheitszertifizierung widerspiegeln.

- Der Vorschlag wird die Entwicklung einer europäischen Cybersicherheitspolitik durch die Harmonisierung der Bedingungen und Anforderungen für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten in der EU unterstützen und fördern. Europäische Systeme für die Cybersicherheitszertifizierung werden sich auf gemeinsame Normen oder Evaluierungskriterien und Prüfverfahren beziehen. Dies wird, wenn auch nur indirekt, wesentlich zur Verbreitung gemeinsamer Sicherheitslösungen in der EU beitragen und dadurch auch Hindernisse für den Binnenmarkt beseitigen.
- Der Rahmen ist so konzipiert, dass die für die Cybersicherheitszertifizierungssysteme notwendige Flexibilität gewährleistet ist. Je nach den spezifischen Cybersicherheitserfordernissen kann ein Produkt oder ein Dienst für ein höheres oder niedrigeres Sicherheitsniveau zertifiziert werden. Europäische Systeme für die Cybersicherheitszertifizierung werden unter Berücksichtigung dieser Flexibilität konzipiert werden und daher verschiedene Vertrauenswürdigkeitsstufen (d. h. niedrig, mittel oder hoch) vorsehen, damit sie für unterschiedliche Zwecke oder in unterschiedlichen Kontexten verwendet werden können.
- Alle oben genannten Elemente werden bewirken, dass die Unternehmen die Cybersicherheitszertifizierung vermehrt als ein wirksames Mittel betrachten, um die Vertrauenswürdigkeitsstufen von IKT-Produkten oder -Diensten zu kommunizieren. In dem Maße, in dem die Cybersicherheitszertifizierung billiger, wirksamer und kommerziell attraktiver wird, werden die Unternehmen größere Anreize haben, ihre Produkte unter dem Aspekt der Cybersicherheit zertifizieren zu lassen, und damit einen Beitrag zur besseren Verbreitung von Cybersicherheitspraktiken bei der Konzeption von IKT-Produkten und -Diensten (eingebaute Cybersicherheit) zu leisten.

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

Nach der NIS-Richtlinie müssen Wirtschaftsbeteiligte in Sektoren, die für unsere Wirtschaft und Gesellschaft von entscheidender Bedeutung sind, wie z. B. Energie, Verkehr, Wasser, Banken, Finanzmarktinfrastrukturen, Gesundheitswesen und digitale Infrastruktur, sowie Anbieter digitaler Dienste (z. B. Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze) Maßnahmen zur angemessenen Beherrschung der Sicherheitsrisiken ergreifen. Die neuen Bestimmungen des vorliegenden Vorschlags ergänzen die Vorschriften der NIS-Richtlinie und gewährleisten die Kohärenz mit ihr, um die Abwehrfähigkeit der EU gegen Cyberangriffe durch mehr Kapazitäten, Zusammenarbeit, Risikomanagement und Sensibilisierung weiter zu verbessern.

Darüber hinaus sind die Bestimmungen zur Cybersicherheitszertifizierung ein wichtiges Instrument für Unternehmen, die unter die NIS-Richtlinie fallen, da sie ihre IKT-Produkte und -Dienste auf der Basis von in der gesamten EU gültigen und anerkannten Cybersicherheitszertifizierungssystemen entsprechend dem Cybersicherheitsrisiko

zertifizieren lassen können. Die Bestimmungen ergänzen auch die in der eIDAS-Verordnung[17] und in der Funkanlagenrichtlinie[18] festgelegten Sicherheitsanforderungen.

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

Die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)[19] enthält Festlegungen für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen, die dem Nachweis dienen, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Verarbeitung von Daten sich an die Bestimmungen der Verordnung gehalten haben. Die Zertifizierung von Datenverarbeitungsvorgängen, die unter die Datenschutz-Grundverordnung fallen, auch wenn solche Vorgänge in Produkte und Dienste eingebettet sind, bleibt von dieser Verordnung unberührt.

Die vorgeschlagene Verordnung wird die Vereinbarkeit mit der Verordnung (EG) Nr. 765/2008 über die Vorschriften für die Akkreditierung und Marktüberwachung[20] durch die Bezugnahme auf die Vorschriften jenes Rahmens für die nationalen Akkreditierungsstellen und Konformitätsbewertungsstellen sicherstellen. Was die Aufsichtsbehörden betrifft, so sieht der Verordnungsvorschlag vor, dass die Mitgliedstaaten nationale Aufsichtsbehörden für die Zertifizierung benennen müssen, die für die Aufsicht sowie für die Überwachung und Durchsetzung der Vorschriften zuständig sind. Diese Stellen bleiben gemäß der Verordnung (EG) Nr. 765/2008 von den Konformitätsbewertungsstellen getrennt.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄSSIGKEIT

- **Rechtsgrundlage**

Die Rechtsgrundlage für ein Tätigwerden der EU ist Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der die Angleichung der Rechtsvorschriften der Mitgliedstaaten im Hinblick auf die Verwirklichung des in Artikel 26 AEUV genannten Ziels, nämlich das ordnungsgemäße Funktionieren des Binnenmarkts, betrifft.

Die auf den Binnenmarkt gestützte Rechtsgrundlage für die Gründung der ENISA wurde vom Gerichtshof in der Rechtssache C-217/04 (*Vereinigtes Königreich gegen Europäisches Parlament und Rat*) aufrechterhalten und durch die Verordnung aus dem Jahr 2013, in der das derzeitige Mandat der Agentur festgelegt wurde, erneut bestätigt. Außerdem würden Tätigkeiten, die die Ziele einer vermehrten Zusammenarbeit und Koordinierung zwischen den

---

17 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.

18 Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG.

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

20 Verordnung (EG) Nr. 765/2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93.

Mitgliedstaaten widerspiegeln, und solche, durch die Kapazitäten auf EU-Ebene zur Ergänzung der Maßnahmen der Mitgliedstaaten ausgebaut werden, in die Kategorie „operative Zusammenarbeit“ fallen. Diese wird in der NIS-Richtlinie (deren Rechtsgrundlage Artikel 114 AEUV ist) eigens als ein Ziel festgelegt, das im Rahmen des CSIRTs-Netzes verfolgt werden soll – diesbezüglich heißt es wie folgt: ... „die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit“ (Artikel 12 Absatz 2). Insbesondere in Artikel 12 Absatz 3 Buchstabe f werden weitere Formen der operativen Zusammenarbeit als Aufgabe des CSIRTs-Netzes genannt, u. a. im Zusammenhang mit i) Kategorien von Risiken und Sicherheitsvorfällen, ii) Frühwarnungen, iii) gegenseitiger Unterstützung und Grundsätzen und Modalitäten der Koordinierung bei der Reaktion der Mitgliedstaaten auf grenzüberschreitende Risiken und Vorfälle.

- Die derzeitige Fragmentierung der Zertifizierungssysteme für IKT-Produkte und -Dienste ist auch eine Folge des Fehlens eines gemeinsamen, rechtsverbindlichen und wirksamen Rahmenprozesses, der für die Mitgliedstaaten gilt. Dies behindert die Schaffung eines Binnenmarktes für IKT-Produkte und -Dienste und beeinträchtigt die Wettbewerbsfähigkeit der europäischen Industrie in diesem Sektor. Mit dem vorliegenden Vorschlag sollen die vorhandene Fragmentierung und die damit verbundenen Hindernisse auf dem Binnenmarkt durch die Schaffung eines gemeinsamen Rahmens für die Ausarbeitung von EU-weit gültigen Systemen für die Cybersicherheitszertifizierung angegangen werden.

Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Das Subsidiaritätsprinzip erfordert eine Bewertung der Notwendigkeit und des Mehrwerts des Handelns der EU. Die Einhaltung des Subsidiaritätsprinzips in diesem Bereich wurde bereits bei der Annahme der derzeitigen ENISA-Verordnung[21] anerkannt.

Cybersicherheit ist ein Thema von gemeinsamem Interesse der Union. Die gegenseitigen Abhängigkeiten zwischen Netz- und Informationssystemen sind so groß, dass die einzelnen Akteure (öffentliche und private Akteure, einschließlich der Bürger) sehr häufig den Bedrohungen nicht begegnen und die Risiken sowie die möglichen Auswirkungen von Cybersicherheitsvorfällen nicht isoliert bewältigen können. Zum einen bedeuten die gegenseitigen, über Landesgrenzen hinweg reichenden Abhängigkeiten, auch hinsichtlich des Betriebs kritischer Infrastrukturen (Energie, Verkehr, Wasser, um nur einige zu nennen), dass Maßnahmen auf europäischer Ebene nicht nur sinnvoll, sondern auch notwendig sind. Zum anderen kann ein Eingreifen der EU durch den Austausch bewährter Verfahren zwischen den Mitgliedstaaten einen positiven „Spill-over“-Effekt haben, der zu mehr Cybersicherheit in der Union führen kann.

Zusammenfassend lässt sich feststellen, dass im aktuellen Kontext und mit Blick auf die künftigen Szenarios **einzelne Maßnahmen der EU-Mitgliedstaaten und eine uneinheitliche Herangehensweise an die Cybersicherheit nicht ausreichen werden, um die kollektive Cyberabwehrfähigkeit der Union zu steigern**.

Ein Tätigwerden der EU wird auch als notwendig erachtet, um Lösungen für das Problem der nebeneinander bestehenden Systeme für die Cybersicherheitszertifizierung zu finden. Hersteller könnten so durch erhebliche Einsparungen bei den Kosten für die Prüfung und

[21] 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.

Neukonzeption von Produkten in vollem Umfang vom Binnenmarkt profitieren. Das aktuelle Abkommen über die gegenseitige Anerkennung (*Mutual Recognition Agreement, MRA*) der Gruppe Hoher Beamter für Informationssicherheit (SOG-IS) beispielsweise hat diesbezüglich zu wichtigen Ergebnissen geführt, zeigte aber auch, dass es aufgrund der ihm gesetzten engen Grenzen nicht geeignet ist, längerfristige nachhaltige Lösungen hervorzubringen, mit denen der Binnenmarkt sein volles Potenzial entfalten könnte.

Der Mehrwert des Tätigwerdens auf EU-Ebene, insbesondere zur Stärkung der Zusammenarbeit zwischen den Mitgliedstaaten, aber auch zwischen den Fachkreisen auf dem Gebiet der Netz- und Informationssicherheit, wurde in den Schlussfolgerungen des Rates[22] von 2016 anerkannt und geht auch klar aus der Bewertung der ENISA hervor.

- **Verhältnismäßigkeit**

Die vorgeschlagenen Maßnahmen gehen nicht über das für die Erreichung der angestrebten Politikziele erforderliche Maß hinaus. Zudem werden weitere einzelstaatliche Maßnahmen in Angelegenheiten der nationalen Sicherheit durch den Geltungsbereich der EU-Maßnahmen nicht beeinträchtigt. Ein Tätigwerden der EU ist daher aus Gründen der Subsidiarität und Verhältnismäßigkeit gerechtfertigt.

- **Wahl des Instruments**

Mit dem vorliegenden Vorschlag wird die Verordnung (EU) Nr. 526/2013 überarbeitet, in der das derzeitige Mandat und die derzeitigen Aufgaben der ENISA festgelegt sind. Angesichts der wichtigen Rolle der ENISA beim Aufbau und bei der Handhabung eines EU-Rahmens für die Cybersicherheitszertifizierung ist es am sinnvollsten, das neue ENISA-Mandat und den besagten Rahmen mit einem einzigen Rechtsinstrument, dem Instrument einer Verordnung, festzulegen.

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

Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften

Im Einklang mit dem Evaluierungsfahrplan[23] hat die Kommission die **Relevanz, Wirkung, Wirksamkeit, Effizienz und Kohärenz sowie den EU-Mehrwert** der Agentur im Hinblick auf ihre Leistungen, Führung, interne Organisationsstruktur und Arbeitsmethoden im Zeitraum 2013-2016 bewertet. Die Hauptergebnisse lassen sich wie im Folgenden dargestellt zusammenfassen (weitere Einzelheiten sind der Arbeitsunterlage der Kommissionsdienststellen über die Folgenabschätzung beigefügt).

- **Relevanz:** Vor dem Hintergrund der technologischen Entwicklungen und der sich ändernden Bedrohungen sowie der dringenden Notwendigkeit einer verbesserten Cybersicherheit in der EU erwiesen sich die Ziele der ENISA als relevant. Die Mitgliedstaaten und die EU-Einrichtungen verlassen sich auf ihre umfassende Fachkompetenz im Bereich der Cybersicherheit. Zudem müssen in den

[22] Schlussfolgerungen des Rates zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche vom 15. November 2016.

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

Mitgliedstaaten Kapazitäten aufgebaut werden, um Bedrohungen besser verstehen und abwehren zu können, und die Interessenträger müssen über alle Themenbereiche und Einrichtungen hinweg zusammenarbeiten. Die Cybersicherheit ist nach wie vor eine zentrale politische Priorität der EU, und von der ENISA wird erwartet, dass sie ihr gerecht wird. Die Ausgestaltung der ENISA als EU-Agentur mit einem befristeten Mandat jedoch i) erlaubt keine langfristige Planung und keine nachhaltige Unterstützung der Mitgliedstaaten und der EU-Organe, ii) kann zu einem rechtlichen Vakuum führen, da die Bestimmungen der NIS-Richtlinie, durch die die ENISA mit Aufgaben betraut wurde, dauerhafter Art sind[24], und iii) lässt sich nicht mit einer Zielvorstellung vereinbaren, die die ENISA mit einem verstärkten EU-Cybersicherheitsökosystem in Verbindung bringt.

- **Wirksamkeit:** Insgesamt hat die ENISA ihre Ziele erreicht und ihre Aufgaben wahrgenommen. Durch ihre Haupttätigkeiten (Aufbau von Kapazitäten, Bereitstellung von Fachwissen, Aufbau von Fachkreisen, Unterstützung der Politik) hat sie einen Beitrag zu mehr Netz- und Informationssicherheit in Europa geleistet. Bei den einzelnen Bereichen bestand allerdings ein gewisses Verbesserungspotenzial. Die Bewertung kam zu dem Schluss, dass die ENISA auf wirksame Weise starke und vertrauensvolle Beziehungen zu einigen ihrer Interessenträger, insbesondere zu den Mitgliedstaaten und den CSIRTs-Kreisen, aufgebaut hat. Maßnahmen im Bereich des Kapazitätsaufbaus wurden vor allem für Mitgliedstaaten mit weniger Ressourcen als wirksam angesehen. Besonders hervorzuheben war die Förderung einer breit angelegten Zusammenarbeit; die Interessenträger stimmten weitgehend darin überein, dass die ENISA eine positive Rolle dabei spielt, Menschen zusammenzuführen. Die ENISA hatte jedoch Schwierigkeiten, auf dem weiten Feld der Netz- und Informationssicherheit große Wirkung zu entfalten. Dies war auch darauf zurückzuführen, dass sie über nur relativ begrenzte personelle und finanzielle Ressourcen verfügte, um ein sehr umfassendes Mandat zu erfüllen. Eine weitere Schlussfolgerung der Bewertung war, dass die ENISA das Ziel der Bereitstellung von Fachwissen nur zum Teil erreichte, was mit den Schwierigkeiten bei der Rekrutierung von Sachverständigen zusammenhing (siehe nachstehenden Abschnitt zur Effizienz).
- **Effizienz:** Trotz ihrer geringen Mittelausstattung (die im Vergleich mit der anderer EU-Agenturen zu den niedrigsten gehört) war die Agentur in der Lage, einen Beitrag zu den gesetzten Zielen zu leisten, wobei sie bei der Nutzung ihrer Ressourcen insgesamt Effizienz bewies. Die Bewertung kam zu dem Schluss, dass die Prozesse im Allgemeinen effizient waren und eine klare Abgrenzung der Zuständigkeiten innerhalb der Organisation eine gute Durchführung der Arbeiten zur Folge hatte. Eine der wesentlichen Herausforderungen in Bezug auf die Effizienz der Agentur betrifft die Schwierigkeiten der ENISA, hoch qualifizierte Sachverständige zu rekrutieren und zu binden. Die Ergebnisse zeigen, dass sich dies durch eine Kombination von Faktoren erklären lässt, u. a. durch die allgemeinen Schwierigkeiten des gesamten öffentlichen Sektors, bei der Einstellung hoch spezialisierter Fachleute mit dem privaten Sektor zu konkurrieren, die Art der Verträge (Befristung), die die Agentur in den meisten Fällen anbieten konnte, und die eher geringe Attraktivität des Standorts der ENISA, z. B. aufgrund der Schwierigkeiten für den Ehepartner, einen Arbeitsplatz zu finden. Die Aufteilung

[24] Verweis auf die Artikel 7, 9, 11, 12 und 19 der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS -Richtlinie).

zwischen Athen und Heraklion erforderte zusätzliche Koordinierungsanstrengungen und verursachte zusätzliche Kosten, aber die Übersiedlung der Abteilung für das Kerngeschäft nach Athen im Jahr 2013 hat die operative Effizienz der Agentur verbessert.

- **Kohärenz:** Die Tätigkeiten der ENISA standen im Allgemeinen mit der Politik und den Aktivitäten der Interessenträger auf nationaler und EU-Ebene in Einklang, auf EU-Ebene muss jedoch der Ansatz im Hinblick auf die Cybersicherheit besser koordiniert werden. Das Potenzial für eine Zusammenarbeit zwischen der ENISA und anderen EU-Einrichtungen wurde noch nicht voll ausgeschöpft. Die Weiterentwicklung der rechtlichen und politischen Landschaft in der EU hatte zur Folge, dass das aktuelle Mandat jetzt weniger stimmig ist.

- **Mehrwert durch EU-Maßnahmen:** Der Mehrwert der ENISA besteht in erster Linie darin, dass die Agentur es versteht, die Zusammenarbeit, insbesondere zwischen den Mitgliedstaaten, aber auch mit den einschlägigen Fachkreisen der Netz- und Informationssicherheit, zu verbessern. Auf EU-Ebene gibt es keinen anderen Akteur, der die Zusammenarbeit eines so großen Spektrums unterschiedlicher Interessenträger im Bereich der Netz- und Informationssicherheit unterstützt. Der Mehrwert der Agentur wurde je nach den verschiedenen Bedürfnissen und Ressourcen der Interessenträger (z. B. große/kleine Mitgliedstaaten, Mitgliedstaaten/Industrie) und der Notwendigkeit seitens der Agentur, bei ihren Aktivitäten Prioritäten gemäß dem Arbeitsprogramm zu setzen, unterschiedlich bewertet. Die Bewertung kam zu dem Schluss, dass eine mögliche Einstellung der Arbeiten der ENISA für alle Mitgliedstaaten eine vertane Chance wäre. Es wird nicht möglich sein, im Bereich der Cybersicherheit im selben Maße zwischen den Mitgliedstaaten Fachkreise zu bilden und zusammenzuarbeiten. Ohne eine stärker zentralisierte EU-Agentur wäre das Gesamtbild uneinheitlicher, wenn ein von der ENISA hinterlassenes Vakuum durch eine bilaterale oder regionale Zusammenarbeit geschlossen werden würde.

Speziell hinsichtlich der bisherigen Leistungen der ENISA und ihrer Zukunft zeichneten sich in der 2017 durchgeführten Konsultation[25] folgende Haupttrends ab:

- Die Gesamtleistung der ENISA im Zeitraum 2013-2016 wurde von der Mehrheit der Teilnehmer (74 %) positiv bewertet. Darüber hinaus vertrat die Mehrheit der Befragten die Auffassung, dass die ENISA ihre einzelnen Ziele erreicht (für jedes der Ziele waren mindestens 63 % dieser Meinung). Die Dienste und Produkte der ENISA werden von fast der Hälfte der Befragten (46 %) regelmäßig (monatlich oder häufiger) genutzt und wegen ihrer Qualität (62 %) geschätzt ebenso wie deshalb, weil sie von einer Einrichtung auf EU-Ebene (83 %) stammen.

[25] 90 Teilnehmer aus 19 Mitgliedstaaten antworteten auf die Konsultation (88 Antworten und zwei Positionspapiere), auch nationale Behörden aus 15 Mitgliedstaaten, darunter Frankreich, Italien, Irland und Griechenland, und acht Dachverbände, die eine beträchtliche Anzahl von europäischen Organisationen vertraten, z. B. die Europäische Bankenvereinigung, Digital Europe (als Vertreter der Digitaltechnikbranche in Europa) und den Europäischen Verband der Telekommunikationsbetreiber (ETNO). Die öffentliche Konsultation zur ENISA wurde durch mehrere andere Quellen ergänzt, u. a. durch folgende: i) ausführliche Interviews mit ca. 50 Schlüsselakteuren aus Cybersicherheitskreisen, ii) eine Befragung des CSIRTs-Netzes, iii) eine Befragung des Verwaltungsrates, des Exekutivrates und der Ständigen Gruppe der Interessenträger der ENISA.

- Die Befragten nannten eine Reihe von Defiziten und Problemen hinsichtlich der Zukunft der Cybersicherheit in der EU; von einer Liste mit 16 Punkten wurden die folgenden fünf am häufigsten genannt: die Zusammenarbeit zwischen den Mitgliedstaaten; die Fähigkeit, massive Cyberangriffe zu verhindern, zu erkennen und zu bewältigen; die Zusammenarbeit zwischen den Mitgliedstaaten in Fragen der Cybersicherheit; die Zusammenarbeit und der Informationsaustausch zwischen verschiedenen Interessenträgern, einschließlich der Zusammenarbeit zwischen öffentlichen und privaten Stellen; der Schutz kritischer Infrastrukturen vor Cyberangriffen.
- Eine große Mehrheit (88 %) der Teilnehmer war der Auffassung, dass die derzeit auf EU-Ebene verfügbaren Instrumente und Mechanismen nicht ausreichen oder nur zum Teil geeignet sind, um diese Defizite und Probleme anzugehen. Die Befragten gaben mit großer Mehrheit (98 %) an, dass eine EU-Einrichtung diesem Bedarf gerecht werden sollte, und 99 % der Teilnehmer meinten, die ENISA sei die dafür richtige Organisation.

Konsultation der Interessenträger

- Zwischen dem 12. April und dem 5. Juli. 2016 hat die Kommission eine öffentliche Konsultation zur Überprüfung der ENISA durchgeführt, zu der 421 Antworten[26] eingingen. Aus den Ergebnissen ging hervor, dass nach Ansicht von 67,5 % der Konsultationsteilnehmer die ENISA eine Rolle bei der Festlegung eines harmonisierten Rahmens für die Sicherheitszertifizierung von IT-Produkten und -Diensten spielen könnte.

Aus den Ergebnissen der 2016 durchgeführten Konsultation zur vertraglichen öffentlich-privaten Partnerschaft für Cybersicherheit[27] im Abschnitt über die Zertifizierung ging Folgendes hervor:

- 50,4 % (d. h. 121 von 240) der Befragten wissen nicht, ob nationale Zertifizierungssysteme in den EU-Mitgliedstaaten gegenseitig anerkannt werden. 25,8 % (62 von 240) antworteten mit „Nein“, während 23,8 % (57 von 240) mit „Ja“ antworteten.
- 37,9 % der Befragten (91 von 240) sind der Ansicht, dass die bestehenden Zertifizierungssysteme nicht den Bedürfnissen der europäischen Industrie gerecht werden. Andererseits haben 17,5 % (42 von 240) – in erster Linie globale Unternehmen, die auf dem europäischen Markt tätig sind –, die gegenteilige Auffassung vertreten.
- 49,6 % (119 von 240) der Befragten meinten, es sei nicht einfach, die Gleichwertigkeit von Normen, Zertifizierungssystemen und Kennzeichnungen nachzuweisen. 37,9 % (91 von 240) antworteten mit „Ich weiß nicht“, während nur 12,5 % (30 von 240) mit „Ja“ antworteten.

[26] 162 Beiträge von Bürgern, 33 von Organisationen der Zivilgesellschaft und Verbraucherschutzverbänden, 186 Beiträge von Unternehmen und 40 von Behörden, darunter von solchen, die für die Durchsetzung der e-Datenschutz-Richtlinie zuständig sind.

[27] 240 Interessenträger von nationalen öffentlichen Verwaltungen, Großunternehmen, KMU, Kleinstunternehmen und Forschungseinrichtungen antworteten auf die Fragen im Abschnitt über die Zertifizierung.

Einholung und Nutzung von Expertenwissen

Die Kommission hat sich auf folgenden externen fachlichen Rat gestützt:

- Study on the Evaluation of ENISA (Ramboll/Carsa 2017; Smart no. 2016/0077),
- Study on ICT Security Certification and Labelling – Evidence gathering and impact assessment (PriceWaterhouseCoopers 2017; SMART no. 2016/0029).

Folgenabschätzung

- Im Bericht über die Folgenabschätzung zu dieser Initiative wurden die folgenden Hauptprobleme benannt, die gelöst werden müssen:
- Unterschiedliche, nebeneinander bestehende Konzepte und Ansätze im Bereich der Cybersicherheit in den Mitgliedstaaten,
- verstreute Ressourcen und uneinheitliche Ansätze aller Organe, Einrichtungen und sonstigen Stellen der EU im Bereich der Cybersicherheit und
- unzureichende Sensibilisierung und Aufklärung der Bürger und Unternehmen in Verbindung mit dem zunehmenden Aufkommen zahlreicher nationalen und sektorspezifischen Zertifizierungssysteme.

In dem Bericht wurden für das ENISA-Mandat folgende Optionen bewertet:

- Wahrung des Status quo, d. h. ein erweitertes, aber dennoch zeitlich befristetes Mandat (Basisszenario),
- Auslaufen des derzeitigen ENISA-Mandats ohne Verlängerung und Einstellung der Arbeit der ENISA (keine Maßnahmen),
- eine „reformierte“ ENISA und
- eine vollständig einsatzfähige EU-Cybersicherheitsagentur.

In dem Bericht wurden die folgenden Optionen für die Cybersicherheitszertifizierung bewertet:

- keine Maßnahme (Basisszenario),
- nichtlegislative (nicht zwingende) Maßnahmen,
- ein Rechtsakt der EU zur Schaffung eines verbindlichen Systems für alle Mitgliedstaaten auf der Grundlage des SOG-IS-Systems und
- ein EU-Rahmen für die allgemeine IKT-Cybersicherheitszertifizierung.

Die Analyse ergab, dass eine „reformierte ENISA“ in Verbindung mit einem EU-Rahmen für die allgemeine IKT-Cybersicherheitszertifizierung die bevorzugte Option ist.

Die bevorzugte Option ging aus der Bewertung als die Lösung hervor, mit der die EU die folgenden Ziele am effektivsten erreichen kann: Verbesserung der Cybersicherheitskapazitäten, der Abwehrbereitschaft, der Zusammenarbeit, der Sensibilisierung und der Transparenz sowie Vermeidung einer Marktfragmentierung. Diese Option weist zudem die größte Übereinstimmung mit den politischen Prioritäten auf, die in der EU-Cybersicherheitsstrategie, in den damit verbundenen Strategien (z. B. NIS-Richtlinie) und in der Strategie für den digitalen Binnenmarkt festgelegt wurden. Zudem ergab die

Konsultation, dass die bevorzugte Option von der Mehrheit der Interessenträger unterstützt wird. Darüber hinaus zeigten die im Rahmen der Folgenabschätzung durchgeführten Analysen, dass sich die Ziele bei dieser Option durch einen angemessenen Ressourceneinsatz erreichen ließen.

Der Ausschuss für Regulierungskontrolle der Kommission gab am 24. Juli zunächst eine negative Stellungnahme und nach der Neuvorlage eine befürwortende Stellungnahme am 25. August 2017 ab. Der geänderte Folgenabschätzungsbericht enthielt weitere Nachweise, die endgültigen Schlussfolgerungen der ENISA-Bewertung und zusätzliche Erläuterungen zu den Politikoptionen und ihren Auswirkungen. In Anhang 1 des endgültigen Folgenabschätzungsberichts wird zusammenfassend dargestellt, wie auf die in der zweiten Stellungnahme des Ausschusses vorgebrachten Bemerkungen eingegangen wurde. Insbesondere wurde der Bericht auf den neuesten Stand gebracht, um die Situation in der EU im Bereich der Cybersicherheit ausführlicher zu beschreiben, einschließlich der Maßnahmen, die in der gemeinsamen Mitteilung „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“ [JOIN(2017) 450] enthalten sind und für die ENISA von besonderer Bedeutung sind: der EU-Konzeptentwurf für Cybersicherheit und das Europäische Forschungs- und Kompetenzzentrum für Cybersicherheit, das die Agentur in Fragen des EU-Forschungsbedarfs beraten würde.

In dem Bericht wird erläutert, wie die Reform der Agentur mit den neuen Aufgaben, besseren Beschäftigungsbedingungen und der strukturellen Zusammenarbeit mit den in diesem Bereich tätigen EU-Organen die Attraktivität der Agentur als Arbeitgeber verbessern und dazu beitragen würde, die mit der Rekrutierung von Sachverständigen zusammenhängenden Probleme zu lösen. Anhang 6 des Berichts enthält auch eine geänderte Aufstellung der geschätzten Kosten der politischen Optionen für die ENISA. Hinsichtlich der Zertifizierungsthematik wurde der Bericht überarbeitet, um die bevorzugte Option ausführlicher, auch mit einer grafischen Darstellung, zu erläutern und um die mit dem neuen Zertifizierungsrahmen verbundenen geschätzten Kosten für die Mitgliedstaaten und die Kommission darzulegen. Die Wahl der ENISA als wichtigster Akteur für den Zertifizierungsrahmen wurde weiter erläutert und mit ihrer einschlägigen Fachkompetenz sowie damit begründet, dass sie die einzige Cybersicherheitsagentur auf EU-Ebene ist. Schließlich wurden auch die Abschnitte über die Zertifizierung überarbeitet, um Aspekte zu klären, die den Unterschied zum aktuellen SOG-IS-System betreffen, um die Vorteile der verschiedenen Politikoptionen zu präzisieren und um darzulegen, dass die Art der unter ein europäisches Zertifizierungssystem fallenden IKT-Produkte und -Dienste in dem jeweils genehmigten System definiert werden wird.

Effizienz der Rechtsetzung und Vereinfachung

Entfällt.

Auswirkungen auf die Grundrechte

Für den Schutz der Privatsphäre und der personenbezogenen Daten natürlicher Personen im Einklang mit den Artikeln 7 und 8 der Charta der Grundrechte der EU ist die Cybersicherheit von entscheidender Bedeutung. Bei Cybersicherheitsvorfällen sind die Privatsphäre und der Schutz der personenbezogenen Daten eindeutig gefährdet. Die Cybersicherheit ist somit eine notwendige Voraussetzung für die Wahrung der Privatsphäre und der Vertraulichkeit personenbezogener Daten. Unter diesem Gesichtspunkt stellt der Vorschlag, der auf die

Stärkung der Cybersicherheit in Europa abzielt, eine wichtige Ergänzung der bestehenden Rechtsvorschriften dar, die das Grundrecht auf den Schutz der Privatsphäre und der personenbezogenen Daten gewährleisten. Die Cybersicherheit ist auch von grundlegender Bedeutung für den Schutz der Vertraulichkeit der elektronischen Kommunikation und somit für die Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit sowie andere damit verbundene Rechte wie das Recht auf Gedanken-, Gewissens- und Religionsfreiheit.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Siehe Finanzbogen

5. WEITERE ANGABEN

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

Die Kommission wird die Anwendung der Verordnung überwachen und dem Europäischen Parlament, dem Rat und dem Europäischen Wirtschafts- und Sozialausschuss alle fünf Jahre einen Bewertungsbericht vorlegen. Diese Berichte werden veröffentlicht und geben detailliert Auskunft über die tatsächliche Anwendung und Durchsetzung dieser Verordnung.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Titel I der Verordnung enthält die allgemeinen Bestimmungen: den Gegenstand (Artikel 1), die Begriffsbestimmungen (Artikel 2), einschließlich Verweise auf einschlägige Begriffsbestimmungen aus anderen EU-Rechtsinstrumenten, etwa aus der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS -Richtlinie), aus der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 und aus der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates zur europäischen Normung.

Titel II der Verordnung enthält die wichtigsten Bestimmungen zur ENISA, der EU-Cybersicherheitsagentur.

In Kapitel I dieses Titels werden das Mandat (Artikel 3), die Ziele (Artikel 4) und die Aufgaben der Agentur (Artikel 5 bis 11) beschrieben.

In Kapitel II wird die Organisation der ENISA beschrieben, zudem enthält es wichtige Bestimmungen über ihre Struktur (Artikel 12). Zudem enthält es Bestimmungen, die die Zusammensetzung, die Abstimmungsregeln und die Funktionen des Verwaltungsrats (Abschnitt 1 Artikel 13 bis 17), den Exekutivausschuss (Abschnitt 2 Artikel 18) und den Exekutivdirektor (Abschnitt 3 Artikel 19) betreffen. Ebenso finden sich dort Regelungen zur Zusammensetzung und Rolle der Ständigen Gruppe der Interessenträger (Abschnitt 4 Artikel 20). Zu guter Letzt wird in Abschnitt 5 dieses Kapitels die Arbeitsweise der Agentur präzisiert, einschließlich der Programmplanung, möglicher Interessenkonflikte, der Transparenz und Vertraulichkeit und des Zugangs zu Dokumenten (Artikel 21 bis 25).

Kapitel III betrifft die Aufstellung und Gliederung des Haushaltsplans der Agentur (Artikel 26 und 27) sowie die Regeln für seine Ausführung (Artikel 28 und 29). Das Kapitel enthält auch Bestimmungen zur Erleichterung der Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen (Artikel 30).

Kapitel IV betrifft das Personal der Agentur. Es enthält allgemeine Bestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen sowie Vorschriften über Vorrechte und Befreiungen (Artikel 31 und 32). Geregelt werden auch die Einstellung und die Ernennung des Exekutivdirektors der Agentur (Artikel 33). Und nicht zuletzt enthält das Kapitel Vorschriften für den Rückgriff auf abgeordnete nationale Sachverständige oder sonstiges Personal, das nicht von der Agentur beschäftigt wird (Artikel 34).

Kapitel V schließlich enthält die allgemeinen Bestimmungen zur Agentur. Gegenstand des Kapitels sind die Rechtsform der Agentur (Artikel 35), Bestimmungen zur Haftung, zur Sprachenregelung und zum Schutz personenbezogener Daten (Artikel 36 bis 38) sowie Sicherheitsvorschriften für den Schutz von Verschlusssachen und nicht als Verschlusssache eingestuften vertraulichen Informationen (Artikel 40). In dem Kapitel sind auch Vorschriften für die Zusammenarbeit der Agentur mit Drittländern und internationalen Organisationen (Artikel 39) festgelegt. Darüber hinaus enthält das Kapitel auch Bestimmungen über den Sitz der Agentur und die Betriebsbedingungen sowie über die Verwaltungskontrolle durch den Europäischen Bürgerbeauftragten (Artikel 41 und 42).

In Titel III der Verordnung wird der europäische Zertifizierungsrahmen für die Cybersicherheit von IKT-Produkten und -Diensten („der **Rahmen**“) als *lex generalis* (Artikel 1) festgelegt. In ihm wird festgelegt, welcher allgemeine Zweck mit europäischen Systemen für die Cybersicherheitszertifizierung verfolgt wird, nämlich dafür zu sorgen, dass IKT-Produkte und -Dienste auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten Anforderungen an ihre Fähigkeit genügen, Handlungen zu widerstehen, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten oder die damit verbundenen Funktionen oder Dienste beeinträchtigen (Artikel 43). Darüber hinaus werden die Sicherheitsziele der europäischen Systeme für die Cybersicherheitszertifizierung aufgeführt (Artikel 45), u. a. die Fähigkeit zum Schutz der Daten gegen einen zufälligen oder unrechtmäßigen Zugang, gegen eine zufällige oder unrechtmäßige Offenlegung, Zerstörung oder Veränderung; genannt werden auch die Inhalte (d. h. die Elemente) der europäischen Systeme für die Cybersicherheitszertifizierung, z. B. die genaue Festlegung ihres Gegenstands und Umfangs, der Sicherheitsziele, Bewertungskriterien usw. (Artikel 47).

In Titel III werden außerdem die wichtigsten Rechtswirkungen der europäischen Systeme für die Cybersicherheitszertifizierung festgelegt, nämlich i) die Verpflichtung zur Einführung des Systems auf nationaler Ebene und die Freiwilligkeit der Zertifizierung; ii) der Verlust der Gültigkeit nationaler Systeme, wenn es für dieselben Produkte oder Dienste ein europäisches System für die Cybersicherheitszertifizierung gibt (Artikel 48 und 49).

In diesem Titel werden das Verfahren für die Annahme europäischer Systeme für die Cybersicherheitszertifizierung und die jeweilige Rolle der Kommission, der ENISA und der Europäischen Gruppe für die Cybersicherheitszertifizierung (die „Gruppe“) festgelegt (Artikel 44). Ebenfalls in diesem Titel enthalten sind Bestimmungen über die Konformitätsbewertungsstellen, einschließlich der Anforderungen an sie, ihrer Befugnisse und Aufgaben, sowie Bestimmungen über die nationalen Aufsichtsbehörden für die Zertifizierung und Sanktionen.

In diesem Titel wird auch die Gruppe als ein wesentliches Gremium eingesetzt, das sich aus Vertretern der nationalen Aufsichtsbehörden für die Zertifizierung zusammensetzt und deren Hauptfunktion darin besteht, mit der ENISA bei der Ausarbeitung europäischer Systeme für die Cybersicherheitszertifizierung zu kooperieren und die Kommission in allgemeinen und spezifischen Fragen der Politik im Bereich der Cybersicherheitszertifizierung zu beraten.

Titel IV der Verordnung enthält die Schlussbestimmungen, in denen die Ausübung der Befugnisübertragung, die Bewertungsanforderungen, Aufhebung und Rechtsnachfolge sowie das Inkrafttreten geregelt sind.

2017/0225 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION -

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

auf Vorschlag der Europäischen Kommission,

nach Übermittlung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[28],

nach Stellungnahme des Ausschusses der Regionen[29],

nach dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Netz- und Informationssysteme sowie Telekommunikationsnetze und -dienste spielen eine lebenswichtige Rolle für die Gesellschaft und sind mittlerweile zum Hauptmotor des Wirtschaftswachstums geworden. Die Informations- und Kommunikationstechnik bildet das Rückgrat der komplexen Systeme, die gesellschaftliche Tätigkeiten unterstützen und unsere Volkswirtschaften in Schlüsselsektoren wie Gesundheit, Energie, Finanzen und Verkehr aufrechterhalten und die insbesondere dafür sorgen, dass der Binnenmarkt reibungslos funktioniert.

(2) Die Nutzung von Netz- und Informationssystemen durch Bürger, Unternehmen und Behörden ist mittlerweile in der Union allgegenwärtig. Digitalisierung und Konnektivität entwickeln sich zu Kernmerkmalen einer ständig steigenden Zahl von Produkten und Dienstleistungen. Mit dem Aufkommen des Internets der Dinge dürften in den nächsten Jahrzehnten Millionen, wenn nicht Milliarden vernetzte digitale Geräte unionsweit Verbreitung finden. Zwar sind immer mehr Geräte mit dem Internet vernetzt, doch verfügen sie über eine nur unzureichende Cybersicherheit, da die Sicherheit und Abwehrfähigkeit dieser Geräte schon bei der Konzeption nicht ausreichend berücksichtigt wurden. Vor diesem Hintergrund führt die geringe Zertifizierung dazu, dass Personen, die IKT-Produkte und -Dienste für unternehmerische oder private Zwecke nutzen, nur unzureichend über deren Cybersicherheitsmerkmale informiert werden, wodurch das Vertrauen in digitale Lösungen untergraben wird.

[28] ABl. C vom , S. .
[29] ABl. C vom , S. .

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personengruppen wie Kinder ausgesetzt sind. Um dieser Gefahr für die Gesellschaft zu begegnen, gilt es alle für die Erhöhung der Cybersicherheit in der EU notwendigen Maßnahmen zu ergreifen, um die Netz- und Informationssysteme, die Telekommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Privatpersonen, Behörden und Unternehmen – von KMU bis zu Betreibern kritischer Infrastrukturen – genutzt werden, vor Cyberbedrohungen zu schützen.

(4) Cyberangriffe nehmen zu und eine Wirtschaft und Gesellschaft, die durch ihre Vernetzung anfälliger für Cyberbedrohungen und -angriffe ist, benötigt daher einen stärkeren Schutz. Auf die häufig grenzüberschreitenden Cyberangriffe reagieren die für die Cybersicherheit zuständigen Behörden jedoch vor allem mit nationalen Strategien, zumal die Zuständigkeiten für die Strafverfolgung an den nationalen Grenzen enden. Cybersicherheitsvorfälle großen Ausmaßes könnten die Bereitstellung wesentlicher Dienste in der gesamten EU empfindlich stören. Vonnöten sind daher effektive Maßnahmen und ein Krisenmanagement auf EU-Ebene, gestützt auf gezielte Strategien, sowie ein breiter angelegtes Instrumentarium für eine europäische Solidarität und gegenseitige Hilfe. Zudem sind eine auf zuverlässigen Daten der Union basierende regelmäßige Überprüfung des Stands der Cybersicherheit und Abwehrfähigkeit in der Union sowie eine systematische Prognose künftiger Entwicklungen, Herausforderungen und Bedrohungen – sowohl auf Unionsebene als auch auf globaler Ebene – für die Entscheidungsträger, die Branche und die Nutzer daher gleichermaßen wichtig.

(5) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbaut und sich wechselseitig verstärkende Ziele unterstützt. Dies beinhaltet eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Stellen der EU. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die einzelstaatliche Maßnahmen vor allem dann ergänzen könnten, wenn es sich um grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß handelt. Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürgerinnen und Bürger sowie die Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Ferner ließe sich das Vertrauen in den digitalen Binnenmarkt weiter erhöhen, wenn transparente Informationen über das Niveau der Sicherheit von IKT-Produkten und -Diensten zur Verfügung stünden. Erleichtert werden kann dies durch eine Zertifizierung, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

(6) Im Jahr 2004 verabschiedeten das Europäische Parlament und der Rat die Verordnung (EG) Nr. 460/2004 zur Errichtung der ENISA[30] als Beitrag zu den Zielen, innerhalb

[30] Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ABl. L 77 vom 13.3.2004, S. 1).

der Union eine hohe und effektive Netz- und Informationssicherheit zu gewährleisten und eine Kultur der Netz- und Informationssicherheit zu entwickeln, die Bürgern, Verbrauchern, Unternehmen und Behörden zugute kommt. Durch die im Jahr 2008 vom Europäischen Parlament und vom Rat erlassene Verordnung (EG) Nr. 1007/2008[31] wurde das Mandat der Agentur bis März 2012 verlängert. Durch die Verordnung (EG) Nr. 580/2011[32] wurde das Mandat der Agentur nochmals bis zum 13. September 2013 verlängert. Im Jahr 2013 erließen das Europäische Parlament und der Rat die Verordnung (EU) Nr. 526/2013[33] über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004, mit der das Mandat der Agentur bis zum Juni 2020 verlängert wurde.

(7) Europa hat bereits wichtige Maßnahmen ergriffen, um die Cybersicherheit zu gewährleisten und das Vertrauen in die digitale Technik zu stärken. Im Jahr 2013 wurde eine EU-Cybersicherheitsstrategie verabschiedet, die der Union als Orientierung für strategische Reaktionen auf Cybersicherheitsbedrohungen und -risiken dienen soll. Im Zuge ihrer Bemühungen, den Online-Schutz der Europäerinnen und Europäer zu erhöhen, verabschiedete die Union im Jahr 2016 mit der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union den ersten Rechtsakt auf dem Gebiet der Cybersicherheit (im Folgenden die „NIS-Richtlinie“). Mit der NIS-Richtlinie wurden Anforderungen an die nationalen Fähigkeiten im Bereich der Cybersicherheit sowie erstmals Mechanismen zur Stärkung der strategischen und operativen Zusammenarbeit zwischen den Mitgliedstaaten festgelegt sowie Verpflichtungen in Bezug auf die Sicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen für die Sektoren, die für die Wirtschaft und Gesellschaft lebenswichtig sind (Energie, Verkehr, Wasserwirtschaft, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, digitale Infrastrukturen) sowie für Anbieter zentraler digitaler Dienste (Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze) eingeführt. Eine zentrale Aufgabe bei der Umsetzung dieser Richtlinie wurde dabei der ENISA zugewiesen. Darüber hinaus ist die wirksame Bekämpfung der Cyberkriminalität als ein Aspekt bei der Verfolgung des übergeordneten Ziels einer hohen Cybersicherheit ein wichtiger Schwerpunkt der Europäischen Sicherheitsagenda.

(8) Seit der Verabschiedung der EU-Cybersicherheitsstrategie im Jahr 2013 und der letzten Überarbeitung des Mandats der Agentur hat sich der gesamtpolitische Rahmen deutlich verändert, auch in Bezug auf die größeren Unwägbarkeiten und die geringere Sicherheit im globalen Umfeld. Vor diesem Hintergrund und angesichts der neuen Unionspolitik im Bereich der Cybersicherheit muss das Mandat der ENISA im Hinblick auf ihre neue Rolle in dem veränderten Cybersicherheitsökosystem überarbeitet werden, damit sie die Union wirksam darin unterstützen kann, auf die

---

31 Verordnung (EG) Nr. 1007/2008 des Europäischen Parlaments und des Rates vom 24. September 2008 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer (ABl. L 293 vom 31.10.2008, S. 1).

32 Verordnung (EG) Nr. 580/2011 des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer (ABl. L 165 vom 24.6.2011, S. 3).

33 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).

Herausforderungen im Bereich der Cybersicherheit zu reagieren, die sich aus dieser grundlegend veränderten Bedrohungslandschaft ergeben und für die, wie in der Bewertung der Agentur bestätigt, das laufende Mandat nicht ausreicht.

(9) Die mit dieser Verordnung errichtete Agentur sollte Rechtsnachfolgerin der durch die Verordnung (EG) Nr. 526/2013 errichteten ENISA sein. Die Agentur sollte die Aufgaben wahrnehmen, die ihr mit dieser Verordnung und den Rechtsakten der Union im Bereich der Cybersicherheit übertragen werden, indem sie unter anderem Sachkenntnis bereitstellt, Beratung bietet und die Rolle eines Informations- und Wissenszentrums der Union übernimmt. Sie sollte den Austausch bewährter Verfahren zwischen den Mitgliedstaaten und privaten Interessenträgern fördern, der Europäischen Kommission und den Mitgliedstaaten strategische Vorschläge unterbreiten, als Bezugspunkt für sektorspezifische politische Initiativen der Union im Bereich der Cybersicherheit dienen und die operative Zusammenarbeit zwischen den Mitgliedstaaten sowie zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU fördern.

(10) Mit dem Beschluss 2004/97/EG, Euratom, der auf der Tagung des Europäischen Rates vom 13. Dezember 2003 angenommen wurde, legten die Vertreter der Mitgliedstaaten fest, dass die ENISA ihren Sitz in Griechenland in einer von der griechischen Regierung zu bestimmenden Stadt haben soll. Der Sitzmitgliedstaat der Agentur sollte die bestmöglichen Voraussetzungen für eine reibungslose und effiziente Tätigkeit der Agentur gewährleisten. Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient erfüllen, Personal einstellen und binden und die Effizienz der Vernetzungsmaßnahmen steigern kann, ist es unbedingt erforderlich, sie an einem geeigneten Standort anzusiedeln, der unter anderem eine angemessene Verkehrsanbindung sowie Einrichtungen für die Ehepartner und Kinder des Personals der Agentur bietet. Die erforderlichen Modalitäten sollten in einem Abkommen zwischen der Agentur und dem Sitzmitgliedstaat festgelegt werden, das nach Billigung durch den Verwaltungsrat der Agentur geschlossen wird.

(11) Angesichts der zunehmenden Herausforderungen, mit denen die Union im Bereich der Cybersicherheit konfrontiert ist, sollten die Mittelzuweisungen für die Agentur erhöht werden, damit ihre finanzielle und personelle Ausstattung ihrer größeren Rolle und ihren umfangreicheren Aufgaben sowie ihrer wichtigen Stellung im Kreise der Organisationen gerecht werden kann, die das digitale Ökosystem der EU verteidigen.

(12) Die Agentur sollte ein hohes Niveau an Sachkenntnis entwickeln und pflegen und durch ihre Unabhängigkeit, die Qualität ihrer Beratung und der von ihr verbreiteten Informationen, die Transparenz ihrer Verfahren und Arbeitsmethoden sowie die Sorgfalt, mit der sie ihre Aufgaben erfüllt, als Bezugspunkt Vertrauen in den Binnenmarkt schaffen. Die Agentur sollte die Bemühungen der Mitgliedstaaten und der Union proaktiv unterstützen und ihre Aufgaben in uneingeschränkter Zusammenarbeit mit den Organen, Einrichtungen und sonstigen Stellen der Union und den Mitgliedstaaten wahrnehmen. Außerdem sollte sich die Agentur auf die Beiträge des Privatsektors sowie auf die Zusammenarbeit mit diesem und anderen einschlägigen Interessenträgern stützen. Mit einer Reihe von Aufgaben sollte bei gleichzeitiger Wahrung der Flexibilität in ihrer Tätigkeit vorgegeben werden, wie die Agentur ihre Ziele erreichen soll.

(13) Die Agentur sollte die Kommission, auch in Bezug auf den Schutz kritischer Infrastrukturen und die Fähigkeit zur Abwehr von Cyberangriffen, mit Beratung, Stellungnahmen und Analysen zu allen Angelegenheiten der Union, die mit der

Ausarbeitung, Aktualisierung und Überprüfung von Strategien und Rechtsvorschriften im Bereich der Cybersicherheit zusammenhängen, unterstützen. Für sektorspezifische Strategien und Rechtsetzungsinitiativen der Union im Zusammenhang mit der Cybersicherheit sollte die Agentur als Bezugspunkt für Beratung und Sachkenntnis dienen.

(14) Die Agentur hat grundsätzlich die Aufgabe, die einheitliche Umsetzung des einschlägigen Rechtsrahmens, vor allem die wirksame Umsetzung der NIS-Richtlinie, zu unterstützen, was für die Stärkung der Abwehrfähigkeit gegen Cyberangriffe unerlässlich ist. Angesichts der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit müssen die Mitgliedstaaten beim Aufbau der Abwehrfähigkeit gegen Cyberangriffe natürlich mit einem umfassenderen und ressortübergreifenden Konzept unterstützt werden.

(15) Die Agentur sollte die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten in ihrem Bemühen um den Auf- und Ausbau der Fähigkeiten und der Bereitschaft zur Verhütung, Erkennung und Bewältigung von Cybersicherheitsproblemen und von Sicherheitsvorfällen im Zusammenhang mit der Netz- und Informationssicherheit unterstützen. So sollte die Agentur den Auf- und Ausbau der nationalen CSIRTs unterstützen, damit sie ein unionsweit hohes Maß an Ausgereiftheit erreichen. Zudem sollte die Agentur die Ausarbeitung und Aktualisierung von Strategien der Union und der Mitgliedstaaten im Bereich der Netz- und Informationssysteme, insbesondere der Cybersicherheit, unterstützen, deren Verbreitung fördern und deren Umsetzung verfolgen. Die Agentur sollte öffentlichen Stellen auch Ausbildungsmaßnahmen und Ausbildungsmaterial anbieten und gegebenenfalls Ausbilder weiterbilden, um die Mitgliedstaaten darin zu unterstützen, eigene Ausbildungskapazitäten aufzubauen.

(16) Die Agentur sollte die auf der Grundlage der NIS-Richtlinie eingesetzte Kooperationsgruppe bei der Wahrnehmung ihrer Aufgaben unterstützen, indem sie vor allem ihre Sachkenntnis und Beratung zur Verfügung stellt und den Austausch bewährter Verfahren erleichtert, insbesondere was die Ermittlung von Betreibern wesentlicher Dienste durch die Mitgliedstaaten in Bezug auf Risiken und Sicherheitsvorfälle anbelangt, auch mit Blick auf grenzüberschreitende Abhängigkeiten.

(17) Die Agentur sollte als Anreiz für die Zusammenarbeit zwischen dem öffentlichen und privaten Sektor, vor allem als Beitrag zum Schutz kritischer Infrastrukturen, den Aufbau sektorbezogener Informationsaustausch- und -analysezentren (*Information Sharing and Analysis Centres* – ISACs) erleichtern, indem sie bewährte Verfahren und Leitfäden zu den vorhandenen Werkzeugen und Verfahren zur Verfügung stellt und aufzeigt, wie regulatorische Fragen im Zusammenhang mit der Informationsweitergabe geklärt werden können.

(18) Die Agentur sollte die nationalen Berichte der CSIRTs und des CERT-EU zusammenstellen und auswerten und darüber hinaus für den Informationsaustausch gemeinsame Regeln aufstellen, die Sprache festlegen und terminologische Vereinbarungen treffen. Im Rahmen der NIS-Richtlinie, die mit der Errichtung des CSIRTs-Netzes die Grundlage für den freiwilligen Austausch technischer Informationen auf operativer Ebene geschaffen hat, sollte die Agentur auch den Privatsektor einbeziehen.

(19) Die Agentur sollte dazu beitragen, dass bei massiven grenzüberschreitenden Cybersicherheitsvorfällen und -krisen eine Reaktion auf EU-Ebene erfolgt. Hierzu

sollte sie u. a. relevante Informationen zusammenstellen und den Kontakt zwischen dem CSIRTs-Netz und den Fachkreisen sowie den für das Krisenmanagement zuständigen Entscheidungsträgern erleichtern. Zudem könnte die Agentur die Bewältigung von Sicherheitsvorfällen aus technischer Sicht unterstützen, indem sie den Austausch entsprechender technischer Lösungen zwischen den Mitgliedstaaten erleichtert und Beiträge für die Öffentlichkeitsarbeit liefert. Die Agentur sollte den Prozess unterstützen, indem sie die Modalitäten einer solchen Zusammenarbeit im Rahmen jährlich stattfindender Cybersicherheitsübungen testet.

(20) Für ihre operativen Aufgaben sollte die Agentur im Wege einer strukturierten Zusammenarbeit in räumlicher Nähe auf den bei der CERT-EU vorhandenen Sachverstand zurückgreifen. Die strukturierte Zusammenarbeit erleichtert die notwendigen Synergien und den Aufbau von Sachkenntnis bei der ENISA. Für die Festlegung der praktischen Aspekte einer solchen Kooperation sollten zwischen den beiden Organisationen die hierfür notwendigen Modalitäten festgelegt werden.

(21) Entsprechend ihren operativen Aufgaben sollte die Agentur in der Lage sein, die Mitgliedstaaten beispielsweise mit Rat, technischer Hilfe oder Analysen von Bedrohungen und Sicherheitsvorfällen zu unterstützen. Der Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen zufolge sollten die Mitgliedstaaten in gutem Glauben untereinander sowie mit der ENISA Informationen über massive Cybersicherheitsvorfälle und -krisen unverzüglich austauschen. Diese Informationen dürften zudem der ENISA helfen, ihre operativen Aufgaben wahrzunehmen.

(22) Als Teil der regulären Zusammenarbeit auf technischer Ebene zur Unterstützung der EU-Lageeinschätzung sollte die Agentur auf der Grundlage öffentlich verfügbarer Informationen, ihrer eigenen Analysen und anhand von Berichten, die sie (auf freiwilliger Basis) von den CSIRTs der Mitgliedstaaten oder den zentralen Anlaufstellen gemäß der NIS-Richtlinie, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol und dem CERT-EU sowie gegebenenfalls dem EU-Zentrum für Informationsgewinnung und -analyse (INTCEN) des Europäischen Auswärtigen Dienstes (EAD) erhalten hat, regelmäßig den EU-Cybersicherheitslagebericht über Cybervorfälle und -bedrohungen erstellen. Der Bericht sollte den einschlägigen Stellen des Rates, der Kommission, der Hohen Vertreterin der Union für die Gemeinsame Außen- und Sicherheitspolitik und dem CSIRTs-Netz zur Verfügung gestellt werden.

(23) Nachträgliche technische Untersuchungen von Sicherheitsvorfällen mit beträchtlichen Auswirkungen in mehreren Mitgliedstaaten, die die Agentur auf Ersuchen der betreffenden Mitgliedstaaten oder im Einvernehmen mit diesen durchführt, sollten sich auf die Verhütung künftiger Sicherheitsvorfälle konzentrieren und unbeschadet jeglicher juristischer oder administrativer Verfahren zur Klärung der Schuld- oder Haftungsfrage durchgeführt werden.

(24) Unbeschadet des Artikels 346 des Vertrags über die Arbeitsweise der Europäischen Union oder anderer politischer Gründe sollten die betreffenden Mitgliedstaaten der Agentur die für die Zwecke der Untersuchung notwendigen Informationen und Hilfen zur Verfügung stellen.

(25) Die Mitgliedstaaten können die von dem Sicherheitsvorfall betroffenen Unternehmen auffordern, mit der Agentur zusammenzuarbeiten und dieser unbeschadet ihres Rechts, sensible Geschäftsinformationen zu schützen, die notwendigen Informationen und Hilfen zur Verfügung stellen.

(26) Um die Herausforderungen im Bereich der Cybersicherheit besser verstehen und den Mitgliedstaaten und EU-Organen langfristige strategische Beratung anbieten zu können, muss die Agentur aktuelle und neu auftretende Risiken analysieren. Hierzu sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und gegebenenfalls Statistikämtern und anderen Stellen einschlägige Informationen sammeln und Analysen neu entstehender Technik sowie themenspezifische Bewertungen dazu durchführen, welche gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Folgen technische Innovationen auf die Netz- und Informationssicherheit, insbesondere die Cybersicherheit, haben. Die Agentur sollte die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der EU darüber hinaus bei der Ermittlung sich abzeichnender Trends und bei der Vermeidung von Problemen im Zusammenhang mit der Cybersicherheit unterstützen, indem sie Analysen der Bedrohungen und Sicherheitsvorfälle durchführt.

(27) Um die Abwehrfähigkeit der Union zu stärken, sollte die Agentur Spitzenkompetenzen im Bereich der Sicherheit der Internetinfrastruktur und kritischer Infrastrukturen aufbauen, um so Beratung, Leitlinien und bewährte Verfahren zur Verfügung stellen zu können. Um den Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen zu erleichtern, sollte die Agentur das Informationsportal der Union aufbauen und pflegen, über das der Öffentlichkeit Informationen der Organe, Einrichtungen und sonstigen Stellen der EU und der Mitgliedstaaten zur Cybersicherheit gegeben werden.

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für potenzielle Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf Authentifizierung und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren.

(29) Um die im Cybersicherheitssektor tätigen Unternehmen und die Nutzer von Cybersicherheitslösungen zu unterstützen, sollte die Agentur eine „Marktbeobachtungsstelle“ aufbauen und pflegen, die die wichtigsten Nachfrage- und Angebotstrends auf dem Cybersicherheitsmarkt regelmäßig analysiert und bekannt macht.

(30) Damit die Agentur ihre Ziele in vollem Umfang verwirklichen kann, sollte sie zu den einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU Kontakt halten – etwa zum CERT-EU, zum Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol, zur Europäischen Verteidigungsagentur (EDA), zur Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA), zur Europäischen Agentur für Flugsicherheit (EASA) und zu sonstigen EU-

Agenturen, die sich mit Fragen der Cybersicherheit beschäftigen. Für den Austausch von Know-how und bewährten Verfahren und für die Beratung zu Aspekten der Cybersicherheit, die sich auf die Arbeit von Datenschutzbehörden auswirken können, sollte die Agentur auch mit diesen in Verbindung stehen. Vertreter der Strafverfolgungs- und der Datenschutzbehörden auf nationaler Ebene und auf Unionsebene sollten als Vertreter für eine Mitwirkung in der Ständigen Gruppe der Interessenträger der Agentur in Frage kommen. Bei ihren Kontakten mit Strafverfolgungsbehörden in Bezug auf Netz- und Informationssicherheitsaspekte, die sich möglicherweise auf deren Arbeit auswirken, sollte die Agentur vorhandene Informationskanäle und bestehende Netze beachten.

(31) Als Mitglied des CSIRTs-Netzes sollte die Agentur, die zudem das Sekretariat des Netzes stellt, über die in der NIS-Richtlinie festgelegten einschlägigen Aufgaben hinaus die CSIRTs der Mitgliedstaaten und das CERT-EU bei der operativen Zusammenarbeit unterstützen. Zudem sollte sie unter gebührender Berücksichtigung der Standardbetriebsverfahren des CSIRTs-Netzes die Zusammenarbeit zwischen den jeweiligen CSIRTs bei Sicherheitsvorfällen, Angriffen oder Störungen der von den CSIRTs verwalteten oder geschützten Netze oder Infrastrukturen, die mindestens zwei CERTs betreffen oder betreffen können, fördern und unterstützen.

(32) Zur Erhöhung der Abwehrbereitschaft der Union bei Cybersicherheitsvorfällen sollte die Agentur auf Unionsebene jährliche Cybersicherheitsübungen organisieren und die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der EU auf deren Ersuchen hin bei der Organisation solcher Übungen unterstützen.

(33) Die Agentur sollte ihre Sachkenntnis im Bereich der Cybersicherheitszertifizierung weiter ausbauen und pflegen, damit sie die Unionspolitik auf diesem Gebiet unterstützen kann. Die Agentur sollte die Nutzung der Cybersicherheitszertifizierung in der Union fördern, auch indem sie zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens auf Unionsebene beiträgt, um so die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten und -Diensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt zu stärken.

(34) Effiziente Cybersicherheitsstrategien sollten sowohl im öffentlichen als auch im privaten Sektor auf sorgfältig entwickelten Risikobewertungsmethoden beruhen. Risikobewertungsmethoden werden auf verschiedenen Ebenen angewandt, ohne dass es eine einheitliche Vorgehensweise für deren effiziente Anwendung gibt. Durch die Förderung und Entwicklung bewährter Verfahren für die Risikobewertung und interoperabler Lösungen für das Risikomanagement innerhalb von Organisationen des öffentlichen und des privaten Sektors wird das Niveau der Cybersicherheit in der Union erhöht. Zu diesem Zweck sollte die Agentur die Zusammenarbeit zwischen Interessenträgern auf Unionsebene unterstützen und Hilfestellung bei deren Bemühungen um die Festlegung und Einführung von europäischen und internationalen Normen für das Risikomanagement und eine messbare Sicherheit in Bezug auf elektronische Produkte, Systeme, Netze und Dienste leisten, die im Zusammenwirken mit Software die Netz- und Informationssysteme bilden.

(35) Die Agentur sollte die Mitgliedstaaten und die Diensteanbieter dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche Cybersicherheit treffen können. So sollten Diensteanbieter und Produkthersteller diese Dienste und Produkte vom Markt nehmen oder umrüsten, wenn sie den Cybersicherheitsstandards nicht genügen. In

Zusammenarbeit mit den zuständigen Behörden kann die ENISA Informationen über das Niveau der Cybersicherheit von Produkten und Diensten verbreiten, die auf dem Binnenmarkt angeboten werden, Anbieter und Hersteller verwarnen und sie auffordern, die Sicherheit, auch die Cybersicherheit, ihrer Produkte und Dienste zu verbessern.

(36) Die Agentur sollte die laufenden Tätigkeiten auf den Gebieten der Forschung, Entwicklung und technologischen Bewertung – insbesondere die im Rahmen der vielfältigen Forschungsinitiativen der Union durchgeführten Tätigkeiten – umfassend berücksichtigen, um die Organe, Einrichtungen und sonstigen Stellen der Union sowie gegebenenfalls die Mitgliedstaaten – auf deren Ersuchen – in Bezug auf den Forschungsbedarf im Bereich der Netz- und Informationssicherheit, insbesondere der Cybersicherheit, zu beraten.

(37) Die Probleme der Cybersicherheit stellen sich weltweit. Um die Sicherheitsstandards, einschließlich der Festlegung gemeinsamer Verhaltensnormen, und den Informationsaustausch zu verbessern sowie eine zügigere internationale Zusammenarbeit bei der Abwehr und einen weltweiten gemeinsamen Ansatz für Probleme der Netz- und Informationssicherheit zu fördern, bedarf es einer engeren internationalen Zusammenarbeit. In dieser Hinsicht sollte die Agentur ein stärkeres Engagement der Union und die Zusammenarbeit mit Drittländern und internationalen Organisationen unterstützen, indem sie den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union gegebenenfalls die erforderlichen Sachkenntnisse und Analysen zur Verfügung stellt.

(38) Die Agentur sollte in der Lage sein, auf Anfragen der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der EU, die von den Zielen der Agentur abgedeckt sind, ad hoc mit Rat und Hilfestellung zu reagieren.

(39) In Bezug auf die Führung der Agentur müssen bestimmte Grundsätze umgesetzt werden, um der Gemeinsamen Erklärung und dem Gemeinsamen Konzept zu entsprechen, die von der Interinstitutionellen Arbeitsgruppe zu den dezentralen Einrichtungen der EU im Juli 2012 vereinbart wurden und deren Zweck darin besteht, die Aktivitäten der Agenturen dynamischer zu gestalten und ihre Leistung zu verbessern. Die Gemeinsame Erklärung und das Gemeinsame Konzept sollten, soweit angemessen, in den Arbeitsprogrammen, den Bewertungen und den Berichterstattungs- und Verwaltungsverfahren der Agentur zur Geltung kommen.

(40) Der Verwaltungsrat, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzt, sollte die allgemeine Ausrichtung der Tätigkeit der Agentur festlegen und dafür sorgen, dass sie ihre Aufgaben im Einklang mit dieser Verordnung wahrnimmt. Der Verwaltungsrat sollte über die erforderlichen Befugnisse verfügen, um den Haushaltsplan zu erstellen und dessen Ausführung zu überprüfen, angemessene Finanzvorschriften und transparente Verfahren für die Entscheidungsfindung der Agentur festzulegen, das einheitliche Programmplanungsdokument der Agentur anzunehmen, sich eine Geschäftsordnung zu geben, den Exekutivdirektor zu ernennen und über die Verlängerung sowie die Beendigung der Amtszeit des Exekutivdirektors zu beschließen.

(41) Damit die Agentur ihre 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 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.

(42) Damit die Agentur reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird, über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt und seine Aufgaben völlig unabhängig wahrnimmt. Der Exekutivdirektor sollte nach Anhörung der Kommission einen Vorschlag für das Arbeitsprogramm der Agentur ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Der Exekutivdirektor sollte einen Jahresbericht ausarbeiten, der dem Verwaltungsrat vorgelegt wird, den Entwurf eines Voranschlags für die Einnahmen und Ausgaben der Agentur erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder wirtschaftlichen Einzelfragen befassen. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen und dass je nach Einzelfrage gegebenenfalls ein repräsentatives Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit gewahrt wird.

(43) Der Exekutivrat sollte dazu beitragen, dass der Verwaltungsrat effektiv arbeiten kann. Im Rahmen seiner vorbereitenden Arbeiten für die Beschlüsse des Verwaltungsrats sollte er die einschlägigen Informationen im Detail prüfen und die sich bietenden Optionen sondieren, zudem sollte er die einschlägigen Beschlüsse des Verwaltungsrats vorbereiten, indem er Beratung und Lösungen anbietet.

(44) Die Agentur sollte über eine Ständige Gruppe der Interessenträger als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, Verbraucherorganisationen und sonstigen Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte Ständige Gruppe der Interessenträger sollte hauptsächlich Fragen behandeln, die die Beteiligten betreffen, und diese der Agentur zur Kenntnis bringen. Die Zusammensetzung der Ständigen Gruppe der Interessenträger und die dieser Gruppe übertragenen Aufgaben, die vor allem aus dem Entwurf des Arbeitsprogramms hervorgehen, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der Agentur ausreichend vertreten sind.

(45) Die Agentur sollte Vorschriften zur Vermeidung und Handhabung von Interessenkonflikten haben. Die Agentur sollte die einschlägigen Bestimmungen der Union in Bezug auf den Zugang der Öffentlichkeit zu Dokumenten gemäß der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates[34] anwenden. Die Verarbeitung personenbezogener Daten durch die Agentur sollte nach der 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[35] erfolgen. Die Agentur sollte die für die Unionsorgane

[34] 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).

[35] ABl. L 8 vom 12.1.2001, S. 1.

geltenden Bestimmungen über den Umgang mit Informationen, insbesondere mit sensiblen Informationen und Verschlusssachen der EU, sowie die entsprechenden einzelstaatlichen Rechtsvorschriften befolgen.

(46) Damit die volle Autonomie und Unabhängigkeit der Agentur gewährleistet ist und sie zusätzliche und neue Aufgaben – auch nicht vorhergesehene Aufgaben in Notfällen – erfüllen kann, sollte die Agentur über einen ausreichenden und eigenständigen Haushalt verfügen, der hauptsächlich durch einen Beitrag der Union und durch Beiträge von Drittländern, die sich an der Arbeit der Agentur beteiligen, finanziert wird. Die Mehrheit der Agenturbediensteten sollte unmittelbar mit der operativen Umsetzung des Mandats der Agentur befasst sein. Dem Sitzmitgliedstaat und anderen Mitgliedstaaten sollte es erlaubt sein, freiwillige Beiträge zu den Einnahmen der Agentur zu leisten. Sämtliche Zuschüsse aus dem Gesamthaushaltsplan der Europäischen Union sollten dem Haushaltsverfahren der Union unterliegen. Ferner sollte die Rechnungsführung der Agentur durch den Rechnungshof geprüft werden, um Transparenz und Rechenschaftspflicht sicherzustellen.

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter Zertifizierung eine Art der Konformitätsbewertung zu verstehen, die sich auf die Cybersicherheitsmerkmale eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht („IKT-Produkte und -Dienste“) und die von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt, durchgeführt wird. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass diese die Kriterien der Cybersicherheit erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die IKT-Produkte und -Dienste geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte Anforderungen an die Cybersicherheit erfüllen.

(48) Die Cybersicherheitszertifizierung spielt eine große Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte und -Dienste zu stärken und deren Sicherheit zu erhöhen. Die Entwicklung des digitalen Binnenmarkts und insbesondere der Datenwirtschaft und des Internets der Dinge kommt nur voran, wenn in der breiten Öffentlichkeit das Vertrauen vorhanden ist, dass diese Produkte und Dienste ein gewisses Maß an Cybersicherheit gewährleisten. Vernetzte und automatisierte Fahrzeuge, elektronische medizinische Geräte, die automatischen Steuerungssysteme der Industrie oder intelligente Netze sind, um nur einige Beispiele zu nennen, Sektoren, in denen die Zertifizierung bereits breiten Einsatz findet oder in naher Zukunft eingesetzt werden soll. Die unter die NIS-Richtlinie fallenden Sektoren sind zudem Sektoren, in denen die Cybersicherheitszertifizierung ein maßgeblicher Faktor ist.

(49) In ihrer Mitteilung aus dem Jahr 2016 „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche“ unterstrich die Kommission die Notwendigkeit hochwertiger, erschwinglicher und interoperabler Produkte und Lösungen für die Cybersicherheit. Allerdings ist das Angebot an IKT-Produkten und -diensten im Binnenmarkt nach wie vor geografisch stark zersplittert. Das liegt daran, dass sich die Cybersicherheitsbranche in Europa überwiegend aufgrund der Nachfrage der nationalen Regierungen entwickelt hat. Zudem gehört der Mangel an interoperablen Lösungen (technischen Normen), Verfahrensweisen und EU-weiten Zertifizierungsmechanismen zu den Defiziten, die den Binnenmarkt im Bereich der

Cybersicherheit beeinträchtigen. Dies macht es zum einen für europäische Unternehmen schwerer, im nationalen, europäischen und weltweiten Wettbewerb zu bestehen. Zum anderen verringert sich dadurch das Angebot an tragfähiger und einsetzbarer Cybersicherheitstechnik, auf die Privatpersonen und Unternehmen zugreifen könnten. Auch in der Halbzeitbewertung der Umsetzung der Strategie für den digitalen Binnenmarkt unterstrich die Kommission die Bedeutung sicherer vernetzter Produkte und Systeme und verwies darauf, dass die Schaffung eines europäischen Rahmens für die IKT-Sicherheit, auf dessen Grundlage Vorschriften für die Organisation der IKT-Sicherheitszertifizierung in der Union festgelegt werden, dafür sorgen kann, dass das Vertrauen in den Binnenmarkt erhalten bleibt und die derzeitige Fragmentierung des Cybersicherheitsmarkts eingedämmt wird.

(50) Derzeit werden IKT-Produkte und -Dienste im Hinblick auf ihre Cybersicherheit kaum zertifiziert, und wenn doch, geschieht dies meist auf Ebene der Mitgliedstaaten oder im Rahmen brancheneigener Programme. So wird ein von einer nationalen Cybersicherheitsbehörde ausgestelltes Zertifikat nicht grundsätzlich auch von anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre Produkte und Dienste möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen. Auch wenn immer neue Systeme entstehen, scheint es kein kohärentes und ganzheitliches Konzept zu geben, das sich mit horizontalen Fragen der Cybersicherheit, etwa im Bereich des Internets der Dinge, befasst. Die vorhandenen Systeme weisen im Hinblick auf Produkterfassung, Vertrauenswürdigkeitsstufen, wesentliche Kriterien und tatsächliche Nutzung erhebliche Mängel und Unterschiede auf.

(51) In der Vergangenheit wurden bereits einige Anstrengungen unternommen, um zu einer gegenseitigen Anerkennung der Zertifikate in Europa zu gelangen. Diese waren jedoch nur zum Teil erfolgreich. Das in dieser Hinsicht wichtigste Beispiel ist die in der Gruppe hoher Beamter für die Sicherheit der Informationssysteme (SOG-IS) getroffene Vereinbarung über die gegenseitige Anerkennung (MRA). Auch wenn diese Vereinbarung das wichtigste Vorbild für die Zusammenarbeit und gegenseitige Anerkennung auf dem Gebiet der Sicherheitszertifizierung ist, hat sie doch einige erhebliche Mängel, was die hohen Kosten und den begrenzten Anwendungsbereich anbelangt. Bislang wurden nur wenige Schutzprofile für digitale Produkte entwickelt – beispielsweise für die digitale Signatur, den digitalen Fahrtenschreiber und intelligente Chipkarten. Was jedoch noch schwerer ins Gewicht fällt, ist die Tatsache, dass die Gruppe nur einen Teil der EU-Mitgliedstaaten umfasst. Dies hat aus Binnenmarktsicht zur Folge, dass die Vereinbarungen der Gruppe nur begrenzt wirksam sind.

(52) Vor diesem Hintergrund gilt es, einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen an die zu entwickelnden europäischen Systeme zur Zertifizierung der Cybersicherheit festgelegt werden, damit die Zertifikate für die IKT-Produkte und -Dienste in allen Mitgliedstaaten anerkannt und verwendet werden können. Mit einem europäischen Rahmen werden zwei Ziele verfolgt: einerseits dürfte er dazu beitragen, das Vertrauen in IKT-Produkte und -Dienste zu erhöhen, die nach solchen Systemen zertifiziert wurden, und andererseits dürften sich so vielfältige, sich widersprechende oder überlappende nationale System für die Cybersicherheitszertifizierung vermeiden lassen, was die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senkt. Die Systeme sollten nichtdiskriminierend sein und sich auf internationale bzw. europäische Normen stützen, sofern diese Normen nicht unwirksam oder

unangemessen im Hinblick auf die Erreichung der legitimen Ziele der EU in diesem Bereich sind.

(53) Die Kommission sollte befugt sein, für bestimmte Gruppen von IKT-Produkten und -Diensten europäische Systeme für die Cybersicherheitszertifizierung anzunehmen. Diese Systeme sollten von nationalen Aufsichtsbehörden für die Zertifizierung umgesetzt und überwacht werden, und die im Rahmen dieser Systeme erteilten Zertifikate sollten unionsweit gültig sein und anerkannt werden. Die von der Industrie oder sonstigen privaten Organisationen betriebenen Zertifizierungssysteme fallen nicht in den Anwendungsbereich dieser Verordnung. Die Stellen, die solche Systeme betreiben, können der Kommission jedoch vorschlagen, ihre Systeme als Grundlage für ein europäisches System in Betracht zu ziehen und sie als ein solches zu genehmigen.

(54) Das Unionsrecht, in dem bestimmte Vorschriften zur Zertifizierung von IKT-Produkten und -Diensten festgelegt sind, bleibt von den Bestimmungen dieser Verordnung unberührt. So enthält die Datenschutz-Grundverordnung Festlegungen für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen, die dem Nachweis dienen, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Verarbeitung von Daten die Bestimmungen der Verordnung einhalten. Solche Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen sollten den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen. Die Zertifizierung von Datenverarbeitungsvorgängen, die unter die Datenschutz-Grundverordnung fallen, auch wenn solche Vorgänge in Produkte und Dienste eingebettet sind, bleibt von dieser Verordnung unberührt.

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen.

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen.

Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „niedrig“, „mittel“ bzw. „hoch“.

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

(58) Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet worden ist, sollten Hersteller von IKT-Produkten und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte oder Dienste bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine Höchstdauer von fünf Jahren erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt werden oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

(59) Es ist notwendig, alle Mitgliedstaaten zur Benennung einer Aufsichtsbehörde für die Cybersicherheitszertifizierung zu verpflichten, die die in ihrem Hoheitsgebiet ansässigen Konformitätsbewertungsstellen und die von diesen ausgestellten Zertifikate im Hinblick auf die Einhaltung der Anforderungen beaufsichtigt, die in dieser Verordnung und in den jeweiligen Cybersicherheitszertifizierungssystemen festgelegt sind. Die nationalen Aufsichtsbehörden für die Zertifizierung sollten Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf die von Konformitätsbewertungsstellen in ihrem Hoheitsgebiet ausgestellten Zertifikate eingereicht werden, bearbeiten, den Beschwerdegegenstand, soweit angemessen, untersuchen und den Beschwerdeführer über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist unterrichten. Darüber hinaus sollten sie mit anderen nationalen Aufsichtsbehörden für die Zertifizierung und anderen öffentlichen Stellen zusammenarbeiten, auch indem sie Informationen über die etwaige Nichtkonformität von IKT-Produkten und -Diensten mit den Anforderungen dieser Verordnung oder bestimmten europäischen Systemen für die Cybersicherheitszertifizierung austauschen.

(60) Für eine einheitliche Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung sollte eine europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) eingesetzt werden, die sich aus den nationalen Aufsichtsbehörden für die Zertifizierung zusammensetzt. Die Gruppe sollte vor allem die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung beraten und unterstützen, die Agentur bei der Ausarbeitung der möglichen Cybersicherheitszertifizierungssysteme unterstützen und mit ihr eng zusammenarbeiten, der Kommission empfehlen, die Agentur mit der Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung zu beauftragen sowie an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung vorhandener europäischer Systeme für die Cybersicherheitszertifizierung abzugeben.

(61) Zur Sensibilisierung und um die Akzeptanz künftiger EU-Cybersicherheitssysteme zu erhöhen, kann die Europäische Kommission allgemeine und sektorspezifische Cybersicherheitsleitlinien herausgeben, die sich beispielsweise auf bewährte Verfahren oder verantwortungsvolles Verhalten im Bereich der Cybersicherheit beziehen, und dabei die Vorteile der Verwendung zertifizierter IKT-Produkte und -Dienste hervorheben.

(62) Die Agentur sollte zur Unterstützung der Cybersicherheitszertifizierung bei der kryptografischen Genehmigung von Produkten, die in Netzen für Verschlusssachen verwendet werden, auch in Kontakt mit dem Sicherheitsausschuss des Rates und den einschlägigen nationalen Gremien stehen.

(63) Um die Kriterien für die Akkreditierung von Konformitätsbewertungsstellen genauer festzulegen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Rechtsakte zu erlassen. Die Kommission sollte im Rahmen ihrer Vorarbeiten – auch auf Sachverständigenebene – geeignete Konsultationen durchführen. Diese Konsultationen sollten im Einklang mit den Grundsätzen durchgeführt werden, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über die bessere Rechtsetzung niedergelegt wurden. Um insbesondere eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, sollten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten erhalten, und ihre Sachverständigen sollten systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission haben, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(64) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden, wenn dies in dieser Verordnung vorgesehen ist. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden.

(65) Die Durchführungsrechtsakte über die europäischen Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten, die Modalitäten für die Durchführung von Umfragen durch die Agentur sowie die Umstände, Formate und Verfahren der Notifizierung akkreditierter Konformitätsbewertungsstellen durch die nationalen Aufsichtsbehörden für die Zertifizierung bei der Kommission sollten nach dem Prüfverfahren erlassen werden.

(66) Die Tätigkeit der Agentur sollte unabhängig bewertet werden. Die Bewertung sollte sich darauf beziehen, inwieweit die Agentur ihre Ziele erreicht, wie sie arbeitet und inwieweit ihre Aufgaben relevant sind. Zudem sollten Wirkung, Wirksamkeit und Effizienz des europäischen Rahmens für Cybersicherheitszertifizierung bewertet werden.

(67) Die Verordnung (EG) Nr. 526/2013 sollte aufgehoben werden.

(68) Da die Ziele dieser Verordnung von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr auf Unionsebene besser zu verwirklichen sind, kann die Union im 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 Verordnung nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus –

HABEN FOLGENDE VERORDNUNG ERLASSEN:

TITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand und Geltungsbereich

Um das ordnungsgemäße Funktionieren des Binnenmarkts zu gewährleisten und um gleichzeitig in der Union ein hohes Niveau in der Cybersicherheit, bei der Fähigkeit zur Abwehr gegen Cyberangriffe und beim Vertrauen in die Cybersicherheit zu erreichen, wird in dieser Verordnung Folgendes festgelegt:

(a) die Ziele, Aufgaben und organisatorischen Aspekte der „EU-Cybersicherheitsagentur“ (ENISA), im Folgenden die „Agentur“ und

(b) ein Rahmen für die Festlegung europäischer Zertifizierungssysteme für die Cybersicherheit, mit dem für IKT-Produkte und Dienste in der Union ein angemessenes Maß an Cybersicherheit gewährleistet werden soll. Dieser Rahmen gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine freiwillige oder verbindliche Zertifizierung.

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:

(1) „Cybersicherheit“ umfasst alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, deren Nutzer und betroffene Personen vor Cyberbedrohungen zu schützen;

(2) „Netz- und Informationssystem“ bezeichnet ein System im Sinne von Artikel 4 Nummer 1 der Richtlinie (EU) 2016/1148;

(3) „nationale Strategie für die Sicherheit von Netz- und Informationssystemen“ bezeichnet einen Rahmen im Sinne von Artikel 4 Nummer 3 der Richtlinie (EU) 2016/1148;

(4) „Betreiber wesentlicher Dienste“ bezeichnet eine öffentliche oder private Einrichtung im Sinne von Artikel 4 Nummer 4 der Richtlinie (EU) 2016/1148;

(5) „Anbieter digitaler Dienste“ bezeichnet eine juristische Person, die einen digitalen Dienst im Sinne von Artikel 4 Nummer 6 der Richtlinie (EU) 2016/1148 anbietet;

(6) „Sicherheitsvorfall“ bezeichnet ein Ereignis im Sinne von Artikel 4 Nummer 7 der Richtlinie (EU) 2016/1148;

(7) „Bewältigung von Sicherheitsvorfällen“ bezeichnet alle Verfahren im Sinne von Artikel 4 Nummer 8 der Richtlinie (EU) 2016/1148;

(8) „Cyberbedrohung“ bezeichnet einen möglichen Umstand oder ein mögliches Ereignis, der bzw. das Netz- und Informationssysteme, deren Nutzer und betroffene Personen beeinträchtigen könnte;

(9) „europäisches System für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, auf Unionsebene festgelegtes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren für die Zertifizierung von Produkten und

Diensten der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden;

(10) „europäisches Cybersicherheitszertifikat“ bezeichnet ein von einer Konformitätsbewertungsstelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt oder ein bestimmter IKT-Dienst die in einem europäischen System für die Cybersicherheitszertifizierung festgelegten besonderen Anforderungen erfüllt;

(11) „IKT-Produkte und -Dienste“ bezeichnet ein Element oder eine Gruppe von Elementen der Netz- und Informationssysteme;

(12) „Akkreditierung“ bezeichnet die Akkreditierung im Sinne von Artikel 2 Nummer 10 der Verordnung (EG) Nr. 765/2008;

(13) „nationale Akkreditierungsstelle“ bezeichnet eine nationale Akkreditierungsstelle im Sinne von Artikel 2 Nummer 11 der Verordnung (EG) Nr. 765/2008;

(14) „Konformitätsbewertung“ bezeichnet die Konformitätsbewertung im Sinne von Artikel 2 Nummer 12 der Verordnung (EG) Nr. 765/2008;

(15) „Konformitätsbewertungsstelle“ bezeichnet eine Konformitätsbewertungsstelle im Sinne von Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008;

(16) „Norm“ bezeichnet eine Norm im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012.

TITEL II
ENISA – die „EU-Cybersicherheitsagentur“

KAPITEL I
MANDAT, ZIELE UND AUFGABEN

Artikel 3
Mandat

1. Die Agentur nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, zu einem hohen Maß an Cybersicherheit innerhalb der Union beizutragen.

2. Die Agentur nimmt die Aufgaben wahr, die ihr durch Rechtsakte der Union übertragen wurden, mit denen die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten auf dem Gebiet der Cybersicherheit angeglichen werden sollen.

3. Von den Zielen und Aufgaben der Agentur unberührt bleiben die Zuständigkeiten der Mitgliedstaaten im Bereich der Cybersicherheit sowie auf jeden Fall Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich.

Artikel 4
Ziele

1. Die Agentur soll aufgrund ihrer Unabhängigkeit, der wissenschaftlichen und technischen Qualität ihrer Beratung und Unterstützung, der von ihr bereitgestellten Informationen, der Transparenz ihrer operativen Verfahren und Arbeitsmethoden sowie der Sorgfalt bei der Wahrnehmung ihrer Aufgaben als Kompetenzzentrum in Fragen der Cybersicherheit dienen.

2. Die Agentur unterstützt die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten bei der Ausarbeitung und Umsetzung von Strategien im Zusammenhang mit der Cybersicherheit.

3. Die Agentur fördert unionsweit den Kapazitätsaufbau und die Abwehrbereitschaft, indem sie die Union, die Mitgliedstaaten sowie öffentliche und private Interessenträger dabei unterstützt, den Schutz ihrer Netz- und Informationssysteme zu verbessern, Fähigkeiten und Kompetenzen auf dem Gebiet der Cybersicherheit aufzubauen und sich gegen Cyberangriffe zu wappnen.

4. Die Agentur fördert auf Unionsebene die Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union sowie den einschlägigen Interessenträgern, auch des Privatsektors, in Fragen, die im Zusammenhang mit der Cybersicherheit stehen.

5. Die Agentur baut die Cybersicherheitskapazitäten auf Unionsebene aus, um – vor allem bei grenzüberschreitenden Sicherheitsvorfällen – die Maßnahmen zu ergänzen, die die Mitgliedstaaten zur Vermeidung von Bedrohungen oder als Reaktion darauf ergreifen.

6. Die Agentur fördert die Nutzung der Zertifizierung, auch indem sie zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens auf Unionsebene im Sinne

des Titels III dieser Verordnung beiträgt, um die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten und -Diensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt zu stärken.

7. Die Agentur fördert ein hohes Problembewusstsein der Bürger und Unternehmen in Fragen der Cybersicherheit.

Artikel 5

Aufgaben in Bezug auf die Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts

Die Agentur trägt zur Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts bei, indem sie

1. insbesondere durch unabhängige Stellungnahmen und durch vorbereitende Arbeiten zur Ausarbeitung und Überprüfung der Unionspolitik und des Unionsrechts auf dem Gebiet der Cybersicherheit Beratung und Unterstützung gewährt und indem sie sektorspezifische Strategien und Rechtsetzungsinitiativen im Bereich der Cybersicherheit vorlegt;

2. die Mitgliedstaaten darin unterstützt, die Unionspolitik und das Unionsrecht auf dem Gebiet der Cybersicherheit, vor allem im Zusammenhang mit der Richtlinie (EU) 2016/1148, kohärent umzusetzen, auch durch Stellungnahmen, Leitlinien, Beratung und bewährte Verfahren zu Themen wie Risikomanagement, Meldung von Sicherheitsvorfällen und Informationsweitergabe, und indem sie den Austausch bewährter Verfahren in diesem Bereich zwischen den zuständigen Behörden erleichtert;

3. ihre Sachkenntnis und Unterstützung in die Arbeit der nach Artikel 11 der Richtlinie (EU) 2016/1148 eingesetzten Kooperationsgruppe einbringt;

4. Folgendes unterstützt:

   (1) die Entwicklung und Umsetzung der Unionspolitik im Bereich der elektronischen Identität und Vertrauensdienste, vor allem durch Beratung und technische Leitlinien sowie durch die Erleichterung des Austauschs bewährter Verfahren zwischen den zuständigen Behörden;

   (2) die Förderung eines höheren Sicherheitsniveaus in der elektronischen Kommunikation, auch indem sie ihre Sachkenntnis und Beratung anbietet und den Austausch bewährter Verfahren zwischen den zuständigen Behörden erleichtert;

5. die regelmäßige Überprüfung der Unionspolitik unterstützt und dazu einen Jahresbericht über die Stand der Umsetzung des jeweiligen Rechtsrahmens vorlegt in Bezug auf:

   (a) die Meldungen von Sicherheitsvorfällen durch die Mitgliedstaaten über die zentrale Anlaufstelle der Kooperationsgruppe nach Artikel 10 Absatz 3 der Richtlinie (EU) 2016/1148;

   (b) die Meldungen von Sicherheitsverletzungen und Integritätsverlusten bei Vertrauensdiensteanbietern, die der Agentur auf der Grundlage von Artikel 19

Absatz 3 der Verordnung (EU) Nr. 910/2014 von den Aufsichtsstellen übermittelt werden;

(c) die Meldungen von Sicherheitsverletzungen durch Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste betreiben, die der Agentur von den zuständigen Behörden auf der Grundlage von Artikel 40 der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] übermittelt werden.

Artikel 6

Aufgaben in Bezug auf den Kapazitätsaufbau

1. Die Agentur unterstützt

(a) die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Kapazitäten für die Bewältigung von Problemen und Vorfällen im Bereich der Cybersicherheit, indem sie ihnen das erforderliche Wissen und die notwendigen Sachkenntnisse zur Verfügung stellt;

(b) die Organe, Einrichtungen und sonstigen Stellen der Union bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Kapazitäten für die Bewältigung von Problemen und Vorfällen im Bereich der Cybersicherheit, indem sie das CERT für die Organe, Agenturen und sonstigen Einrichtungen der Union (CERT-EU) angemessen unterstützt;

(c) die Mitgliedstaaten auf deren Ersuchen beim Aufbau nationaler Computer-Notfallteams (CSIRTs) nach Artikel 9 Absatz 5 der Richtlinie (EU) 2016/1148;

(d) die Mitgliedstaaten auf deren Ersuchen bei der Ausarbeitung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen nach Artikel 7 Absatz 2 der Richtlinie (EU) 2016/1148; zudem fördert die Agentur die unionsweite Verbreitung dieser Strategien und verfolgt deren Umsetzung, um bewährte Verfahren bekannt zu machen;

(e) die Organe der Union bei der Ausarbeitung und Überprüfung von Unionsstrategien zur Cybersicherheit, fördert deren Verbreitung und verfolgt die Fortschritte bei deren Umsetzung;

(f) die CSIRTs der Mitgliedstaaten und der Union bei der Anhebung des Niveaus ihrer Fähigkeiten, auch durch die Förderung des Dialogs und Informationsaustauschs, damit jedes CSIRT entsprechend dem Stand der Technik einen gemeinsamen Satz an Minimalfähigkeiten hat und entsprechend der bewährten Praxis arbeitet;

(g) die Mitgliedstaaten durch die Organisation jährlicher groß angelegter Cybersicherheitsübungen auf Unionsebene nach Artikel 7 Absatz 6 und durch die Abgabe von Empfehlungen, die sie aus der Auswertung der Übungen und der bei diesen gemachten Erfahrungen ableitet;

(h) einschlägige öffentliche Stellen, indem sie diesen, gegebenenfalls in Zusammenarbeit mit Interessenträgern, Fortbildungen zur Cybersicherheit anbietet;

(i) die Kooperationsgruppe durch den Austausch bewährter Verfahren, vor allem zur Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten, auch im Zusammenhang mit grenzüberschreitenden Abhängigkeiten, im Hinblick auf Risiken

und Sicherheitsvorfälle, nach Artikel 11 Absatz 3 Buchstabe l der Richtlinie (EU) 2016/1148.

2. Die Agentur erleichtert die Einrichtung sektorbezogener Informationsaustausch- und -analysezentren (*Information Sharing and Analysis Centres* – ISACs) und unterstützt diese dauerhaft, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, indem sie bewährte Verfahren und Leitlinien zu den verfügbaren Instrumenten und Verfahren sowie zur Bewältigung rechtlicher Fragen im Zusammenhang mit der Informationsweitergabe bereitstellt.

Artikel 7

Aufgaben in Bezug auf die operative Zusammenarbeit auf Unionsebene

1. Die Agentur unterstützt die operative Zusammenarbeit zwischen den zuständigen öffentlichen Stellen untereinander und zwischen den Interessenträgern.

2. Die Agentur arbeitet auf operativer Ebene mit den Organen, Einrichtungen und sonstigen Stellen der Union zusammen und entwickelt Synergien mit diesen Stellen, zu denen auch das CERT-EU sowie die für Cyberkriminalität und die Aufsicht über den Datenschutz zuständigen Stellen zählen, um Fragen von gemeinsamem Interesse anzugehen, unter anderem durch

   (a) den Austausch von Know-how und bewährten Verfahren;

   (b) die Bereitstellung von Beratung und Leitlinien zu einschlägigen Themen im Zusammenhang mit der Cybersicherheit;

   (c) die Festlegung praktischer Modalitäten für die Wahrnehmung besonderer Aufgaben in Absprache mit der Kommission.

3. Die Agentur führt die Sekretariatsgeschäfte des CSIRTs-Netzes nach Artikel 12 Absatz 2 der Richtlinie (EU) 2016/1148 und erleichtert aktiv den Informationsaustausch und die Zusammenarbeit zwischen dessen Mitgliedern.

4. Die Agentur trägt zur operativen Zusammenarbeit innerhalb des CSIRTs-Netzes bei und unterstützt die Mitgliedstaaten, indem sie

   (a) diese berät, wie sie ihre Fähigkeiten zur Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen verbessern können;

   (b) auf deren Ersuchen bei Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen technische Hilfe zur Verfügung stellt;

   (c) Anfälligkeiten, Artefakte und Sicherheitsvorfälle analysiert.

Bei der Wahrnehmung dieser Aufgaben arbeiten die Agentur und das CERT-EU in strukturierter Weise zusammen, um vor allem bei operativen Aspekten Synergien nutzen zu können.

5. Auf Ersuchen von zwei oder mehreren betroffenen Mitgliedstaaten und zu dem alleinigen Zweck, Beratung im Hinblick auf die Vermeidung künftiger Sicherheitsvorfälle anzubieten, unterstützt die Agentur, nachdem Unternehmen gemäß der Richtlinie (EU) 2016/1148 Sicherheitsvorfälle mit beträchtlichen oder

erheblichen Auswirkungen gemeldet hatten, eine technische Ex-post-Untersuchung oder führt diese selbst durch. Eine derartige Untersuchung führt die Agentur auch dann durch, wenn sie bei solchen Sicherheitsvorfällen, von denen mindestens zwei Mitgliedstaaten betroffen sind, von der Kommission im Einvernehmen mit den betroffenen Mitgliedstaaten in einem hinreichend begründeten Ersuchen dazu aufgefordert wurde.

Der Umfang der Untersuchung und das bei einer solchen Untersuchung einzuhaltende Verfahren werden zwischen den betroffenen Mitgliedstaaten und der Agentur vereinbart; etwaige laufende strafrechtliche Untersuchungen desselben Sicherheitsvorfalls bleiben hiervon unberührt. Zum Abschluss der Untersuchung erstellt die Agentur einen technischen Abschlussbericht, in den insbesondere die Informationen und Kommentare der betroffenen Mitgliedstaaten und Unternehmen einfließen und der mit den betroffenen Mitgliedstaaten abgestimmt wird. Eine Zusammenfassung des Berichts mit den Empfehlungen zur Vermeidung künftiger Sicherheitsvorfälle wird dem CSIRTs-Netz zugeleitet.

6. Die Agentur organisiert auf Unionsebene jährliche Cybersicherheitsübungen und unterstützt die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der EU auf deren Ersuchen hin bei der Organisation solcher Übungen. Die jährlichen Übungen auf Unionsebene umfassen technische, operative und strategische Elemente und dienen der Vorbereitung der gemeinsamen Reaktion der Union auf massive, grenzüberschreitende Cybersicherheitsvorfälle. Die Agentur unterstützt gemeinsam mit den jeweiligen ISACs gegebenenfalls auch die Organisation sektorspezifischer Cybersicherheitsübungen und genehmigt den ISACs die Teilnahme an Cybersicherheitsübungen auf Unionsebene.

7. Die Agentur erstellt regelmäßig einen technischen Lagebericht über die Cybersicherheit in der EU auf der Grundlage von frei zugänglichen Informationen, eigenen Analysen und Berichten, die ihr u. a. übermittelt werden von den CSIRTs der Mitgliedstaaten (auf freiwilliger Basis) oder den zentralen Anlaufstellen im Sinne der NIS-Richtlinie (Artikel 14 Absatz 5) sowie dem bei Europol angesiedelten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und dem CERT-EU.

8. Die Agentur trägt zur Entwicklung gemeinsamer Maßnahmen bei, mit denen auf Ebene der Union und der Mitgliedstaaten auf massive, grenzüberschreitende Cybersicherheitsvorfälle oder Cyberkrisen reagiert werden kann, indem sie insbesondere:

   (a) Berichte aus nationalen Quellen als Beitrag zu einer gemeinsamen Lageerfassung zusammenstellt;

   (b) für einen effizienten Informationsfluss und Mechanismen sorgt, die zwischen dem CSIRTs-Netz und den fachlichen und politischen Entscheidungsträgern auf EU-Ebene eine abgestufte Vorgehensweise ermöglichen;

   (c) die technische Bewältigung eines Sicherheitsvorfalls oder einer Krise unterstützt, auch durch die Erleichterung der Weitergabe technischer Lösungen zwischen den Mitgliedstaaten;

   (d) die öffentliche Kommunikation im Umfeld des Sicherheitsvorfalls oder der Krise unterstützt;

   (e) die Kooperationspläne für die Reaktion auf solche Sicherheitsvorfälle oder Krisen testet.

Artikel 8

Aufgaben in Bezug auf den Markt, die Cybersicherheitszertifizierung und die Normung

Die Agentur

(a) unterstützt und fördert die Entwicklung und Umsetzung der Unionspolitik auf dem Gebiet der Cybersicherheitszertifizierung von IKT-Produkten und -Diensten, wie in Titel III dieser Verordnung festgelegt, indem sie

(1) mögliche europäische Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten nach Artikel 44 dieser Verordnung ausarbeitet;

(2) die Kommission bei der Wahrnehmung der Sekretariatsgeschäfte der nach Artikel 53 eingesetzten Gruppe für die Cybersicherheitszertifizierung unterstützt;

(3) in Zusammenarbeit mit nationalen Aufsichtsbehörden für die Zertifizierung Leitlinien zusammenstellt und veröffentlicht sowie bewährte Verfahren im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten und -Diensten entwickelt;

(b) erleichtert die Ausarbeitung und Übernahme europäischer und internationaler Normen für das Risikomanagement und die Sicherheit von IKT-Produkten und -Diensten, bietet nach Artikel 19 Absatz 2 der Richtlinie (EU) 2016/1148 in Zusammenarbeit mit den Mitgliedstaaten Beratung an und erlässt Leitlinien für die technischen Bereiche, die sich auf die Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beziehen, sowie für bereits vorhandene Normen, auch nationale Normen der Mitgliedstaaten;

(c) führt regelmäßig Analysen der wichtigsten Angebots- und Nachfragetrends auf dem Cybersicherheitsmarkt durch, um den Cybersicherheitsmarkt in der Union zu fördern.

Artikel 9

Aufgaben in Bezug auf Wissen, Informationen und Sensibilisierung

Die Agentur

(a) führt Analysen neu entstehender Technik durch und bietet themenspezifische Bewertungen der von den technischen Innovationen zu erwartenden gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Auswirkungen auf die Cybersicherheit;

(b) führt langfristige strategische Analysen der Cybersicherheitsbedrohungen und Sicherheitsvorfälle durch, um neu auftretende Trends erkennen und dazu beitragen zu können, Probleme im Zusammenhang mit der Cybersicherheit zu vermeiden;

(c) stellt in Zusammenarbeit mit den Sachverständigen der Behörden der Mitgliedstaaten Beratung, Leitlinien und bewährte Verfahren für die Sicherheit der Netz- und Informationssysteme zur Verfügung, vor allem für die Sicherheit der Internet-Infrastruktur und der Infrastrukturen, die die in Anhang II der Richtlinie (EU) 2016/1148 aufgeführten Sektoren unterstützen;

(d) bündelt die von den Organen, Einrichtungen und sonstigen Stellen der Union bereitgestellten Informationen zur Cybersicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung;

(e) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Verfahren zur Verfügung, die sich an Bürger und Organisationen wenden;

(f) erhebt und analysiert öffentlich verfügbare Informationen über signifikante Sicherheitsvorfälle und stellt Berichte mit dem Ziel zusammen, den Unternehmen und Bürgern unionsweit Orientierungshilfen an die Hand zu geben;

(g) organisiert in Zusammenarbeit mit den Mitgliedstaaten sowie den Organen, Einrichtungen und sonstigen Stellen der Union regelmäßige Aufklärungskampagnen, um die Cybersicherheit und ihre Sichtbarkeit in der Union zu erhöhen.

Artikel 10

Aufgaben in Bezug auf Forschung und Innovation

Im Zusammenhang mit der Forschung und Innovation

(a) berät die Agentur die Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten im Bereich der Cybersicherheit, damit die Voraussetzung für wirksame Reaktionen auf die gegenwärtigen oder sich abzeichnenden Risiken und Bedrohungen, auch in Bezug auf neue und aufkommende Informations- und Kommunikationstechnik (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;

(b) beteiligt sich die Agentur dort, wo die Kommission ihr die einschlägigen Befugnisse übertragen hat, an der Durchführungsphase von Förderprogrammen für Forschung und Innovation oder als Begünstige.

Artikel 11

Aufgaben in Bezug auf die internationale Zusammenarbeit

Die Agentur unterstützt die Bemühungen der Union um Zusammenarbeit mit Drittländern und internationalen Organisationen, um die internationale Zusammenarbeit in Angelegenheiten der Cybersicherheit zu fördern, indem sie

(a) – soweit zweckmäßig – bei der Organisation von internationalen Übungen als Beobachterin mitwirkt, die Ergebnisse solcher Übungen analysiert und sie dem Verwaltungsrat vorlegt;

(b) auf Ersuchen der Kommission den Austausch bewährter Verfahren zwischen den einschlägigen internationalen Organisationen erleichtert;

(c) der Kommission auf deren Ersuchen mit Sachkenntnis zur Seite steht.

KAPITEL II
ORGANISATION DER AGENTUR

Artikel 12
Struktur

Die Verwaltungs- und Leitungsstruktur der Agentur setzt sich wie folgt zusammen:

(a) einem Verwaltungsrat, der die in Artikel 14 genannten Funktionen ausübt;

(b) einem Exekutivrat, der die in Artikel 18 genannten Funktionen ausübt;

(c) einem Exekutivdirektor, der die in Artikel 19 genannten Zuständigkeiten wahrnimmt;

(d) einer Ständigen Gruppe der Interessenträger, die die in Artikel 20 genannten Funktionen ausübt.

ABSCHNITT 1
VERWALTUNGSRAT

Artikel 13
Zusammensetzung des Verwaltungsrats

1. Dem Verwaltungsrat gehören je ein Vertreter jedes Mitgliedstaats und zwei von der Kommission ernannte Vertreter an. Alle Vertreter verfügen über Stimmrecht.

2. Jedes Mitglied des Verwaltungsrats hat einen Stellvertreter, der das Mitglied im Fall seiner Abwesenheit vertritt.

3. Die Mitglieder des Verwaltungsrats und ihre Stellvertreter werden aufgrund ihrer Kenntnisse auf dem Gebiet der Cybersicherheit ernannt, wobei ihren einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen Rechnung zu tragen ist. 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.

Artikel 14
Funktionen des Verwaltungsrats

1. Der Verwaltungsrat

   (a) bestimmt die allgemeine Ausrichtung der Tätigkeit der Agentur und sorgt auch dafür, dass die Agentur bei ihrer Arbeit die in dieser Verordnung niedergelegten Vorschriften und Grundsätze beachtet. Er sorgt zudem für die Abstimmung der Arbeit der Agentur mit den Tätigkeiten, die von den Mitgliedstaaten und auf Unionsebene durchgeführt werden;

(b) nimmt den Entwurf des in Artikel 21 genannten einheitlichen Programmplanungsdokuments der Agentur an, bevor dieser der Kommission zur Stellungnahme vorgelegt wird;

(c) nimmt – unter Berücksichtigung der Stellungnahme der Kommission – das einheitliche Programmplanungsdokument der Agentur nach Artikel 17 mit der Zweidrittelmehrheit seiner Mitglieder an;

(d) stellt mit der Zweidrittelmehrheit seiner Mitglieder den jährlichen Haushaltsplan der Agentur fest und übt andere Funktionen in Bezug auf den Haushalt der Agentur gemäß Kapitel III aus;

(e) bewertet und genehmigt den konsolidierten Jahresbericht über die Tätigkeiten der Agentur und übermittelt den Bericht zusammen mit seiner Bewertung bis zum 1. Juli des folgenden Jahres dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof. Der Jahresbericht enthält den Jahresabschluss und Ausführungen darüber, inwiefern die Agentur die vorgegebenen Leistungsindikatoren erfüllt hat. Der Jahresbericht wird veröffentlicht;

(f) erlässt nach Artikel 29 die für die Agentur geltende Finanzregelung;

(g) nimmt eine Betrugsbekämpfungsstrategie an, die den diesbezüglichen Risiken entspricht und an einer Kosten-Nutzen-Analyse der durchzuführenden Maßnahmen orientiert ist;

(h) erlässt Vorschriften zur Unterbindung und Bewältigung von Interessenkonflikten bei seinen Mitgliedern;

(i) sorgt ausgehend von den Erkenntnissen und Empfehlungen, die sich aus den Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und den verschiedenen internen und externen Prüfberichten und Bewertungen ergeben haben, für angemessene Folgemaßnahmen;

(j) gibt sich eine Geschäftsordnung;

(k) nimmt nach Absatz 2 in Bezug auf das Personal der Agentur die Befugnisse wahr, die der Anstellungsbehörde durch das Statut der Beamten der Europäischen Union bzw. der Stelle, die zum Abschluss der Dienstverträge ermächtigt ist, durch die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union übertragen wurden („Befugnisse der Anstellungsbehörde“);

(l) erlässt gemäß dem Verfahren des Artikels 110 des Statuts der Beamten Durchführungsbestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen für die sonstigen Bediensteten;

(m) ernennt den Exekutivdirektor und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn nach Artikel 33 seines Amtes;

(n) ernennt einen Rechnungsführer, bei dem es sich um den Rechnungsführer der Kommission handeln kann, der in der Wahrnehmung seiner Aufgaben völlig unabhängig ist;

(o) fasst unter Berücksichtigung der Tätigkeitserfordernisse der Agentur und unter Beachtung der Grundsätze einer wirtschaftlichen Haushaltsführung alle Beschlüsse über die Schaffung und, falls notwendig, Änderung der Organisationsstruktur der Agentur;

(p) genehmigt den Abschluss von Arbeitsvereinbarungen nach Artikel 7 und Artikel 39.

2. Der Verwaltungsrat fasst gemäß nach Artikel 110 des Statuts der Beamten, einen Beschluss auf der Grundlage von Artikel 2 Absatz 1 des Statuts der Beamten und von Artikel 6 der Beschäftigungsbedingungen für die sonstigen Bediensteten, mit dem er die einschlägigen Befugnisse einer Anstellungsbehörde dem Exekutivdirektor überträgt und die Bedingungen festlegt, unter denen die Befugnisübertragung ausgesetzt werden kann. Der Exekutivdirektor kann diese Befugnisse einer nachgeordneten Ebene übertragen.

3. Wenn außergewöhnliche Umstände dies erfordern, kann der Verwaltungsrat durch Beschluss die Übertragung der Befugnisse der Anstellungsbehörde auf den Exekutivdirektor sowie die von diesem vorgenommene Weiterübertragung von Befugnissen vorübergehend aussetzen und die Befugnisse selbst ausüben oder sie einem seiner Mitglieder oder einem anderen Bediensteten als dem Exekutivdirektor übertragen.

Artikel 15
Vorsitz des Verwaltungsrats

Der Verwaltungsrat wählt aus dem Kreis seiner Mitglieder mit der Zweidrittelmehrheit seiner Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden für die Dauer von vier Jahren, wobei eine einmalige Wiederwahl zulässig ist. Endet jedoch ihre Mitgliedschaft im Verwaltungsrat während ihrer Amtszeit, so endet auch ihre Amtszeit automatisch am selben Tag. Der stellvertretende Vorsitzende tritt im Fall der Verhinderung des Vorsitzenden von Amts wegen an dessen Stelle.

Artikel 16
Sitzungen des Verwaltungsrats

1. Der Verwaltungsrat wird von seinem Vorsitzenden einberufen.

2. Der Verwaltungsrat tritt mindestens zweimal jährlich zu einer ordentlichen Sitzung zusammen. Auf Antrag des Vorsitzenden, der Kommission oder mindestens eines Drittels seiner Mitglieder tritt er darüber hinaus zu außerordentlichen Sitzungen zusammen.

3. Der Exekutivdirektor nimmt an den Sitzungen des Verwaltungsrats ohne Stimmrecht teil.

4. Mitglieder der Ständigen Gruppe der Interessenträger können auf Einladung des Vorsitzes an den Sitzungen des Verwaltungsrats ohne Stimmrecht teilnehmen.

5. Die Mitglieder des Verwaltungsrats und ihre Stellvertreter können sich nach Maßgabe seiner Geschäftsordnung von Beratern oder Experten unterstützen lassen.

6. Die Sekretariatsgeschäfte des Verwaltungsrats werden von der Agentur wahrgenommen.

Artikel 17
Abstimmungsregeln des Verwaltungsrates

1. Der Verwaltungsrat fasst seine Beschlüsse mit der Mehrheit seiner Mitglieder.

2. Für die Annahme des einheitlichen Programmplanungsdokuments und des jährlichen Haushaltsplans sowie für die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors ist eine Mehrheit von zwei Dritteln aller Mitglieder des Verwaltungsrats erforderlich.

3. Jedes Mitglied hat eine Stimme. In Abwesenheit eines Mitglieds kann sein Stellvertreter dessen Stimmrecht ausüben.

4. Der Vorsitzende nimmt an den Abstimmungen teil.

5. Der Exekutivdirektor nimmt nicht an den Abstimmungen teil.

6. Die näheren Einzelheiten der Abstimmungsmodalitäten, insbesondere die Voraussetzungen, unter denen ein Mitglied im Namen eines anderen Mitglieds handeln kann, werden in der Geschäftsordnung des Verwaltungsrats festgelegt.

ABSCHNITT 2
EXEKUTIVRAT

Artikel 18
Exekutivrat

1. Der Verwaltungsrat wird von einem Exekutivrat unterstützt.

2. Der Exekutivrat

   (a) bereitet die Beschlussvorlagen für den Verwaltungsrat vor;

   (b) stellt zusammen mit dem Verwaltungsrat sicher, dass ausgehend von den Ergebnissen und Empfehlungen im Rahmen der Untersuchungen des OLAF und der externen oder internen Prüfberichte und Bewertungen angemessene Folgemaßnahmen getroffen werden;

   (c) unterstützt und berät unbeschadet der Aufgaben des Exekutivdirektors nach Artikel 19 den Exekutivdirektor bei der Umsetzung der verwaltungs- und haushaltsbezogenen Beschlüsse des Verwaltungsrats.

3. Der Exekutivrat besteht aus fünf Mitgliedern, die aus den Reihen der Mitglieder des Verwaltungsrats ernannt werden; darunter befinden sich der Vorsitzende des Verwaltungsrats, der zugleich auch Vorsitzender des Exekutivrats sein kann, und einer der Vertreter der Kommission. Der Exekutivdirektor nimmt an den Sitzungen des Exekutivrats ohne Stimmrecht teil.

4. Die Amtszeit der Mitglieder des Exekutivrats beträgt vier Jahre. Sie kann verlängert werden.

5. Der Exekutivrat tritt mindestens einmal alle drei Monate zusammen. Der Vorsitzende des Exekutivrats beruft auf Antrag der Mitglieder zusätzliche Sitzungen ein.

6. Der Verwaltungsrat legt die Geschäftsordnung des Exekutivrats fest.

7. In dringenden Fällen kann der Exekutivrat im Namen des Verwaltungsrats bestimmte vorläufige Beschlüsse fassen, vor allem in Verwaltungsangelegenheiten, einschließlich der Aussetzung der Übertragung der Befugnisse der Anstellungsbehörde, und in Haushaltsangelegenheiten.

ABSCHNITT 3
EXEKUTIVDIREKTOR

Artikel 19
Zuständigkeiten des Exekutivdirektors

1. Die Agentur wird von ihrem Exekutivdirektor geleitet, der bei der Wahrnehmung seiner Aufgaben unabhängig ist. Der Exekutivdirektor ist gegenüber dem Verwaltungsrat rechenschaftspflichtig.

2. Der Exekutivdirektor erstattet dem Europäischen Parlament über die Erfüllung seiner Aufgaben Bericht, wenn er dazu aufgefordert wird. Der Rat kann den Exekutivdirektor auffordern, über die Erfüllung seiner Aufgaben Bericht zu erstatten.

3. Der Exekutivdirektor ist dafür verantwortlich,

   (a) die laufenden Geschäfte der Agentur zu führen;

   (b) die vom Verwaltungsrat gefassten Beschlüsse umzusetzen;

   (c) den Entwurf des einheitlichen Programmplanungsdokuments auszuarbeiten und dem Verwaltungsrat vor der Übermittlung an die Kommission vorzulegen;

   (d) das einheitliche Programmplanungsdokument umzusetzen und dem Verwaltungsrat hierüber Bericht zu erstatten;

   (e) den konsolidierten Jahresbericht über die Tätigkeit der Agentur auszuarbeiten und dem Verwaltungsrat zur Bewertung und Annahme vorzulegen;

   (f) einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen der nachträglichen Bewertungen auszuarbeiten und alle zwei Jahre der Kommission über die erzielten Fortschritte Bericht zu erstatten;

   (g) einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen interner oder externer Prüfberichte sowie der Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) auszuarbeiten und der Kommission zweimal jährlich und dem Verwaltungsrat regelmäßig über die erzielten Fortschritte Bericht zu erstatten;

   (h) den Entwurf der für die Agentur geltenden Finanzregelung auszuarbeiten;

   (i) den Entwurf des Voranschlags der Einnahmen und Ausgaben der Agentur auszuarbeiten und ihren Haushaltsplan auszuführen;

   (j) die finanziellen Interessen der Union durch vorbeugende Maßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch wirksame Kontrollen und, falls Unregelmäßigkeiten festgestellt werden, durch Einziehung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch Verhängung wirksamer, verhältnismäßiger und abschreckender verwaltungsrechtlicher und finanzieller Sanktionen zu schützen;

(k) eine Betrugsbekämpfungsstrategie für die Agentur auszuarbeiten und dem Verwaltungsrat zur Genehmigung vorzulegen;

(l) Kontakte zur Wirtschaft und zu Verbraucherorganisationen im Hinblick auf einen regelmäßigen Dialog mit den einschlägigen Interessenträgern aufzubauen und zu pflegen;

(m) sonstige dem Exekutivdirektor durch diese Verordnung übertragene Aufgaben wahrzunehmen.

4. Soweit erforderlich kann der Exekutivdirektor im Rahmen des Mandats der Agentur sowie entsprechend ihren Zielen und Aufgaben Ad-hoc-Arbeitsgruppen aus Sachverständigen – auch von den zuständigen Behörden der Mitgliedstaaten – einsetzen. Der Verwaltungsrat wird hiervon vorab unterrichtet. Die Verfahren, die insbesondere die Zusammensetzung dieser Arbeitsgruppen, die Bestellung der Sachverständigen der Arbeitsgruppen durch den Exekutivdirektor und die Arbeitsweise der Arbeitsgruppen betreffen, werden in den internen Verfahrensvorschriften der Agentur festgelegt.

5. Der Exekutivdirektor beschließt, inwieweit es notwendig ist, Mitarbeiter in einem oder mehreren Mitgliedstaaten einzusetzen, damit die Agentur ihre Aufgaben effizient und wirksam wahrnehmen kann. Bevor er über die Einrichtung einer Außenstelle beschließt, holt der Exekutivdirektor die vorherige Zustimmung der Kommission, des Verwaltungsrats und des betreffenden Mitgliedstaats bzw. der betreffenden Mitgliedstaaten ein. In dem Beschluss wird der Umfang der in der Außenstelle auszuübenden Tätigkeiten so festgelegt, dass unnötige Kosten und eine Überschneidung der Verwaltungsfunktionen mit denen der Agentur vermieden werden. Soweit dies angemessen oder notwendig ist, wird mit dem/den betreffenden Mitgliedstaat(en) eine entsprechende Vereinbarung getroffen.

ABSCHNITT 4
STÄNDIGE GRUPPE DER INTERESSENTRÄGER

Artikel 20
Ständige Gruppe der Interessenträger

1. Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors eine Ständige Gruppe der Interessenträger ein, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, Verbrauchergruppen, wissenschaftliche Sachverständige für die Cybersicherheit sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.

2. Die Verfahren für die Ständige Gruppe der Interessenträger, die insbesondere die Anzahl, die Zusammensetzung, die Ernennung der Mitglieder durch den Verwaltungsrat, den Vorschlag des Exekutivdirektors und die Arbeitsweise der Gruppe betreffen, werden in den internen Verfahrensvorschriften der Agentur festgelegt und öffentlich bekannt gemacht.

3. Den Vorsitz der Ständigen Gruppe der Interessenträger führt der Exekutivdirektor oder eine vom Exekutivdirektor jeweils ernannte Person.

4. Die Amtszeit der Mitglieder der Ständigen Gruppe der Interessenträger beträgt zweieinhalb Jahre. Die Mitglieder des Verwaltungsrats dürfen nicht Mitglieder der Ständigen Gruppe der Interessenträger sein. Sachverständige der Kommission und aus den Mitgliedstaaten können an den Sitzungen der Ständigen Gruppe der Interessenträger teilnehmen und an ihrer Arbeit mitwirken. Vertreter anderer Stellen, die vom Exekutivdirektor für relevant erachtet werden und die der Ständigen Gruppe der Interessenträger nicht angehören, können zur Teilnahme an den Sitzungen der Ständigen Gruppe der Interessenträger und zur Mitarbeit an ihrer Arbeit eingeladen werden.

5. Die Ständige Gruppe der Interessenträger berät die Agentur bei der Durchführung ihrer Tätigkeiten. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Arbeitsprogramm der Agentur und bei der Gewährleistung der Kommunikation mit den einschlägigen Interessenträgern bezüglich aller Fragen im Zusammenhang mit dem Arbeitsprogramm.

ABSCHNITT 5
ARBEITSWEISE

Artikel 21
Einheitliches Programmplanungsdokument

1. Die Agentur handelt in Übereinstimmung mit einem einheitlichen Programmplanungsdokument, das ihre jährliche und mehrjährige Programmplanung mit allen ihren geplanten Tätigkeiten enthält.

2. Jedes Jahr erstellt der Exekutivdirektor einen Entwurf des einheitlichen Programmplanungsdokuments mit der jährlichen und mehrjährigen Programmplanung und der entsprechenden Personal- und Finanzplanung nach Artikel 32 der Delegierten Verordnung (EU) Nr. 1271/2013[36] der Kommission und unter Berücksichtigung der von der Kommission festgelegten Leitlinien.

3. Bis zum 30. November eines jeden Jahres nimmt der Verwaltungsrat das in Absatz 1 genannte einheitliche Programmplanungsdokument an und leitet es spätestens bis zum 31. Januar des Folgejahres sowie jede spätere Aktualisierung dieses Dokuments an das Europäische Parlament, den Rat und die Kommission weiter.

4. Das einheitliche Programmplanungsdokument wird nach der endgültigen Feststellung des Gesamthaushaltsplans der Union endgültig und ist, erforderlichenfalls, entsprechend anzupassen.

5. Das Jahresarbeitsprogramm enthält detaillierte Ziele und Angaben zu den erwarteten Ergebnissen, einschließlich Erfolgsindikatoren. Es enthält zudem eine Beschreibung der zu finanzierenden Maßnahmen sowie Angaben zur Höhe der für die einzelnen Maßnahmen vorgesehenen finanziellen und personellen Ressourcen gemäß den Grundsätzen der maßnahmenbezogenen Aufstellung des Haushaltsplans und des

---

[36] Delegierte Verordnung (EU) Nr. 1271/2013 der Kommission vom 30. September 2013 über die Rahmenfinanzregelung für Einrichtungen gemäß Artikel 208 der Verordnung (EU, Euratom) Nr. 966/2012 des Europäischen Parlaments und des Rates (ABl. L 328 vom 7.12.2013, S. 42).

maßnahmenbezogenen Managements. Das Jahresarbeitsprogramm muss mit dem mehrjährigen Arbeitsprogramm nach Absatz 7 im Einklang stehen. Es ist klar darin anzugeben, welche Aufgaben im Vergleich zum vorangegangenen Haushaltsjahr hinzugefügt, verändert oder gestrichen wurden.

6. Der Verwaltungsrat ändert das angenommene Jahresarbeitsprogramm, wenn der Agentur eine neue Aufgabe übertragen wird. Wesentliche Änderungen des jährlichen Arbeitsprogramms werden nach demselben Verfahren angenommen wie das ursprüngliche jährliche Arbeitsprogramm. Der Verwaltungsrat kann dem Exekutivdirektor die Befugnis übertragen, nicht wesentliche Änderungen am Jahresarbeitsprogramm vorzunehmen.

7. Im mehrjährigen Arbeitsprogramm der Agentur wird die strategische Gesamtplanung einschließlich der Ziele, erwarteten Ergebnisse und Leistungsindikatoren festgelegt. Es umfasst auch die Ressourcenplanung mit einem mehrjährigen Finanz- und Personalplan.

8. Die Ressourcenplanung wird jährlich aktualisiert. Die strategische Programmplanung ist zu aktualisieren, wann immer dies geboten erscheint und insbesondere wenn dies notwendig ist, um dem Ergebnis der in Artikel 56 genannten Bewertung Rechnung zu tragen.

Artikel 22
Interessenerklärung

1. Die Mitglieder des Verwaltungsrats, der Exekutivdirektor und die von den Mitgliedstaaten auf Zeit abgeordneten Beamten geben eine Verpflichtungserklärung und eine Interessenerklärung ab, aus der hervorgeht, ob direkte oder indirekte Interessen bestehen, die ihre Unabhängigkeit beeinträchtigen könnten. Die Erklärungen müssen der Wahrheit entsprechen und vollständig sein; sie werden jedes Jahr schriftlich abgegeben und, wann immer erforderlich, aktualisiert.

2. Die Mitglieder des Verwaltungsrats, der Exekutivdirektor und externe Sachverständige, die in den Ad-hoc-Arbeitsgruppen mitwirken, geben spätestens zu Beginn jeder Sitzung eine wahrheitsgetreue und vollständige Erklärung über alle Interessen ab, die ihre Unabhängigkeit in Bezug auf die Tagesordnungspunkte beeinträchtigen könnten, und beteiligen sich nicht an den Diskussionen und den Abstimmungen über solche Punkte.

3. Die Agentur legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten der Vorschriften über Interessenerklärungen nach den Absätzen 1 und 2 fest.

Artikel 23
Transparenz

1. Die Agentur übt ihre Tätigkeiten mit einem hohen Maß an Transparenz und im Einklang mit Artikel 25 aus.

2. Die Agentur stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere zu ihren eigenen Arbeitsergebnissen, erhalten. Ferner veröffentlicht sie die nach Artikel 22 abgegebenen Interessenerklärungen.

3. Der Verwaltungsrat kann auf Vorschlag des Exekutivdirektors gestatten, dass interessierte Kreise als Beobachter an bestimmten Tätigkeiten der Agentur teilnehmen.

4. Die Agentur legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Transparenzregelungen fest.

Artikel 24
Vertraulichkeit

1. Unbeschadet des Artikels 25 gibt die Agentur Informationen, die bei ihr eingehen oder von ihr verarbeitet werden und die auf begründetes Ersuchen ganz oder teilweise vertraulich behandelt werden sollen, nicht an Dritte weiter.

2. Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, die Mitglieder der Ständigen Gruppe der Interessenträger, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal der Agentur, einschließlich der von den Mitgliedstaaten auf Zeit abgeordneten Beamten, unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

3. Die Agentur legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Vertraulichkeitsregelungen fest.

4. Soweit es zur Erfüllung der Aufgaben der Agentur erforderlich ist, beschließt der Verwaltungsrat, die Agentur zum Umgang mit Verschlusssachen zu ermächtigen. In diesem Fall legt der Verwaltungsrat im Einvernehmen mit den Dienststellen der Kommission interne Verfahrensvorschriften zur Anwendung der Sicherheitsgrundsätze, die in den Beschlüssen (EU, Euratom) 2015/443[37] und 2015/444[38] der Kommission niedergelegt sind, fest. Diese Vorschriften betreffen unter anderem die Bestimmungen über den Austausch, die Verarbeitung und die Speicherung von Verschlusssachen.

Artikel 25
Zugang zu Dokumenten

1. Die Verordnung (EG) Nr. 1049/2001 findet Anwendung auf die Dokumente der Agentur.

2. Der Verwaltungsrat legt innerhalb von sechs Monaten nach Errichtung der Agentur die Modalitäten zur Durchführung der Verordnung (EG) Nr. 1049/2001 fest.

3. Gegen Entscheidungen der Agentur nach Artikel 8 der Verordnung (EG) Nr. 1049/2001 kann nach Maßgabe von Artikel 228 AEUV bzw. 263 AEUV Beschwerde beim Bürgerbeauftragten eingelegt oder Klage beim Gerichtshof der Europäischen Union erhoben werden.

---

37 Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 14).

38 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).

KAPITEL III
AUFSTELLUNG UND GLIEDERUNG DES HAUSHALTSPLANS

Artikel 26
Aufstellung des Haushaltsplans

1. Der Exekutivdirektor erstellt jedes Jahr den Entwurf des Voranschlags der Einnahmen und Ausgaben der Agentur für das folgende Haushaltsjahr und legt ihn dem Verwaltungsrat zusammen mit dem Entwurf des Stellenplans vor. Einnahmen und Ausgaben müssen ausgeglichen sein.

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 der Agentur für das folgende Haushaltsjahr.

3. Der Verwaltungsrat übermittelt jedes Jahr bis zum 31. Januar der Kommission und den Drittländern, mit denen die Union Abkommen nach Artikel 39 geschlossen hat, den in Absatz 2 genannten Voranschlag, der Teil des Entwurfs des einheitlichen Programmplanungsdokuments ist.

4. Die Kommission setzt aufgrund dieses Voranschlags die von ihr für erforderlich erachteten Mittelansätze für den Stellenplan und den Betrag des Zuschusses aus dem Gesamthaushaltsplan in den Haushaltsplanentwurf der Union ein, den sie nach den Artikeln 313 und 314 AEUV dem Europäischen Parlament und dem Rat vorlegt.

5. Das Europäische Parlament und der Rat bewilligen die Mittel für den Beitrag für die Agentur.

6. Das Europäische Parlament und der Rat legen den Stellenplan der Agentur fest.

7. Der Haushaltsplan der Agentur wird zusammen mit dem einheitlichen Programmplanungsdokument vom Verwaltungsrat angenommen. Er wird endgültig, sobald der Gesamthaushaltsplan der Union endgültig festgestellt ist. Gegebenenfalls nimmt der Verwaltungsrat eine Anpassung des Haushaltsplans der Agentur und des einheitlichen Programmplanungsdokuments entsprechend dem Gesamthaushaltsplan der Union vor.

Artikel 27
Gliederung des Haushaltsplans

1. Unbeschadet sonstiger Ressourcen gliedern sich die Einnahmen der Agentur wie folgt:

   (a) ein Beitrag aus dem Haushalt der Union;

   (b) Einnahmen, die konkreten Ausgabenpositionen im Einklang mit der in Artikel 29 genannten Finanzregelung zugewiesen werden;

   (c) Unionsmittel in Form von Übertragungsvereinbarungen oder Ad-hoc-Finanzhilfen im Einklang mit der in Artikel 29 genannten Finanzregelung der Agentur und den Bestimmungen der einschlägigen Instrumente zur Unterstützung der Unionspolitik;

(d) Beiträge von Drittländern, die sich nach Artikel 39 an der Arbeit der Agentur beteiligen;

(e) freiwillige Zahlungen oder Sachleistungen von Mitgliedstaaten; Mitgliedstaaten, die einen freiwilligen Beitrag leisten, können aufgrund dessen keine bestimmten Rechte oder Dienstleistungen beanspruchen.

2. Die Ausgaben der Agentur umfassen Aufwendungen für Personal, Verwaltung, technische Unterstützung, Infrastruktur, Betriebskosten und Ausgaben, die sich aus Verträgen mit Dritten ergeben.

Artikel 28
Ausführung des Haushaltsplans

1. Der Exekutivdirektor trägt die Verantwortung für die Ausführung des Haushaltsplans der Agentur.

2. Der interne Rechnungsprüfer der Kommission übt gegenüber der Agentur dieselben Befugnisse wie gegenüber den Kommissionsdienststellen aus.

3. Bis zum 1. März des jeweils folgenden Haushaltsjahres (1. März des Jahres n+1) übermittelt der Rechnungsführer der Agentur dem Rechnungsführer der Kommission und dem Rechnungshof den vorläufigen Jahresabschluss.

4. Nach Eingang der Bemerkungen des Rechnungshofes zum vorläufigen Jahresabschluss der Agentur, erstellt der Rechnungsführer in eigener Verantwortung den endgültigen Jahresabschluss der Agentur.

5. Der Exekutivdirektor legt den endgültigen Jahresabschluss dem Verwaltungsrat zur Stellungnahme vor.

6. Der Exekutivdirektor übermittelt den Bericht über die Haushaltsführung und das Finanzmanagement bis zum 31. März des Jahres n+1 dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof.

7. Der Rechnungsführer leitet den endgültigen Jahresabschluss zusammen mit der Stellungnahme des Verwaltungsrats bis zum 1. Juli des Jahres n+1 dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof zu.

8. Gleichzeitig mit der Übermittlung des endgültigen Jahresabschlusses leitet der Rechnungsführer auch dem Rechnungshof eine Erklärung über die Vollständigkeit dieses endgültigen Jahresabschlusses mit Kopie an den Rechnungsführer der Kommission zu.

9. Der Exekutivdirektor veröffentlicht den endgültigen Jahresabschluss bis zum 15. November des Folgejahres.

10. Der Exekutivdirektor übermittelt dem Rechnungshof zum 30. September des Jahres n+1 eine Antwort auf dessen Bemerkungen und leitet eine Kopie dieser Antwort auch dem Verwaltungsrat und der Kommission zu.

11. Der Exekutivdirektor übermittelt dem Europäischen Parlament auf dessen Anfrage nach Artikel 165 Absatz 3 der Haushaltsordnung alle Informationen, die für die ordnungsgemäße Abwicklung des Entlastungsverfahrens für das betreffende Haushaltsjahr erforderlich sind.

12. Auf Empfehlung des Rates erteilt das Europäische Parlament dem Direktor vor dem 15. Mai des Jahres n+2 Entlastung für die Ausführung des Haushaltsplans für das Jahr n.

Artikel 29
Finanzregelung

Der Verwaltungsrat erlässt nach Konsultation der Kommission die für die Agentur geltende Finanzregelung. Die Finanzregelung darf von der Delegierten Verordnung (EU) Nr. 1271/2013 nur abweichen, wenn dies für den Betrieb der Agentur eigens erforderlich ist und die Kommission vorher ihre Zustimmung erteilt hat.

Artikel 30
Betrugsbekämpfung

1. Zur Erleichterung der Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gemäß der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates[39] tritt die Agentur binnen sechs Monaten nach Aufnahme ihrer Tätigkeit der Interinstitutionellen Vereinbarung vom 25. Mai 1999 über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei und erlässt die einschlägigen Vorschriften, die für sämtliche Mitarbeiter der Agentur gelten, nach dem Muster im Anhang der genannten Vereinbarung.

2. Der Rechnungshof ist befugt, bei allen Empfängern von Finanzhilfen sowie bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel von der Agentur erhalten haben, Rechnungsprüfungen anhand von Unterlagen und vor Ort durchzuführen.

3. Das OLAF kann gemäß den Bestimmungen und Verfahren der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates und der 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 Union vor Betrug und anderen Unregelmäßigkeiten[40] Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob im Zusammenhang mit von der Agentur gewährten Finanzhilfen oder von ihr finanzierten Aufträgen ein Betrugs- oder Korruptionsdelikt oder eine sonstige rechtswidrige Handlung zum Nachteil der finanziellen Interessen der Union vorliegt.

4. Unbeschadet der Absätze 1, 2 und 3 müssen Kooperationsvereinbarungen mit Drittländern und internationalen Organisationen, Verträge, Finanzhilfevereinbarungen und Finanzhilfebeschlüsse der Agentur Bestimmungen enthalten, die den Rechnungshof und das OLAF ausdrücklich ermächtigen, derartige

---

39 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).

40 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).

Rechnungsprüfungen und Untersuchungen im Rahmen ihrer jeweiligen Zuständigkeiten durchzuführen.

KAPITEL IV
PERSONAL DER AGENTUR

Artikel 31
Allgemeine Bestimmungen

Für das Personal der Agentur gelten das Statut der Beamten, die Beschäftigungsbedingungen für die sonstigen Bediensteten und die im gegenseitigen Einvernehmen der Organe der Union erlassenen Regelungen zur Durchführung dieser Bestimmungen.

Artikel 32
Vorrechte und Befreiungen

Das dem Vertrag über die Europäische Union und dem AEUV beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union findet auf die Agentur und ihr Personal Anwendung.

Artikel 33
Exekutivdirektor

1. Der Exekutivdirektor wird als Zeitbediensteter der Agentur nach Artikel 2 Buchstabe a der Beschäftigungsbedingungen für die sonstigen Bediensteten eingestellt.
2. Der Exekutivdirektor wird vom Verwaltungsrat aus einer Liste von Kandidaten, die die Kommission im Anschluss an ein offenes und transparentes Auswahlverfahren vorgeschlagen hat, ernannt.
3. Beim Abschluss des Vertrags des Exekutivdirektors wird die Agentur durch den Vorsitzenden des Verwaltungsrats vertreten.
4. Vor der Ernennung wird der vom Verwaltungsrat ausgewählte Kandidat aufgefordert, eine Erklärung vor dem zuständigen Ausschuss des Europäischen Parlaments abzugeben und Fragen der Mitglieder zu beantworten.
5. Die Amtszeit des Exekutivdirektors beträgt fünf Jahre. Zum Ende dieses Zeitraums nimmt die Kommission eine Bewertung vor, bei der die Leistung des Exekutivdirektors und die künftigen Aufgaben und Herausforderungen der Agentur berücksichtigt werden.
6. Der Verwaltungsrat beschließt über die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors mit der Zweidrittelmehrheit seiner stimmberechtigten Mitglieder.
7. Der Verwaltungsrat kann auf Vorschlag der Kommission unter Berücksichtigung der Bewertung nach Absatz 5 die Amtszeit des Exekutivdirektors einmal um höchstens fünf Jahre verlängern.
8. Der Verwaltungsrat unterrichtet das Europäische Parlament über seine Absicht, die Amtszeit des Exekutivdirektors zu verlängern. Innerhalb von drei Monaten vor der

Verlängerung der Amtszeit gibt der Exekutivdirektor, sofern er dazu aufgefordert wird, vor dem zuständigen Ausschuss des Europäischen Parlaments eine Erklärung ab und beantwortet Fragen der Mitglieder.

9. Ein Exekutivdirektor, dessen Amtszeit verlängert wurde, darf nicht an einem anderen Auswahlverfahren für dieselbe Stelle teilnehmen.

10. Der Exekutivdirektor kann nur durch einen Beschluss des Verwaltungsrats auf Vorschlag der Kommission seines Amtes enthoben werden.

Artikel 34
Abgeordnete nationale Sachverständige und sonstiges Personal

1. Die Agentur kann auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht von der Agentur selbst beschäftigt wird. Für dieses Personal gelten das Statut der Beamten und die Beschäftigungsbedingungen für die sonstigen Bediensteten nicht.

2. Der Verwaltungsrat beschließt eine Regelung über zur Agentur abgeordnete nationale Sachverständige.

KAPITEL V
ALLGEMEINE BESTIMMUNGEN

Artikel 35
Rechtsform der Agentur

1. Die Agentur ist eine Einrichtung der Union und besitzt Rechtspersönlichkeit.

2. Die Agentur besitzt in jedem Mitgliedstaat die weitestgehende Rechts- und Geschäftsfähigkeit, die juristischen Personen nach einzelstaatlichem Recht zuerkannt ist. Sie kann insbesondere bewegliches und unbewegliches Vermögen erwerben oder veräußern und ist vor Gericht parteifähig, oder beides.

3. Die Agentur wird von ihrem Exekutivdirektor vertreten.

Artikel 36
Haftung der Agentur

1. Die vertragliche Haftung der Agentur bestimmt sich nach dem für den betreffenden Vertrag geltenden Recht.

2. Für Entscheidungen aufgrund einer Schiedsklausel in einem von der Agentur geschlossenen Vertrag ist der Gerichtshof der Europäischen Union zuständig.

3. Im Bereich der außervertraglichen Haftung ersetzt die Agentur den durch sie selbst oder ihre Bediensteten in Ausübung ihrer Tätigkeit verursachten Schaden nach den allgemeinen Grundsätzen, die den Rechtsordnungen der Mitgliedstaaten gemeinsam sind.

4. In Streitsachen über den Schadensersatz ist der Gerichtshof der Europäischen Union zuständig.

5. Die persönliche Haftung der Bediensteten gegenüber der Agentur bestimmt sich nach den für sie geltenden Beschäftigungsbedingungen.

Artikel 37
Sprachenregelung

1. Für die Agentur gilt die Verordnung Nr. 1 des Rates[41]. Die Mitgliedstaaten und die anderen von ihnen benannten Stellen können sich an die Agentur in einer Amtssprache der Organe der Union ihrer Wahl wenden und erhalten eine Antwort in dieser Sprache.

2. Die für die Arbeit der Agentur erforderlichen Übersetzungsdienste werden vom Übersetzungszentrum für die Einrichtungen der Europäischen Union erbracht.

Artikel 38
Schutz personenbezogener Daten

1. Die Verarbeitung personenbezogener Daten durch die Agentur unterliegt der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates[42].

2. Der Verwaltungsrat beschließt die Durchführungsbestimmungen nach Artikel 24 Absatz 8 der Verordnung (EG) Nr. 45/2001. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EG) Nr. 45/2001 durch die Agentur erforderlich sind, festlegen.

Artikel 39
Zusammenarbeit mit Drittländern und internationalen Organisationen

1. Die Agentur kann mit den zuständigen Behörden von Drittländern und mit internationalen Organisationen zusammenarbeiten, soweit dies zur Verwirklichung der Ziele dieser Verordnung erforderlich ist. Zu diesem Zweck kann die Agentur, nach vorheriger Genehmigung durch die Kommission, Arbeitsvereinbarungen mit den Behörden von Drittländern und internationalen Organisationen treffen. Diese Vereinbarungen begründen keine rechtlichen Verpflichtungen für die Union und ihre Mitgliedstaaten.

2. Die Agentur steht der Beteiligung von Drittländern offen, die entsprechende Übereinkünfte mit der Europäischen Union getroffen haben. Gemäß den einschlägigen Bestimmungen dieser Übereinkünfte werden Vereinbarungen getroffen, die insbesondere Art, Umfang und Form einer Beteiligung dieser Länder an der Tätigkeit der Agentur festlegen; hierzu zählen auch Bestimmungen über die Beteiligung an den von der Agentur durchgeführten Initiativen, finanzielle Beiträge und Personal. In Personalfragen müssen derartige Vereinbarungen in jedem Fall mit dem Beamtenstatut vereinbar sein.

3. Der Verwaltungsrat verabschiedet eine Strategie für die Beziehungen zu Drittländern oder internationalen Organisationen in Bezug auf Angelegenheiten, für die die

---

41 Verordnung Nr. 1 zur Regelung der Sprachenfrage für die Europäische Atomgemeinschaft (ABl. 17 vom 6.10.1958, S. 401).

42 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).

Agentur zuständig ist. Die Kommission stellt durch den Abschluss einer entsprechenden Arbeitsvereinbarung mit dem Exekutivdirektor der Agentur sicher, dass die Agentur im Rahmen ihres Mandats und des bestehenden institutionellen Rahmens handelt.

Artikel 40

Sicherheitsvorschriften für den Schutz von Verschlusssachen und nicht als Verschlusssache eingestuften vertraulichen Informationen

In Absprache mit der Kommission legt die Agentur die für sie geltenden Sicherheitsvorschriften fest, mit denen die in den Sicherheitsvorschriften der Kommission für den Schutz von Verschlusssachen der Europäischen Union und nicht als Verschlusssache eingestuften sensiblen Informationen enthaltenen Sicherheitsgrundsätze angewandt werden, die in den Beschlüssen (EU, Euratom) 2015/443 und 2015/444 festgelegt sind. Dies betrifft unter anderem die Bestimmungen über den Austausch, die Verarbeitung und die Speicherung derartiger Informationen.

Artikel 41

Sitzabkommen und Arbeitsbedingungen

1. Die notwendigen Regelungen über die Unterbringung der Agentur in dem Mitgliedstaat, in dem sie ihren Sitz hat, und über die Einrichtungen, die von diesem Mitgliedstaat zur Verfügung zu stellen sind, sowie die besonderen Vorschriften, die im Sitzmitgliedstaat der Agentur für den Exekutivdirektor, die Mitglieder des Verwaltungsrats, das Personal der Agentur und für Familienangehörige dieser Personen gelten, werden in einem Sitzabkommen festgelegt, das nach Billigung durch den Verwaltungsrat zwischen der Agentur und dem Sitzmitgliedstaat spätestens am [zwei Jahre nach Inkrafttreten dieser Verordnung] geschlossen wird.

2. Der Sitzmitgliedstaat der Agentur gewährleistet die bestmöglichen Voraussetzungen für das reibungslose Funktionieren der Agentur, einschließlich der Erreichbarkeit des Standortes, des Vorhandenseins adäquater Bildungseinrichtungen für die Kinder der Mitglieder des Personals und eines angemessenen Zugangs zu Arbeitsmarkt, Sozialversicherung und medizinischer Versorgung für Kinder und Ehegatten.

Artikel 42

Verwaltungskontrolle

Die Tätigkeit der Agentur unterliegt der Aufsicht des Bürgerbeauftragten nach Artikel 228 AEUV.

TITEL III
ZERTIFIZIERUNGSRAHMEN FÜR DIE CYBERSICHERHEIT

Artikel 43

Europäische Systeme für die Cybersicherheitszertifizierung

Ein europäisches System für die Cybersicherheitszertifizierung dient der Bescheinigung, dass die nach einem solchen System zertifizierten IKT-Produkte und -Dienste auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten Anforderungen an ihre Fähigkeit genügen, Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden.

Artikel 44

Ausarbeitung und Annahme eines europäischen Systems für die Cybersicherheitszertifizierung

1. Im Auftrag der Kommission arbeitet die ENISA ein mögliches europäisches System für die Cybersicherheitszertifizierung aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt. Die Mitgliedstaaten oder die nach Artikel 53 eingesetzte Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) kann der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

3. Die ENISA legt der Kommission das nach Absatz 2 ausgearbeitete mögliche europäische System für die Cybersicherheitszertifizierung vor.

4. Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems kann die Kommission nach Artikel 55 Absatz 2 Durchführungsrechtsakte erlassen, in denen für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

5. Die ENISA unterhält eine eigene Website, auf der sie über die europäischen Systeme für die Cybersicherheitszertifizierung informiert und für diese wirbt.

Artikel 45

Sicherheitsziele der europäischen Systeme für die Cybersicherheitszertifizierung

Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das – soweit zutreffend – den folgenden Sicherheitszielen Rechnung trägt:

(a) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden gegen eine zufällige oder unbefugte Speicherung, Verarbeitung oder Preisgabe sowie gegen einen zufälligen oder unbefugten Zugriff geschützt.

(b) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden gegen eine zufällige oder unbefugte Zerstörung, einen zufälligen Verlust oder eine zufällige Änderung geschützt.

(c) Es wird gewährleistet, dass befugte Personen, Programme oder Maschinen exklusiven Zugriff auf die Daten, Dienste oder Funktionen haben, zu denen sie zugangsberechtigt sind.

(d) Es wird protokolliert, welche Daten, Funktionen oder Dienste zu welchem Zeitpunkt von wem übermittelt bzw. genutzt worden sind.

(e) Es wird gewährleistet, dass überprüft werden kann, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt und von wem zugegriffen wurde oder wer zu welchem Zeitpunkt Daten, Dienste oder Funktionen genutzt hat.

(f) Bei einem physischen oder technischen Sicherheitsvorfall werden die Daten, Dienste und Funktionen zeitnah wieder verfügbar gemacht und der Zugang zu ihnen zeitnah wieder hergestellt.

(g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit aktueller Software, die keine bekannten Schwachstellen aufweist, bereitgestellt werden und mit Mechanismen für sichere Software-Updates ausgestattet sind.

Artikel 46

Vertrauenswürdigkeitsstufen der europäischen Systeme für die Cybersicherheitszertifizierung

1. Ein europäisches System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ angeben.

2. Die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ erfüllen jeweils folgende Kriterien:

(a) Die Vertrauenswürdigkeitsstufe „niedrig“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein begrenztes Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

(b) Die Vertrauenswürdigkeitsstufe „mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

(c) Die Vertrauenswürdigkeitsstufe „hoch“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „mittel“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Artikel 47

Elemente der europäischen Systeme für die Cybersicherheitszertifizierung

1. Ein europäisches System für die Cybersicherheitszertifizierung muss folgende Elemente enthalten:

(a) Gegenstand und Umfang der Zertifizierung, darunter auch Art oder Kategorie der erfassten IKT-Produkte und -Dienste;

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen IKT-Produkte und -Dienste geprüft werden, z. B. durch die Bezugnahme auf europäische oder internationale Normen oder technische Spezifikationen;

(c) gegebenenfalls eine oder mehrere Vertrauenswürdigkeitsstufen;

(d) besondere Bewertungskriterien und -methoden sowie Bewertungsarten für den Nachweis, dass die in Artikel 45 festgelegten Ziele eingehalten werden;

(e) für die Zertifizierung erforderliche Informationen, die ein Antragsteller der Konformitätsbewertungsstelle vorzulegen hat;

(f) Bedingungen für die Verwendung von Siegeln oder Kennzeichen, sofern das System solche vorsieht;

(g) Vorschriften für die Überwachung der Einhaltung der mit dem Zertifikat verbundenen Anforderungen, sofern das System eine Aufsicht vorsieht, einschließlich der Mechanismen für den Nachweis der fortgesetzten Einhaltung der festgelegten Cybersicherheitsanforderungen;

(h) Bedingungen für die Gewährung, Aufrechterhaltung, Fortführung, Ausweitung und Verringerung des Zertifizierungsumfangs;

(i) Vorschriften, die greifen, wenn die zertifizierten IKT-Produkte und -Dienste den Zertifizierungsanforderungen nicht genügen;

(j) Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen von IKT-Produkten und -Diensten;

(k) Vorschriften für die Konformitätsbewertungsstellen über die Aufbewahrung von Aufzeichnungen;

(l) Angabe nationaler Systeme für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten und -Diensten;

(m) Inhalt der ausgestellten Zertifikate.

2. Die für das System festgelegten Anforderungen dürfen in keinem Widerspruch zu geltenden rechtlichen Anforderungen stehen, vor allem nicht zu solchen Anforderungen, die sich aus harmonisiertem Unionsrecht ergeben.

3. Soweit dies in einem Rechtsakt der Union so festgelegt ist, kann eine Zertifizierung auf der Grundlage eines europäischen Systems für die Cybersicherheitszertifizierung für den Nachweis der Konformitätsvermutung mit den Anforderungen jenes Rechtsakts verwendet werden.

4. Mangels harmonisierter Rechtsvorschriften der Union kann auch ein Mitgliedstaat festlegen, dass ein europäisches System für die Cybersicherheitszertifizierung für die Feststellung der Konformitätsvermutung mit den rechtlichen Anforderungen verwendet werden kann.

Artikel 48
Cybersicherheitszertifizierung

1. Für IKT-Produkte und -Dienste, die auf der Grundlage eines nach Artikel 44 angenommenen europäischen Systems für die Cybersicherheitszertifizierung zertifiziert wurden, gilt die Vermutung der Konformität mit den Anforderungen dieses Systems.

2. Die Zertifizierung ist freiwillig, sofern nicht anderweitig im Unionsrecht festgelegt.

3. Ein europäisches Cybersicherheitszertifikat nach diesem Artikel wird von den in Artikel 51 genannten Konformitätsbewertungsstellen auf der Grundlage der Kriterien des nach Artikel 44 angenommenen europäischen Systems für die Cybersicherheitszertifizierung ausgestellt.

4. Abweichend von Absatz 3 kann in hinreichend begründeten Fällen ein einzelnes europäisches System für die Cybersicherheitszertifizierung vorsehen, dass ein im Rahmen dieses Systems erteiltes europäisches Cybersicherheitszertifikat nur von einer öffentlichen Stelle ausgestellt werden kann. Bei einer solchen öffentlichen Stelle muss es sich um eine der folgenden Stellen handeln:

   (a) eine nationale Aufsichtsbehörde für die Zertifizierung nach Artikel 50 Absatz 1;

   (b) eine als Konformitätsbewertungsstelle akkreditierte Stelle nach Artikel 51 Absatz 1 oder

   (c) eine auf der Grundlage von Rechtsvorschriften, Rechtsverordnungen oder sonstigen amtlichen Verwaltungsverfahren eines Mitgliedstaats eingesetzte Stelle, die die Anforderungen an die Stellen erfüllt, die Produkte, Verfahren und Dienste nach ISO/IEC 17065:2012 zertifizieren.

5. Die natürliche oder juristische Person, die ihre IKT-Produkte oder -Dienste zur Zertifizierung einreicht, hat der in Artikel 51 genannten Konformitätsbewertungsstelle alle für das Zertifizierungsverfahren notwendigen Informationen vorzulegen.

6. Zertifikate werden für eine Höchstdauer von drei Jahren erteilt und können unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden.

7. Ein nach diesem Artikel ausgestelltes europäisches Cybersicherheitszertifikat wird in allen Mitgliedstaaten anerkannt.

Artikel 49

Nationale Cybersicherheitszertifizierungssysteme und Cybersicherheitszertifikate

1. Unbeschadet des Absatzes 3 werden nationale Systeme für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam, der in dem nach Artikel 44 Absatz 4 erlassenen Durchführungsrechtsakt festgelegt ist. Bereits vorhandene nationale Systeme für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte und -Dienste, die nicht unter ein europäisches System für die Cybersicherheitszertifizierung fallen, bleiben bestehen.
2. Die Mitgliedstaaten führen keine neuen nationalen Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten ein, die unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.
3. Vorhandene Zertifikate, die auf der Grundlage nationaler Systeme für die Cybersicherheitszertifizierung ausgestellt wurden, bleiben bis zum Ende ihrer Geltungsdauer gültig.

Artikel 50

Nationale Aufsichtsbehörden für die Zertifizierung

1. Jeder Mitgliedstaat benennt eine nationale Aufsichtsbehörde für die Zertifizierung.
2. Jeder Mitgliedstaat teilt der Kommission den Namen der benannten Behörde mit.
3. Jede nationale Aufsichtsbehörde für die Zertifizierung ist im Hinblick auf ihre Organisation, Finanzierungsentscheidungen, Rechtsform und Entscheidungsfindung unabhängig von den Stellen, die sie beaufsichtigt.
4. Die Mitgliedstaaten sorgen für eine angemessene Ausstattung der nationalen Aufsichtsbehörden für die Zertifizierung, damit diese ihre Befugnisse ausüben und die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen können.
5. Im Hinblick auf eine wirksame Durchführung dieser Verordnung sollten diese Behörden in der nach Artikel 53 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung in aktiver, wirksamer, effizienter und sicherer Weise mitarbeiten.
6. Die nationalen Aufsichtsbehörden für die Zertifizierung haben folgende Aufgaben:
   (a) Überwachung und Durchsetzung der in diesem Titel genannten Bestimmungen auf nationaler Ebene und Beaufsichtigung der Übereinstimmung der von den in ihrem jeweiligen Hoheitsgebiet ansässigen Konformitätsbewertungsstellen ausgestellten Zertifikate mit den in diesem Titel und in dem entsprechenden europäischen System für die Cybersicherheitszertifizierung genannten Anforderungen;
   (b) Überwachung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen für die Zwecke dieser Verordnung, auch in

Bezug auf deren Notifizierung und die in Artikel 52 genannten einschlägigen Aufgaben;

(c) Bearbeitung von Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf Zertifikate eingereicht werden, die von Konformitätsbewertungsstellen in ihrem Hoheitsgebiet ausgestellt wurden, Untersuchung des Beschwerdegegenstands, soweit angemessen, und Unterrichtung des Beschwerdeführers über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist;

(d) Zusammenarbeit mit anderen nationalen Aufsichtsbehörden für die Zertifizierung und anderen öffentlichen Stellen; dies beinhaltet auch den Informationsaustausch über die etwaige Nichtkonformität von IKT-Produkten und -Diensten mit den Anforderungen dieser Verordnung oder bestimmten europäischen Systemen für die Cybersicherheitszertifizierung;

(e) Verfolgung einschlägiger Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung.

7. Jede nationale Aufsichtsbehörde für die Zertifizierung hat mindestens die folgenden Befugnisse:

(a) Sie kann Konformitätsbewertungsstellen und die Inhaber europäischer Cybersicherheitszertifikate auffordern, ihr sämtliche Auskünfte zu erteilen, die sie für die Erfüllung ihrer Aufgaben benötigt;

(b) sie kann Untersuchungen in Form von Rechnungsprüfungen bei Konformitätsbewertungsstellen und Inhabern europäischer Cybersicherheitszertifikate durchführen, um die Einhaltung der Bestimmungen des Titels III zu überprüfen;

(c) sie kann im Einklang mit einzelstaatlichem Recht geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Konformitätsbewertungsstellen oder die Inhaber von Zertifikaten den Anforderungen dieser Verordnung oder eines europäischen Systems für die Cybersicherheitszertifizierung genügen;

(d) sie erhält Zugang zu den Räumlichkeiten von Konformitätsbewertungsstellen und von Inhabern europäischer Cybersicherheitszertifikate zum Zweck der Durchführung von Untersuchungen im Einklang mit den Verfahrensvorschriften der Union oder des Mitgliedstaats;

(e) sie kann im Einklang mit einzelstaatlichem Recht Zertifikate widerrufen, die den Anforderungen dieser Verordnung oder eines europäischen Systems für die Cybersicherheitszertifizierung nicht genügen;

(f) sie kann nach Artikel 54 und im Einklang mit einzelstaatlichem Recht Strafen verhängen und die unverzügliche Beendigung der Verletzung der in dieser Verordnung festgelegten Verpflichtungen anordnen.

8. Die nationalen Aufsichtsbehörden für die Zertifizierung arbeiten untereinander und mit der Kommission zusammen und tauschen insbesondere Informationen, Erfahrungen und bewährte Verfahren im Zusammenhang mit der Cybersicherheitszertifizierung und technischen Fragen in Bezug auf die Cybersicherheit von IKT-Produkten und -Diensten aus.

Artikel 51

Konformitätsbewertungsstellen

1. Die Konformitätsbewertungsstellen werden von den nach der Verordnung (EG) Nr. 765/2008 benannten nationalen Akkreditierungsstellen nur dann akkreditiert, wenn sie die im Anhang dieser Verordnung aufgeführten Anforderungen erfüllen.

2. Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die Konformitätsbewertungsstelle die Anforderungen dieses Artikels erfüllt. Die Akkreditierungsstellen widerrufen die einer Konformitätsbewertungsstelle nach Absatz 1 erteilte Akkreditierung, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

Artikel 52

Notifizierung

1. Für jedes nach Artikel 44 angenommene europäische System für die Cybersicherheitszertifizierung notifizieren die nationalen Aufsichtsbehörden für die Zertifizierung der Kommission die Konformitätsbewertungsstellen, die für die Erteilung von Zertifikaten entsprechend den in Artikel 46 genannten Vertrauenswürdigkeitsstufen akkreditiert wurden, sowie unverzüglich etwaige diesbezügliche Änderungen.

2. Ein Jahr nach Inkrafttreten eines europäischen Systems für die Cybersicherheitszertifizierung veröffentlicht die Kommission im *Amtsblatt der Europäischen Union* eine Liste der notifizierten Konformitätsbewertungsstellen.

3. Geht der Kommission nach Ablauf der in Absatz 2 genannten Frist eine Notifizierung zu, so veröffentlicht sie die Änderungen an der in Absatz 2 genannten Liste innerhalb von zwei Monaten ab dem Zeitpunkt des Eingangs dieser Notifizierung im *Amtsblatt der Europäischen Union*.

4. Eine nationale Aufsichtsbehörde für die Zertifizierung kann bei der Kommission die Streichung einer von dieser Aufsichtsbehörde notifizierten Konformitätsbewertungsstelle aus der in Absatz 2 genannten Liste beantragen. Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* die entsprechenden Änderungen der Liste innerhalb eines Monats ab dem Zeitpunkt, zu dem der Antrag der nationalen Aufsichtsbehörde für die Zertifizierung eingegangen ist.

5. Die Kommission kann im Wege von Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Notifizierungen nach Absatz 1 festlegen. Diese Durchführungsrechtsakte werden nach dem in Artikel 55 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 53

Europäische Gruppe für die Cybersicherheitszertifizierung

1. Die Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) wird eingesetzt.

2. Die Gruppe setzt sich aus den nationalen Aufsichtsbehörden für die Zertifizierung zusammen. Die nationalen Aufsichtsbehörden für die Zertifizierung werden durch ihre Leiter oder durch andere hochrangige Vertreter vertreten.

3. Die Gruppe hat folgende Aufgaben:

   (a) Sie berät und unterstützt die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung dieses Titels, insbesondere in politischen Fragen der Cybersicherheitszertifizierung, bei der Koordinierung von Politikkonzepten und bei der Ausarbeitung europäischer Systeme für die Cybersicherheitszertifizierung;

   (b) sie unterstützt und berät die ENISA bei der Ausarbeitung eines möglichen Systems nach Artikel 44 und arbeitet hierbei mit der ENISA zusammen;

   (c) sie schlägt der Kommission vor, die Agentur mit der Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung nach Artikel 44 zu beauftragen;

   (d) sie gibt an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung vorhandener europäischer Systeme für die Cybersicherheitszertifizierung ab;

   (e) sie prüft die einschlägigen Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung und tauscht Informationen über bewährte Verfahren für Cybersicherheitszertifizierungssysteme aus;

   (f) sie erleichtert im Wege eines Informationsaustauschs die Zusammenarbeit zwischen den nationalen Aufsichtsbehörden für die Zertifizierung nach diesem Titel, vor allem durch die Festlegung von Methoden für einen effizienten Austausch von Informationen über alle Fragen der Cybersicherheitszertifizierung.

4. Die Kommission führt den Vorsitz der Gruppe und nimmt mit Unterstützung der ENISA nach Artikel 8 Buchstabe a deren Sekretariatsgeschäfte wahr.

Artikel 54
Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diesen Titel und die europäischen Systeme für die Cybersicherheitszertifizierung zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen [bis zum .... /unverzüglich] mit und melden ihr etwaige spätere Änderungen.

TITEL IV
SCHLUSSBESTIMMUNGEN

Artikel 55
Ausschussverfahren

1. Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

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

Artikel 56
Bewertung und Überarbeitung

1. Spätestens fünf Jahre nach dem in Artikel 58 genannten Zeitpunkt und danach alle fünf Jahre bewertet die Kommission die Wirkung, Wirksamkeit und Effizienz der Agentur und ihrer Arbeitsmethoden und prüft, ob das Mandat der Agentur möglicherweise geändert werden muss und welche finanziellen Auswirkungen eine solche Änderung hätte. In der Bewertung werden alle Rückmeldungen an die Agentur in Bezug auf ihre Tätigkeiten berücksichtigt. Gelangt die Kommission zu der Auffassung, dass Ziele, Mandat und Aufgaben der Agentur deren Fortbestehen nicht länger rechtfertigen, kann sie eine Änderung dieser Verordnung im Hinblick auf die für die Agentur geltenden Bestimmungen vorschlagen.

2. Die Bewertung erstreckt sich auch auf die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels III im Hinblick auf die Ziele, für IKT-Produkte und -Dienste in der Union ein angemessenes Maß an Cybersicherheit und einen besser funktionierenden Binnenmarkt zu gewährleisten.

3. Die Kommission übermittelt den Bewertungsbericht zusammen mit ihren Schlussfolgerungen dem Europäischen Parlament, dem Rat und dem Verwaltungsrat. Die Ergebnisse des Bewertungsberichts werden öffentlich bekannt gemacht.

Artikel 57
Aufhebung und Rechtsnachfolge

1. Die Verordnung (EG) Nr. 526/2013 wird mit Wirkung vom [...] aufgehoben.

2. Bezugnahmen auf die Verordnung (EG) Nr. 526/2013 und auf die ENISA gelten als Bezugnahmen auf diese Verordnung und auf die Agentur.

3. Die Agentur ist in Bezug auf das Eigentum und alle Übereinkünfte, rechtlichen Verpflichtungen, Beschäftigungsverträge, finanziellen Verpflichtungen und Verbindlichkeiten Rechtsnachfolger der durch die Verordnung (EG) Nr. 526/2013 errichteten Agentur. Alle vom Verwaltungsrat und vom Exekutivrat getroffenen Entscheidungen bleiben gültig, sofern sie den Bestimmungen dieser Verordnung nicht zuwiderlaufen.

4. Die Agentur wird zum [...] auf unbegrenzte Zeit errichtet.

5. Der nach Artikel 24 Absatz 4 der Verordnung (EG) Nr. 526/2013 ernannte Exekutivdirektor bleibt für die restliche Dauer seiner Amtszeit der Exekutivdirektor der Agentur.

6. Die nach Artikel 6 der Verordnung (EG) Nr. 526/2013 ernannten Mitglieder des Verwaltungsrats und ihre Stellvertreter bleiben für die restliche Dauer ihrer Amtszeit Mitglieder des Verwaltungsrats der Agentur und deren Stellvertreter.

Artikel 58

Inkrafttreten

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

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

Geschehen zu Brüssel am […]

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

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“).

1.2. Politikbereich(e)

Politikbereich: 09 - Kommunikationsnetze, Inhalte und Technologien

Aktivität: 09 02 - Digitaler Binnenmarkt

1.3. Art des Vorschlags/der Initiative

☒ Der Vorschlag/Die Initiative betrifft **eine neue Maßnahme (Titel III – Zertifizierung)**

☐ Der Vorschlag/Die Initiative betrifft **eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**[43]

☒ Der Vorschlag/Die Initiative betrifft **die Verlängerung einer bestehenden Maßnahme (Titel II – Mandat der ENISA)**

☐ Der Vorschlag/Die Initiative betrifft **eine neu ausgerichtete Maßnahme**

1.4. Ziel(e)

1.4.1. Mit dem Vorschlag/der Initiative verfolgte mehrjährige strategische Ziele der Kommission

1. Verbesserung der Abwehrfähigkeit der Mitgliedstaaten, der Unternehmen und der EU insgesamt

2. Gewährleistung des ordnungsgemäßen Funktionierens des EU-Binnenmarktes für IKT-Produkte und -Dienste

3. Steigerung der globalen Wettbewerbsfähigkeit von im IKT-Bereich tätigen Unternehmen in der EU.

4. Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, die Cybersicherheit benötigen

1.4.2. Einzelziel(e)

Unter Berücksichtigung der allgemeinen Ziele im umfassenderen Kontext der überarbeiteten Cybersicherheitsstrategie sollen durch die genauere Festlegung des Zuständigkeitsbereichs und des Mandats der ENISA und durch die Schaffung eines europäischen Zertifizierungsrahmens für IKT-Produkte und -Dienste die folgenden spezifischen Ziele erreicht werden:

1. Ausbau der **Kapazitäten und der Abwehrbereitschaft** der Mitgliedstaaten und Unternehmen
2. Verbesserung der **Zusammenarbeit und der Koordinierung** zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU
3. Ausbau der **Kapazitäten auf EU-Ebene, um die Maßnahmen der**

[43] Im Sinne des Artikels 54 Absatz 2 Buchstabe a oder b der Haushaltsordnung.

Mitgliedstaaten zu ergänzen, insbesondere im Fall von grenzüberschreitenden Cyberkrisen.

4. Stärkere **Sensibilisierung** der Bürger und Unternehmen für Fragen der Cybersicherheit.
5. Stärkung des Vertrauens in den digitalen Binnenmarkt und in digitale Innovationen durch die Verbesserung der allgemeinen Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit[44] von IKT-Produkten und -Diensten.

Die ENISA wird zur Erreichung der oben genannten Ziele beitragen durch Folgendes:

Verstärkte Unterstützung der Politikgestaltung – Bereitstellung von Orientierungshilfen und Beratung der Kommission und der Mitgliedstaaten bei der Aktualisierung und Weiterentwicklung eines zusammenhängenden Regelungsrahmens im Bereich der Cybersicherheit sowie sektorspezifischer politischer und rechtlicher Initiativen, bei denen es um Fragen der Cybersicherheit geht; Beitrag zur Arbeit der Kooperationsgruppe (Artikel 11 der Richtlinie (EU) 2016/1148) durch die Bereitstellung von Kompetenz und Unterstützung; Unterstützung der Entwicklung und der Umsetzung von Politik im Bereich der elektronischen Identität und Vertrauensdienste; Förderung des Austauschs bewährter Verfahren zwischen den zuständigen Behörden;

Verstärkte Unterstützung des Kapazitätsaufbaus – Unterstützung der Mitgliedstaaten, der Organe, Einrichtungen und sonstigen Stellen der Union, um die Prävention, Erkennung und Analyse von Cybersicherheitsproblemen und -Vorfällen sowie die Fähigkeit, darauf zu reagieren, weiterzuentwickeln und zu verbessern; Unterstützung der Mitgliedstaaten, auf deren Ersuchen hin, beim Aufbau nationaler Computer-Notfallteams und bei der Ausarbeitung nationaler Cybersicherheitsstrategien; Unterstützung der Organe der Union bei der Ausarbeitung und Überprüfung der Cybersicherheitsstrategien der Union; Veranstaltung von Fortbildungen zur Cybersicherheit; Unterstützung der Mitgliedstaaten beim Austausch bewährter Verfahren im Rahmen der Kooperationsgruppe; Erleichterung des Aufbaus sektorbezogener Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISAC);

Unterstützung der operativen Zusammenarbeit und des Krisenmanagements – Unterstützung der Zusammenarbeit zwischen den zuständigen öffentlichen Stellen sowie zwischen den Interessenträgern durch die Einführung einer systematischen Zusammenarbeit mit den Organen, Einrichtungen und sonstigen Stellen der Union, die sich mit Cybersicherheit, Cyberkriminalität und dem Schutz der Privatsphäre sowie personenbezogener Daten befassen; Führung der Sekretariatsgeschäfte des CSIRTs-Netzes (Artikel 12 Absatz 2 der Richtlinie (EU) 2016/1148) und Beitrag zur operativen Zusammenarbeit innerhalb des Netzes, indem die Mitgliedstaaten auf deren Ersuchen hin in Zusammenarbeit mit dem CERT-EU unterstützt werden; Veranstaltung regelmäßiger Übungen zur Cybersicherheit; Beitrag zur Ausarbeitung einer auf Kooperation beruhenden Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß; Durchführung nachträglicher technischer Untersuchungen signifikanter

[44] Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit bedeutet, dass den Nutzern ausreichende Informationen über die Cybersicherheitseigenschaften bereitgestellt werden, um das Sicherheitsniveau eines bestimmten IKT-Produkts, eines bestimmten IKT-Dienstes oder eines bestimmten IKT-Verfahrens objektiv feststellen zu können.

Sicherheitsvorfälle – in Zusammenarbeit mit dem CSIRTs-Netz – und Abgabe von Empfehlungen für das weitere Vorgehen;

Marktbezogene Aufgaben (Normung, Zertifizierung) – Wahrnehmung einer Reihe von Aufgaben, die speziell den Binnenmarkt stärken: Cybersicherheits-„Marktbeobachtungsstelle“, die einschlägige Trends auf dem Cybersicherheitsmarkt analysiert, um Angebot und Nachfrage besser aufeinander abzustimmen; Unterstützung und Förderung der Entwicklung und Umsetzung der Unionspolitik im Bereich der Cybersicherheitszertifizierung von IKT-Produkten und -Diensten durch die Ausarbeitung möglicher europäischer Cybersicherheitszertifizierungssysteme für IKT-Produkte und -Dienste, Führung der Sekretariatsgeschäfte für die Gruppe für die Cybersicherheitszertifizierung in der Union, Bereitstellung von Leitlinien und bewährten Verfahren für Sicherheitsanforderungen an IKT-Produkte und -Dienste in Zusammenarbeit mit den nationalen Zertifizierungsaufsichtsbehörden und der Industrie; **Unterstützung der Verbesserung der Wissensgrundlage, Information und Sensibilisierung** – Hilfestellung und Beratung für die Kommission und die Mitgliedstaaten, damit diese in Fragen der Netz- und Informationssicherheit und ihrer Anwendung auf die Interessenträger der Branche unionsweit einen hohen Wissensstand erreichen. Dies setzt auch voraus, dass Informationen über die Sicherheit von Netz- und Informationssystemen [oder über die Cybersicherheit] zusammengeführt, aufbereitet und der Öffentlichkeit über ein spezielles Portal zur Verfügung gestellt werden. Ein weiteres wichtiges Element sind an die breite Öffentlichkeit gerichtete Sensibilisierungsmaßnahmen und Informationskampagnen zu Cybersicherheitsrisiken.

Verstärkte Förderung von Forschung und Innovation – Beratung zum Forschungsbedarf und zur Prioritätensetzung im Bereich der Cybersicherheit;

Unterstützung der internationalen Zusammenarbeit – Unterstützung der Bemühungen der Union um Zusammenarbeit mit Drittländern und internationalen Organisationen zur Förderung der internationalen Zusammenarbeit auf dem Gebiet der Cybersicherheit.

ZERTIFIZIERUNG

Der Zertifizierungsrahmen wird zum Erreichen der Ziele beitragen durch die Verbesserung der allgemeinen Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit[45] von IKT-Produkten und -Diensten, um das Vertrauen in den digitalen Binnenmarkt und in digitale Innovationen zu stärken. Dies sollte auch dazu beitragen, ein Nebeneinander unterschiedlicher Zertifizierungssysteme in der EU und der damit verbundenen Sicherheitsanforderungen und Bewertungskriterien in den einzelnen Mitgliedstaaten und Sektoren zu vermeiden.

1.4.3. Erwartete Ergebnisse und Auswirkungen

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

Eine gestärkte ENISA (die die Kapazitäten, Prävention, Zusammenarbeit und Sensibilisierung auf EU-Ebene unterstützt und daher so ausgestaltet ist, dass sie die Abwehrfähigkeit gegenüber Cyberangriffen in der EU insgesamt verbessert) sowie die

[45] Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit bedeutet, dass den Nutzern ausreichende Informationen über die Cybersicherheitseigenschaften bereitgestellt werden, um das Sicherheitsniveau eines bestimmten IKT-Produkts, eines bestimmten IKT-Dienstes oder eines bestimmten IKT-Verfahrens objektiv feststellen zu können.

Unterstützung des EU-Zertifizierungsrahmens für IKT-Produkte und -Dienste wird voraussichtlich folgende Auswirkungen haben (nicht erschöpfende Liste):

Gesamtauswirkungen

- Insgesamt positive Auswirkungen auf den Binnenmarkt infolge eines weniger fragmentierten Marktes und der Stärkung des Vertrauens in die digitale Technik durch eine bessere Zusammenarbeit, stärker harmonisierte Ansätze bei den EU-Cybersicherheitsstrategien und mehr Kapazitäten auf EU-Ebene. Indem ein Beitrag zur Senkung der Cybersicherheits-/Cyberkriminalitätskosten geleistet wird, deren wirtschaftliche Folgen in der Union auf 0,41 % des BIP der EU (etwa 55 Milliarden EUR) geschätzt werden, dürfte die Initiative sich wirtschaftlich insgesamt positiv auswirken.

Konkrete Ergebnisse

Größere Kapazitäten und Abwehrbereitschaft der Mitgliedstaaten und Unternehmen im Bereich der Cybersicherheit

- Größere Kapazitäten und Abwehrbereitschaft der Mitgliedstaaten im Bereich der Cybersicherheit (die auf langfristige strategische Analysen von Cyberbedrohungen und Cybersicherheitsvorfällen, auf Leitlinien und Berichte, auf die Vermittlung von Fachwissen und bewährten Verfahren, auf die Verfügbarkeit von Fortbildungen und Fortbildungsmaterial und auf intensivere CyberEurope-Übungen zurückgehen)

- Bessere Fähigkeiten der privaten Akteure, die auf die Unterstützung beim Aufbau von Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISAC) in verschiedenen Sektoren zurückzuführen sind

- Größere Abwehrbereitschaft der EU und der Mitgliedstaaten im Bereich der Cybersicherheit, da gut eingespielte, vereinbarte Pläne für den Fall grenzüberschreitender Cybersicherheitsvorfälle von großem Ausmaß vorliegen, die bei CyberEurope-Übungen getestet wurden;

Bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU

- Bessere Zusammenarbeit sowohl innerhalb des öffentlichen und des privaten Sektors als auch zwischen dem öffentlichen und dem privaten Sektor;

- Größere Kohärenz bei der grenz- und sektorenübergreifenden Herangehensweise an die Umsetzung der NIS-Richtlinie;

- Bessere Zusammenarbeit im Bereich der Zertifizierung dank eines institutionellen Rahmens, der die Entwicklung europäischer Cybersicherheitszertifizierungssysteme und die Entwicklung einer gemeinsamen Politik auf diesem Gebiet ermöglicht.

Mehr Kapazitäten auf EU-Ebene, um die Maßnahmen der Mitgliedstaaten zu ergänzen

- Bessere „operative Kapazität der EU“, um die Maßnahmen der Mitgliedstaaten zu ergänzen und sie, auf ihr Ersuchen hin, bei begrenzten und vorab festgelegten Diensten zu unterstützen. Dies wird sich auf den Erfolg der Prävention und der Feststellung von Sicherheitsvorfällen sowie der Reaktion darauf sowohl auf der Ebene der Mitgliedstaaten und als auch auf Unionsebene voraussichtlich positiv auswirken.

Stärkere Sensibilisierung der Bürger und Unternehmen für Fragen der Cybersicherheit

- Größeres allgemeines Problembewusstsein bei Bürgern und Unternehmen bezüglich Fragen der Cybersicherheit

- Bessere Fähigkeit, beim Kauf von IKT-Produkten und -Diensten aufgrund der Cybersicherheitszertifizierung fundierte Entscheidungen zu treffen

Größeres Vertrauen in den digitalen Binnenmarkt und in digitale Innovationen durch mehr Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit von IKT-Produkten und -Diensten

- Mehr Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit[46] von IKT-Produkten und -Diensten dank einfacherer Verfahren für die Sicherheitszertifizierung durch einen EU-weiten Rahmen

- Größere Vertrauenswürdigkeit hinsichtlich der Sicherheitsmerkmale von IKT-Produkten und -Diensten

- Größere Verbreitung der Sicherheitszertifizierung, für die Anreize gesetzt werden durch vereinfachte Verfahren, geringere Kosten und die Perspektive EU-weiter Geschäftsmöglichkeiten, die nicht durch eine Fragmentierung des Marktes behindert werden

- Verbesserte Wettbewerbsfähigkeit innerhalb des Cybersicherheitsmarktes in der EU aufgrund von niedrigeren Kosten und eines geringeren Verwaltungsaufwands für KMU und der Beseitigung potenzieller Marktzugangshemmnisse in Form von zahlreichen nationalen Zertifizierungssystemen

Sonstige

- Für keines der Ziele wird mit signifikanten ökologischen Auswirkungen gerechnet.

- Für den EU-Haushalt sind Effizienzgewinne infolge einer verstärkte Zusammenarbeit und Koordinierung der Tätigkeiten zwischen den Organen, Einrichtungen und sonstigen Stellen der EU zu erwarten.

1.4.4. Leistungs- und Erfolgsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Realisierung des Vorschlags/der Initiative verfolgen lässt.

(a)

Ziel: Ausbau der Kapazitäten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen:

- Anzahl der von der ENISA organisierten Fortbildungen
- Geografische Abdeckung der von der ENISA geleisteten direkten Unterstützung (Anzahl der Länder und Gebiete)
- Niveau der Abwehrbereitschaft der Mitgliedstaaten hinsichtlich der Ausgereiftheit der CSIRTs und der Überwachung von cybersicherheitsbezogenen Regulierungsmaßnahmen
- Anzahl der von der ENISA bereitgestellten Verfahren für kritische Infrastrukturen, die sich unionsweit bewährt haben
- Anzahl der von der ENISA bereitgestellten Verfahren für KMU, die sich unionsweit bewährt haben

[46] Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit bedeutet, dass den Nutzern ausreichende Informationen über die Cybersicherheitseigenschaften bereitgestellt werden, um das Sicherheitsniveau eines bestimmten IKT-Produkts, eines bestimmten IKT-Dienstes oder eines bestimmten IKT-Verfahrens objektiv feststellen zu können.

- Veröffentlichung jährlicher strategischer Analysen von Cyberbedrohungen und Cybersicherheitsvorfällen durch die ENISA, um neu aufkommende Trends zu erkennen
- Regelmäßiger Beitrag der ENISA zur Arbeit der Cybersicherheit-Arbeitsgruppen der europäischen Normungsorganisationen.

Ziel: Verbesserung der Zusammenarbeit und der Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU:

- Anzahl der Mitgliedstaaten, die Empfehlungen und Stellungnahmen der ENISA in ihre politischen Entscheidungsprozesse einbezogen haben
- Anzahl der Organe, Einrichtungen und sonstigen Stellen der EU, die Empfehlungen und Stellungnahmen der ENISA in ihre politischen Entscheidungsprozesse einbezogen haben
- Regelmäßige Ausführung des Arbeitsprogramms des CSIRTs-Netzes sowie gutes Funktionieren der IT-Infrastruktur und der Kommunikationskanäle des CSIRTs-Netzes
- Anzahl der technischen Berichte, die der Kooperationsgruppe zur Verfügung gestellt und von ihr genutzt werden
- Kohärenter Ansatz bei der grenz- und sektorenübergreifenden Durchführung der NIS-Richtlinie
- Anzahl der von der ENISA durchgeführten Bewertungen der Einhaltung der Rechtsvorschriften
- Anzahl der in verschiedenen Sektoren - insbesondere für kritische Infrastrukturen - vorhandenen ISAC
- Einrichtung und regelmäßiger Betrieb von Informationsplattformen für die Verbreitung von Informationen zur Cybersicherheit, die von Organen, Einrichtungen und sonstigen Stellen der EU stammen
- Regelmäßiger Beitrag zur Ausarbeitung der EU-Arbeitsprogramme für Forschung und Innovation
- Abschluss einer Vereinbarung über die Zusammenarbeit zwischen der ENISA, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und dem CERT-EU
- Anzahl der Zertifizierungssysteme, die im Rahmen enthalten sind und gemäß dem Rahmen entwickelt wurden

Ziel: Ausbau der Kapazitäten auf EU-Ebene, um die Maßnahmen der Mitgliedstaaten zu ergänzen, insbesondere im Fall von grenzüberschreitenden Cyberkrisen:

- Veröffentlichung jährlicher strategischer Analysen von Cyberbedrohungen und Cybersicherheitsvorfällen durch die ENISA, um neu aufkommende Trends zu erkennen
- Veröffentlichung aggregierter Informationen über Sicherheitsvorfälle, die von der ENISA im Rahmen der NIS-Richtlinie gemeldet werden
- Anzahl der von der Agentur koordinierten europaweiten Übungen und Anzahl der beteiligten Mitgliedstaaten und Organisationen
- Anzahl der von den Mitgliedstaaten an die ENISA gerichteten Ersuchen um

Unterstützung bei der Reaktion auf Notfälle, die von der Agentur bearbeitet wurden

- Anzahl der Analysen zu Anfälligkeiten, Artefakten und Sicherheitsvorfällen, die von der ENISA in Zusammenarbeit mit dem CERT-EU durchgeführt wurden
- Verfügbarkeit von EU-weiten Lageberichten, die auf Informationen beruhen, die der ENISA von den Mitgliedstaaten und anderen Stellen im Fall von grenzüberschreitenden Cybersicherheitsvorfällen von großem Ausmaß zur Verfügung gestellt werden.

Ziel: Stärkere Sensibilisierung der Bürger und Unternehmen für Fragen der Cybersicherheit:

- Regelmäßige Durchführung von EU-weiten und nationalen Sensibilisierungskampagnen und regelmäßige Aktualisierung der Themen entsprechend dem neuen Lernbedarf
- Stärkere Sensibilisierung der Bürgerinnen und Bürger der EU für Fragen der Cybersicherheit
- Regelmäßige Durchführung eines Quiz zur Cybersicherheit mit dem Ziel, den Prozentsatz der richtigen Antworten allmählich zu erhöhen
- Regelmäßige Veröffentlichung von bewährten Verfahren im Bereich der Cybersicherheit und der Cyberhygiene, die sich gezielt an Mitarbeiter und Organisationen richten

Ziel: Stärkung des Vertrauens in den digitalen Binnenmarkt und in digitale Innovationen durch die Verbesserung der allgemeinen Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit[47] von IKT-Produkten und -Diensten:

- Anzahl der Systeme, die den EU-Rahmen befolgen
- Geringere Kosten für den Erhalt eines IKT-Sicherheitszertifikats
- Anzahl der auf die IKT-Zertifizierung spezialisierten Konformitätsbewertungsstellen in allen Mitgliedstaaten
- Einsetzung der Europäischen Gruppe für die Cybersicherheitszertifizierung und regelmäßige Veranstaltung von Sitzungen
- Leitlinien für die Zertifizierung nach dem bestehenden EU-Rahmen
- Regelmäßige Veröffentlichung von Analysen der wichtigsten Trends auf dem Cybersicherheitsmarkt der EU
- Anzahl der nach den Regeln des europäischen IKT-Sicherheitszertifizierungsrahmens zertifizierten IKT-Produkte und -Dienste
- Größere Anzahl von Endnutzern, die die Sicherheitsmerkmale von IKT-Produkten und -Diensten kennen

(b)

[47] Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit bedeutet, dass den Nutzern ausreichende Informationen über die Cybersicherheitseigenschaften bereitgestellt werden, um das Sicherheitsniveau eines bestimmten IKT-Produkts, eines bestimmten IKT-Dienstes oder eines bestimmten IKT-Verfahrens objektiv feststellen zu können.

1.4.5. Kurz- oder langfristig zu deckender Bedarf

Mit Blick auf die regulatorischen Anforderungen und die sich schnell entwickelnde Cybersicherheitsbedrohungslage muss das Mandat der ENISA dahingehend überarbeitet werden, dass neue Aufgaben und Funktionen festgelegt werden, um die Mitgliedstaaten, die EU-Organe und andere Interessenträger wirksam und effizient in ihren Bemühungen um einen sicheren Cyberraum in der Europäischen Union zu unterstützen. Der vorgeschlagene Geltungsbereich des Mandats ist genau abgegrenzt, wobei die Bereiche gestärkt werden, in denen die Agentur einen eindeutigen Mehrwert unter Beweis gestellt hat, und neue Bereiche hinzugefügt werden, in denen Unterstützung im Hinblick auf die neuen politischen Prioritäten und Instrumente benötigt wird, insbesondere im Hinblick auf die NIS-Richtlinie, die Überprüfung der EU-Cybersicherheitsstrategie, den EU-Konzeptentwurf für Cybersicherheit für die Zusammenarbeit bei Cyberkrisen und die IKT-Sicherheitszertifizierung. Durch das vorgeschlagene neue Mandat soll die Agentur eine stärkere Rolle spielen und mehr im Mittelpunkt stehen, insbesondere indem sie auch den Mitgliedstaaten aktiver bei der Bekämpfung besonderer Gefahren hilft (operative Kapazität) und indem sie zu einem Kompetenzzentrum wird, das die Mitgliedstaaten und die Kommission bei der Cybersicherheitszertifizierung unterstützt.

Gleichzeitig werden mit dem Vorschlag ein europäischer Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten sowie die wesentlichen Funktionen und Aufgaben der ENISA im Bereich der Cybersicherheitszertifizierung festgelegt. Der Rahmen enthält gemeinsame Vorschriften und Verfahren, die die Einführung EU-weiter Cybersicherheitszertifizierungssysteme für bestimmte IKT-Produkte/-Dienste oder Cybersicherheitsrisiken ermöglichen. Auf der Grundlage der in diesem Rahmen geschaffenen europäischen Systeme für die Cybersicherheitszertifizierung können in allen Mitgliedstaaten gültige und anerkannte Zertifikate ausgestellt und die gegenwärtige Marktfragmentierung abgebaut werden.

1.4.6. Mehrwert aufgrund des Tätigwerdens der Union

Die Cybersicherheit ist ein wirklich globales Thema, das seinem Wesen nach grenzüberschreitend ist und wegen der wechselseitigen Abhängigkeiten zwischen Netzen und Informationssystemen immer mehr zu einem sektorübergreifenden Thema wird. Die Anzahl, Komplexität und Größenordnung von Cybersicherheitsvorfällen und ihre Auswirkungen auf Wirtschaft und Gesellschaft nehmen im Laufe der Zeit zu und dürften parallel zu technologischen Entwicklungen wie der Verbreitung des „Internets der Dinge“ weiter steigen. Dies bedeutet, dass die Notwendigkeit verstärkter gemeinsamer Anstrengungen der Mitgliedstaaten, der EU-Organe und der privaten Interessenträger bei der Bewältigung der Cybersicherheitsbedrohungen in Zukunft voraussichtlich nicht geringer werden wird.

Seit ihrer Gründung im Jahr 2004 hat die ENISA das Ziel verfolgt, die Zusammenarbeit zwischen den Mitgliedstaaten und den NIS-Akteuren zu fördern, auch indem sie die Zusammenarbeit zwischen öffentlichem und privatem Sektor unterstützt hat. Diese Unterstützung der Zusammenarbeit umfasste die fachliche Arbeit, die geleistet wurde, um ein EU-weites Bild der Bedrohungslandschaft zu vermitteln, die Einsetzung von Sachverständigengruppen und die Veranstaltung von europaweiten Übungen zu Cybersicherheitsvorfällen und zum Krisenmanagement für den öffentlichen und den privaten Sektor (insbesondere „CyberEurope“). Durch die NIS-Richtlinie wurde die ENISA mit zusätzlichen Aufgaben betraut, u. a. mit der Wahrnehmung der Sekretariatsgeschäfte des CSIRTs-Netzes für die operative Zusammenarbeit der

Mitgliedstaaten.

Der Mehrwert des Tätigwerdens auf EU-Ebene, insbesondere zur Stärkung der Zusammenarbeit zwischen den Mitgliedstaaten, aber auch zwischen NIS-Fachkreisen, wurde in den Schlussfolgerungen des Rates[48] von 2016 anerkannt und geht auch eindeutig aus der Bewertung der ENISA im Jahr 2017 hervor, die gezeigt hat, dass der Mehrwert der Agentur in erster Linie in ihrer Fähigkeit besteht, die Zusammenarbeit zwischen diesen Interessenträgern zu stärken. Auf EU-Ebene gibt es keinen anderen Akteur, der die Zusammenarbeit ebenso unterschiedlicher Interessenträger im Bereich der NIS unterstützt.

Der Mehrwert der ENISA, der sich aus der Zusammenführung der Cybersicherheitskreise und der einschlägigen Interessenträger ergibt, ist auch im Bereich der Zertifizierung gegeben. Die Zunahme der Cyberkriminalität und der Bedrohungen der Sicherheit haben nationale Initiativen entstehen lassen, in deren Rahmen hohe Cybersicherheits- und Zertifizierungsanforderungen an die in herkömmlicher Infrastruktur verwendeten IKT-Komponenten festgelegt wurden. Diese Initiativen sind zwar wichtig, sie sind jedoch mit der Gefahr verbunden, dass der Binnenmarkt fragmentiert wird und Hindernisse für die Interoperabilität entstehen. Ein IKT-Anbieter muss unter Umständen mehrere Zertifizierungsverfahren durchlaufen, um seine Produkte in mehreren Mitgliedstaaten verkaufen zu können. Die Wirkungslosigkeit/Ineffizienz der derzeitigen Zertifizierungssysteme wird ohne ein Tätigwerden der EU wahrscheinlich nicht gelöst werden. Ohne Maßnahmen dürfte die Fragmentierung des Marktes durch das Aufkommen neuer Zertifizierungssysteme kurz- bis mittelfristig (in den nächsten 5 bis 10 Jahren) sehr wahrscheinlich zunehmen. Der Mangel an Koordinierung und Interoperabilität zwischen solchen Systemen ist ein Faktor, der das Potenzial des digitalen Binnenmarkts schmälert. Dies ist ein Beleg für den Mehrwert der Festlegung eines europäischen Rahmens für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten, durch den die richtigen Voraussetzungen geschaffen werden, um das mit dem Nebeneinanderbestehen mehrerer Zertifizierungsverfahren in verschiedenen Mitgliedstaaten verbundene Problem wirksam zu bewältigen, die Zertifizierungskosten zu senken und dadurch die Zertifizierung in der EU aus kommerzieller und wettbewerblicher Sicht insgesamt attraktiver zu machen.

1.4.7. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Im Einklang mit der Rechtsgrundlage der ENISA hat die Kommission eine Bewertung der Agentur vorgenommen, zu der eine unabhängige Studie sowie eine öffentliche Konsultation gehörten. Die Bewertung kam zu dem Schluss, dass die ENISA-Ziele nach wie vor relevant sind. Vor dem Hintergrund der technologischen Entwicklungen und der sich ändernden Bedrohungen sowie der Notwendigkeit einer verbesserten Netz- und Informationssicherheit (NIS) in der EU wird technisches Fachwissen über die Entwicklung von Fragen der Netz- und Informationssicherheit benötigt. In den Mitgliedstaaten müssen Kapazitäten aufgebaut werden, um Bedrohungen verstehen und abwehren zu können, und die Interessenträger müssen über alle Themenbereiche und Einrichtungen hinweg zusammenarbeiten.

Die Agentur hat erfolgreich zu einer verstärkten Netz- und Informationssicherheit in Europa beigetragen, indem sie den Kapazitätsaufbau in 28 Mitgliedstaaten angeboten, die

[48] Schlussfolgerungen des Rates zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche vom 15. November 2016.

Zusammenarbeit zwischen Mitgliedstaaten und Interessenträgern der Netz- und Informationssicherheit verbessert, Fachwissen bereitgestellt, Fachkreise aufgebaut und die Politik unterstützt hat.

Zwar ist es der ENISA auf dem weiten Feld der NIS zumindest bis zu einem gewissen Grad gelungen, Wirkung zu erzielen, doch hat sie es nicht vermocht, einen starken Markennamen zu entwickeln und als *das* Kompetenzzentrum in Europa anerkannt zu werden. Erklären lässt sich dies durch das weit gefasste Mandat der ENISA, dem keine entsprechend großen Ressourcen gegenüberstanden. Zudem ist die ENISA die einzige EU-Agentur mit einem befristeten Mandat, wodurch sie in der Entwicklung langfristiger Zielvorstellungen und in der nachhaltigen Unterstützung ihrer Interessenträger eingeschränkt wird. Dies steht auch im Widerspruch zu den Bestimmungen der NIS-Richtlinie, durch die die ENISA mit unbefristeten Aufgaben betraut wird.

Für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten gibt es derzeit keinen europäischen Rahmen. Die Zunahme der Cyberkriminalität und der Bedrohungen der Sicherheit haben jedoch nationale Initiativen entstehen lassen, die die Gefahr einer Fragmentierung des Binnenmarkts mit sich bringen.

1.4.8. Vereinbarkeit mit anderen Finanzierungsinstrumenten sowie mögliche Synergieeffekte

Die Initiative stimmt in hohem Maße mit den vorhandenen Strategien überein, insbesondere im Bereich des Binnenmarktes. Sie wurde entsprechend dem allgemeinen Konzept für die Cybersicherheit, das bei der Überprüfung der Strategie für einen digitalen Binnenmarkt festgelegt wurde, ausgearbeitet und soll ein umfassendes Bündel von Maßnahmen ergänzen, etwa die Überprüfung der EU-Cybersicherheitsstrategie, den Konzeptentwurf für die Zusammenarbeit bei Cyberkrisen und Initiativen zur Bekämpfung der Cyberkriminalität. Sie würde für eine Angleichung an die Bestimmungen der bestehenden EU-Rechtsvorschriften, insbesondere der NIS-Richtlinie, sorgen und auf ihnen aufbauen, um die Abwehrfähigkeit gegenüber Cyberangriffen in der EU durch bessere Fähigkeiten, Zusammenarbeit, Risikomanagement, Zusammenarbeit und Sensibilisierung für Cybersicherheit weiterzuentwickeln.

Die vorgeschlagenen Zertifizierungsmaßnahmen sollten auf die potenzielle Fragmentierung abstellen, die durch bestehende und neu entstehende nationale Zertifizierungssysteme verursacht wird, und somit einen Beitrag zur Entwicklung des digitalen Binnenmarktes leisten. Ferner unterstützt und ergänzt die Initiative die Umsetzung der NIS-Richtlinie, indem sie Unternehmen, die der Richtlinie unterliegen, ein Werkzeug an die Hand gibt, um die Einhaltung der NIS-Anforderungen in der gesamten Europäischen Union nachzuweisen.

Der Vorschlag für einen europäischen Rahmen für die IKT-Cybersicherheitszertifizierung berührt nicht die Datenschutz-Grundverordnung[49] und insbesondere die einschlägigen Bestimmungen über die Zertifizierung[50], da diese für die Sicherheit der Verarbeitung personenbezogener Daten gelten. Und nicht zuletzt sollten sich die im künftigen europäischen Rahmen vorgeschlagenen Systeme so weit wie möglich auf internationale

[49] Verordnung (EU) 2016/679 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).

[50] Zum Beispiel die Artikel 42 (Zertifizierung) und 43 (bescheinigende Stellen) sowie die Artikel 57, 58 und 70 in Bezug auf die Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden und die Aufgaben des Europäischen Datenschutzausschusses.

Normen stützen, um Handelshemmnisse zu vermeiden und die Kohärenz mit internationalen Initiativen sicherzustellen.

1.5. Laufzeit der Maßnahme und Dauer ihrer finanziellen Auswirkungen

☐ Vorschlag/Initiative mit **befristeter Laufzeit**

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

– ☐ Finanzielle Auswirkungen: JJJJ bis JJJJ

☒ Vorschlag/Initiative mit **unbefristeter Laufzeit**

– Umsetzung mit einer Anlaufphase von 2019 bis 2020,

– anschließend reguläre Umsetzung.

1.6. Vorgeschlagene Methode(n) der Mittelverwaltung[51]

☒ **Direkte Verwaltung** durch die Kommission (Titel III – Zertifizierung)

– ☐ Exekutivagenturen

☐ **Geteilte Verwaltung** mit Mitgliedstaaten

☒ **Indirekte Verwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

☐ internationale Einrichtungen und deren Agenturen (bitte angeben);

☐ die EIB und den Europäischen Investitionsfonds;

☒ Einrichtungen im Sinne der Artikel 208 und 209 der Haushaltsordnung (Titel II – ENISA)

☐ öffentlich-rechtliche Körperschaften;

☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern sie ausreichende Finanzsicherheiten bieten;

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

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

Bemerkungen

Die Verordnung deckt Folgendes ab:

- In Titel II der vorgeschlagenen Verordnung wird das Mandat der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) neu gefasst und ihr eine wichtige Rolle bei der Zertifizierung zugewiesen, während

- in Titel III ein Rahmen für die Schaffung europäischer Systeme für die Zertifizierung der Cybersicherheit von IKT-Produkten und -Diensten festgelegt wird, in dem die ENISA eine entscheidende Rolle spielt.

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

2. VERWALTUNGSMASSNAHMEN

2.1. Monitoring und Berichterstattung

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

Das Monitoring beginnt unmittelbar nach der Verabschiedung des Rechtsinstruments, und der Schwerpunkt wird auf seiner Anwendung liegen. Die Kommission wird Sitzungen mit der ENISA, Vertretern der Mitgliedstaaten (z. B. Sachverständigengruppe) und den relevanten Interessenträgern organisieren, insbesondere um die Umsetzung der Vorschriften über die Zertifizierung, etwa wie die Einsetzung des Verwaltungsrates, zu erleichtern.

Die erste Bewertung sollte fünf Jahre nach dem Inkrafttreten des Rechtsakts stattfinden, sofern ausreichende Daten zur Verfügung stehen. Eine explizite Bewertungs- und Überprüfungsklausel [Artikel XXX], wonach die Kommission eine unabhängige Bewertung durchführen wird, ist im Rechtsinstrument vorgesehen. Die Kommission wird dem Europäischen Parlament und dem Rat in der Folgezeit über die Ergebnisse ihrer Bewertung Bericht erstatten, erforderlichenfalls zusammen mit einem Vorschlag zur Überarbeitung des Rechtsakts, um die Auswirkungen der Verordnung und ihren Mehrwert zu ermitteln. Weitere Bewertungen sollten alle fünf Jahre stattfinden. Dabei wird die Bewertungsmethodik der Leitlinien der Kommission für eine bessere Rechtsetzung angewandt werden. Diese Bewertungen werden mithilfe von gezielten Sachverständigendiskussionen, Studien und umfassenden Konsultationen der Interessenträger durchgeführt werden.

Der Exekutivdirektor der ENISA sollte dem Verwaltungsrat alle zwei Jahre eine Ex-post-Bewertung der Tätigkeiten der ENISA vorlegen. Außerdem sollte die Agentur einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen nachträglicher Bewertungen erstellen und der Kommission alle zwei Jahre über die Fortschritte berichten. Der Verwaltungsrat sollte dafür zuständig sein, die angemessene Weiterbehandlung der Schlussfolgerungen zu verfolgen.

Behauptete Missstände bei der Tätigkeit der Agentur können vom Europäischen Bürgerbeauftragten nach Artikel 228 des Vertrags über die Arbeitsweise der Europäischen Union untersucht werden.

Die Daten für das geplante Monitoring würden überwiegend von der ENISA, der Europäischen Gruppe für die Cybersicherheitszertifizierung, der Kooperationsgruppe, dem CSIRTs-Netz und den Behörden der Mitgliedstaaten stammen. Neben den Daten aus den Berichten (einschließlich der jährlichen Tätigkeitsberichte) der ENISA, der Europäischen Gruppe für die Cybersicherheitszertifizierung, der Kooperationsgruppe und des CSIRTs-Netzes werden im Bedarfsfall spezielle Datenerfassungsinstrumente verwendet werden (z. B. Umfragen bei nationalen Behörden, Eurobarometer und Berichte von der Kampagne „Monat der Cybersicherheit“ und europaweite Übungen).

2.2. Verwaltungs- und Kontrollsystem

2.2.1. Ermittelte Risiken

Die ermittelten Risiken sind gering. Es gibt bereits eine Agentur der Union, und ihr Mandat wird genau abgegrenzt sein, wobei die Bereiche gestärkt werden, in denen die Agentur einen

eindeutigen Mehrwert unter Beweis gestellt hat, und neue Bereiche hinzugefügt werden, in denen Unterstützung im Hinblick auf die neuen politischen Prioritäten und Instrumente benötigt wird, insbesondere im Hinblick auf die NIS-Richtlinie, die Überprüfung der EU-Cybersicherheitsstrategie, den angekündigten EU-Konzeptentwurf für Cybersicherheit für die Zusammenarbeit bei Cyberkrisen und die IKT-Sicherheitszertifizierung.

Der Vorschlag präzisiert daher die Aufgaben der Agentur und führt zu Effizienzgewinnen. Die vermehrten operativen Zuständigkeiten und Aufgaben stellen kein echtes Risiko dar, da sie die Maßnahmen der Mitgliedstaaten ergänzen und sie auf ihr Ersuchen hin sowie hinsichtlich begrenzter und vorab festgelegter Dienste unterstützen würden.

Ferner wird durch das gemäß dem Gemeinsamen Konzept vorgeschlagene Modell der Agentur eine ausreichende Kontrolle sichergestellt, die gewährleistet, dass die ENISA auf ihre Ziele hinarbeitet. Die operativen und finanziellen Risiken der vorgeschlagenen Änderungen dürften begrenzt sein.

Gleichzeitig muss für angemessene finanzielle Ressourcen gesorgt werden, damit die ENISA die ihr durch das neue Mandat übertragenen Aufgaben erfüllen kann, auch im Bereich der Zertifizierung.

2.2.2. Beabsichtigte Kontrollmethode(n)

Die Rechnungsführung der Agentur wird dem Rechnungshof zur Genehmigung vorgelegt und ist Gegenstand des Entlastungsverfahrens. Rechnungsprüfungen sind vorgesehen.

Zudem unterliegt die Tätigkeit der Agentur der Aufsicht des Bürgerbeauftragten gemäß Artikel 228 AEUV.

Siehe auch Abschnitte 2.1 und 2.2.1.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen vorhanden oder vorgesehen sind.

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

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

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

- Die Agentur tritt innerhalb von sechs Monaten ab dem Tag des Inkrafttretens dieser Verordnung der Interinstitutionellen Vereinbarung vom 11 September 2013 zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Kommission der Europäischen Gemeinschaften über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei und erlässt unverzüglich die entsprechenden Bestimmungen

nach dem Muster in der Anlage zu der Vereinbarung, die für sämtliche Mitarbeiter der Agentur gelten.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n)

- Bestehende Haushaltslinien

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

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
		GM/ NGM [52]	von EFTA-Ländern [53]	von Kandidatenländern [54]	von Drittländern	nach Artikel 21 Absatz 2 Buchstabe b der Haushaltsordnung
1a Wettbewerbsfähigkeit im Dienste von Wachstum und Beschäftigung	09 02 03 ENISA sowie Zertifizierung der Sicherheit von Informations- und Kommunikationstechnik	GM	JA	NEIN	NEIN	NEIN
5 Verwaltungsausgaben	09 01 01 Ausgaben für Beamte und Bedienstete auf Zeit im Politikbereich „Kommunikationsnetze, Inhalte und Technologien“ 09 01 02 Ausgaben für Beamte und Bedienstete auf Zeit im Politikbereich	NGM	NEIN	NEIN	NEIN	NEIN

[52] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.
[53] EFTA: Europäische Freihandelsassoziation.
[54] Kandidatenländer und gegebenenfalls potenzielle Kandidatenländer des Westbalkans.

	„Kommunikationsnetze, Inhalte und Technologien“ 09 01 02 11 Sonstige Verwaltungsausgaben					

3.2. Geschätzte Auswirkungen auf die Ausgaben

3.2.1. Übersicht

in Mio. EUR (3 Dezimalstellen)

Rubrik des mehrjährigen Finanzrahmens	1a	Wettbewerbsfähigkeit im Dienste von Wachstum und Beschäftigung

ENISA			**Ausgangsbasis** **2017 (31.12.2016)**	**2019** ***(ab 1.7.2019)***	**2020**	**2021**	**2022**	**INSGESAMT**
Titel 1: Personalausgaben *(einschließlich Ausgaben für die Einstellung von Personal, Schulungen, soziomedizinische Infrastruktur und externe Dienste)*	Verpflichtungen	(1)	6,387	9,899	12,082	13,349	13,894	**49,224**
	Zahlungen	(2)	6,387	9,899	12,082	13,349	13,894	**49.,224**
Titel 2: Infrastruktur- und Betriebsausgaben	Verpflichtungen	(1a)	1,770	1,957	2,232	2,461	2,565	**9,215**
	Zahlungen	(2 a)	1,770	1,957	2,232	2,461	2,565	**9,215**
Titel 3: Operative Ausgaben	Verpflichtungen	(3 a)	3,086	4,694	6,332	6,438	6,564	**24,028**
	Zahlungen	(3b)	3,086	4,694	6,332	6,438	6,564	**24,028**
Mittel INSGESAMT für die ENISA	Verpflichtungen	=1+1 a +3a	**11,244**	16,550	20,646	22,248	23,023	**82,467**
	Zahlungen	=2+2 a	**11,244**	**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

		+3b							

Rubrik des mehrjährigen Finanzrahmens	**5**	Verwaltungsausgaben

in Mio. EUR (3 Dezimalstellen)

		2019 *(ab 1.7.2019)*	**2020**	**2021**	**2022**	**INSGESAMT**
GD: CNECT						
• Personalausgaben		0,216	0,846	0,846	0,846	**2,754**
• Sonstige Verwaltungsausgaben		0,102	0,235	0,238	0,242	**0,817**
GD CNECT **INSGESAMT**	Mittel	0,318	1,081	1,084	1,088	**3,571**

Die Personalkosten wurden ausgehend von dem geplanten Einstellungsdatum berechnet (die Beschäftigung soll ab dem 1.7.2019 beginnen).

Die Angaben für die Personalausgaben für den Zeitraum nach 2020 sind vorläufige Angaben und berühren nicht die Vorschläge der Kommission für den mehrjährigen Finanzrahmen nach 2020.

Mittel INSGESAMT unter der RUBRIK 5 des mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	0,318	1,081	1,084	1,088	**3,571**

in Mio. EUR (3 Dezimalstellen)

		2019	2020	2021	2022	INSGESAMT
Mittel INSGESAMT unter den RUBRIKEN 1 bis 5 des mehrjährigen Finanzrahmens	Verpflichtungen	16,868	21,727	23,332	24,11	**86,038**
	Zahlungen	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Geschätzte Auswirkungen auf die Mittel der Agentur

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

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

Mittel für Verpflichtungen in Mio. EUR (3 Dezimalstellen)

Ziele und Ergebnisse angeben[55] ⇩	**2019**	**2020**	**2021**	**2022**	**INSGESAMT**
Ausbau der Kapazitäten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen	1,408	1,900	1,931	1,969	7,208
Verbesserung der Zusammenarbeit und der Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU	0,939	1,266	1,288	1,313	4,806
Ausbau der Kapazitäten auf EU-Ebene, um die Maßnahmen der Mitgliedstaaten zu ergänzen, insbesondere im Fall von grenzüberschreitenden Cyberkrisen	0,704	0,950	0,965	0,985	3,604
Sensibilisierung der Bürger und Unternehmen für Fragen der Cybersicherheit	0,704	0,950	0,965	0,985	3,604
Stärkung des Vertrauens in den digitalen Binnenmarkt und in digitale Innovationen durch die Verbesserung der allgemeinen Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit von IKT-Produkten und -Diensten	0,939	1,266	1,288	1,313	4,806
GESAMTKOSTEN	4,694	6,332	6,437	6,565	24,028

[55] Diese Tabelle enthält nur die operativen Ausgaben gemäß Titel 3.

3.2.3. Geschätzte Auswirkungen auf die Humanressourcen der Agentur

3.2.3.1. Übersicht

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

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

in Mio. EUR (3 Dezimalstellen)

	Q3/4 2019	**2020**	**2021**	**2022**
Auf Zeit beschäftigte Bedienstete (Besoldungsgruppe AD)	4,242	5,695	6,381	6,709
Auf Zeit beschäftigte Bedienstete (Besoldungsgruppe AST)	1,601	1,998	2,217	2,217
Vertragsbedienstete	2,041	2,041	2,041	2,041
Abgeordnete nationale Sachverständige	0,306	0,447	0,656	0,796
INSGESAMT	**8,190**	**10,181**	**11,295**	**11,763**

Die Personalkosten wurden ausgehend von dem geplanten Einstellungsdatum berechnet (für die derzeitigen ENISA-Mitarbeiter wurde eine vollständige Beschäftigung ab dem 1.1.2019 angenommen). Für die neuen Mitarbeiter wurde von einer schrittweisen Besetzung der Planstellen ab dem 1.7.2019 und von einer vollständigen Besetzung der Planstellen im Jahr 2022 ausgegangen. Die Angaben für die Personalausgaben für den Zeitraum nach 2020 sind vorläufige Angaben und berühren nicht die Vorschläge der Kommission für den mehrjährigen Finanzrahmen nach 2020.

Geschätzte personelle Auswirkungen (zusätzliche VZÄ) – Stellenplan

Funktions- und Besoldungsgruppen	2017 **Derzeitige ENISA**	Q3/Q4 2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	

AD5					
AD Insgesamt	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
AST Insgesamt	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
AST/SC Insgesamt					
GESAMT	48	12	10	7	3

Aufgaben des zusätzlichen AD-/AST-Personals für die Verwirklichung der in Abschnitt 1.4.2 beschriebenen Ziele des Instruments:

Aufgaben	AD	AST	ANS	Insgesamt
Politikgestaltung und Kapazitätsaufbau	8	1		9
Operative Zusammenarbeit	8	1	7	16
Zertifizierung (marktbezogene Aufgaben)	9	3	2	14
Wissen, Information und Sensibilisierung	1	1		2
INSGESAMT	26	6	9	41

Beschreibung der auszuführenden Aufgaben:

Aufgaben	**Zusätzliche Ressourcen benötigt**
Entwicklung und Umsetzung der EU-Politik und Aufbau von Kapazitäten	Zu den Aufgaben würde Folgendes gehören: Unterstützung der Kooperationsgruppe, Unterstützung der kohärenten grenzüberschreitenden NIS-Umsetzung, regelmäßige Berichterstattung über den Stand der Umsetzung des EU-Rechtsrahmens; Beratung und Koordinierung sektoraler Initiativen im Bereich der Cybersicherheit, einschließlich der Sektoren

	Energie, Verkehr (z. B. Luftverkehr/Straßenverkehr/Seeverkehr/vernetzte Fahrzeuge), Gesundheit und Finanzen sowie Unterstützung des Aufbaus von Informationsaustausch- und -analysezentren (ISAC) in verschiedenen Sektoren.
Operative Zusammenarbeit und Krisenmanagement	**Die Aufgaben würden Folgendes einschließen:** Führung der Sekretariatsgeschäfte des CSIRTs-Netzes, indem u. a. sichergestellt wird, dass die IT-Infrastruktur und die Kommunikationskanäle des CSIRTs-Netzes gut funktionieren. Gewährleistung einer strukturierten Zusammenarbeit mit dem CERT-EU, dem EC3 und anderen maßgeblichen EU-Einrichtungen. Veranstaltung von **CyberEurope-Übungen**[56] – Aufgaben im Zusammenhang damit, dass die Übung nicht mehr alle zwei Jahre, sondern jährlich stattfinden soll, und Aufgaben, durch die sichergestellt wird, dass bei den Übungen Sicherheitsvorfälle von Anfang bis Ende behandelt werden. **Technische Unterstützung** - Zu den Aufgaben würde die strukturierte Zusammenarbeit mit dem CERT-EU gehören, um technische Hilfe im Falle erheblicher Sicherheitsvorfälle bereitzustellen und die Analyse von Sicherheitsvorfällen zu unterstützen. Dies würde die Unterstützung der Mitgliedstaaten bei der Bewältigung von Sicherheitsvorfällen und bei der Analyse von Anfälligkeiten, Artefakten und Sicherheitsvorfällen beinhalten. Ebenso eingeschlossen wäre die Erleichterung der Zusammenarbeit zwischen den einzelnen Mitgliedstaaten bei der Krisenreaktion durch die Analyse und Aggregierung der nationalen Lageberichte auf der Grundlage der Informationen, die der Agentur von den Mitgliedstaaten und anderen Einrichtungen zur Verfügung gestellt werden. **Konzeptentwurf zur koordinierten Reaktion auf grenzüberschreitende**

[56] CyberEurope ist die bislang größte und umfassendste EU-Übung zur Cybersicherheit, an der mehr als 700 Cybersicherheitsexperten aus allen 28 EU-Mitgliedstaaten beteiligt waren. Sie findet alle zwei Jahre statt. Die Bewertung der ENISA und der EU-Cybersicherheitsstrategie aus dem Jahr 2013 deuten darauf hin, dass viele Interessenträger es befürworten, CyberEurope angesichts der sich schnell entwickelnden Cyberbedrohungen jährlich zu veranstalten. Dies ist jedoch derzeit in Anbetracht der begrenzten Ressourcen der Agentur nicht möglich.

	Cybersicherheitsvorfälle großen Ausmaßes – die Agentur wird zur Entwicklung einer auf Kooperation beruhenden Reaktion der Union und der Mitgliedstaaten auf massive grenzüberschreitende Cybersicherheitsvorfälle oder -krisen beitragen durch eine Reihe von Aufgaben, die vom Beitrag zu einer Lageeinschätzung auf Unionsebene bis zur Erprobung der Notfallpläne für Sicherheitsvorfälle reichen. **Nachträgliche technische Untersuchungen von Sicherheitsvorfällen** – Durchführung von oder Beitrag zu nachträglichen Untersuchungen von Sicherheitsvorfällen in Zusammenarbeit mit den CSIRTs-Netz mit dem Ziel, Empfehlungen abzugeben und die Fähigkeiten durch öffentliche Berichte zur besseren Vermeidung künftiger Sicherheitsvorfälle zu stärken.
Marktbezogene Aufgaben (Normung, Zertifizierung)	Die Aufgaben würden die aktive Unterstützung der innerhalb des Zertifizierungsrahmens vorgenommenen Arbeiten umfassen, einschließlich der Bereitstellung von Fachwissen zur Entwicklung möglicher europäischer Systeme für die Cybersicherheitszertifizierung. Die Aufgaben werden auch die Unterstützung der Entwicklung und der Umsetzung der Unionspolitik im Bereich der Normung, Zertifizierung und Marktüberwachung beinhalten - dies wird die Erleichterung der Einführung von Normen für das Risikomanagement bei elektronischen Produkten, Systemen, Netzen und Diensten und die Beratung von Betreibern wesentlicher Dienste und von Anbietern digitaler Dienste in Bezug auf die Anforderungen an die technische Sicherheit voraussetzen. Zu den Aufgaben wird außerdem die Bereitstellung von Analysen der wichtigsten Trends auf dem Cybersicherheitsmarkt gehören.
Wissen und Information, Sensibilisierung	Im Vorschlag wird der Agentur eine neue Aufgabe zugewiesen, die darin besteht, das „Informationsdrehkreuz“ der Union aufzubauen und zu pflegen, um einen leichteren Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und möglichen Abhilfemaßnahmen sicherzustellen. Zu den Aufgaben würde auch gehören, dass die von den Organen, Einrichtungen und sonstigen Stellen der Union bereitgestellten Informationen zur

	Sicherheit von Netz- und Informationssystemen, insbesondere zur Cybersicherheit, zusammengeführt, geordnet und der Öffentlichkeit über ein spezielles Portal zur Verfügung gestellt werden. Die Aufgaben würden ferner die Unterstützung der ENISA-Aktivitäten im Bereich der Sensibilisierung umfassen, damit die Agentur die Möglichkeit hat, die Anstrengungen zu intensivieren.

3.2.3.2. Geschätzter Personalbedarf bei der übergeordneten GD

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

– ☒ Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

Schätzung in ganzzahligen Werten (oder mit höchstens einer Dezimalstelle)

		Zusätzlicher Personalbedarf			
	Basisjahr 2017	Q3/4 2019	2020	2021	2020
• **Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)**					
09 01 01 01 (am Sitz und in den Vertretungen der Kommission)	1	2	3		
• **Externes Personal (in Vollzeitäquivalenten: VZÄ)**[57]					
09 01 02 01 (VB, ANS und LAK der Globaldotation)	1	2			
INSGESAMT		**4**	**3**		

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	Vertretung der Kommission im Verwaltungsrat der Agentur. Ausarbeitung einer Stellungnahme der Kommission zum einheitlichen Programmplanungsdokument der ENISA und Überwachung dessen Umsetzung. Überwachung der Erstellung des Haushaltsplans der Agentur und dessen Ausführung. Unterstützung der Agentur bei der Entwicklung ihrer Tätigkeiten gemäß den Strategien der Union, u. a. durch Teilnahme an relevanten Sitzungen. Überwachung der Umsetzung des Rahmens für europäische Systeme für die Zertifizierung der Cybersicherheit von IKT-Produkten und -Diensten. Pflege von Kontakten mit den Mitgliedstaaten und anderen maßgeblichen Interessenträgern hinsichtlich der Zertifizierungsbemühungen. Zusammenarbeit mit der ENISA bezüglich der möglichen Systeme. Ausarbeitung möglicher europäischer Cybersicherheitssysteme.
Externes	Siehe oben.

[57] VB = Vertragsbedienstete, ÖB = Örtliche Bedienstete, ANS = Abgeordnete nationale Sachverständige, LAK = Leiharbeitskräfte, JSD = junge Sachverständige in Delegationen.

Personal	

3.2.4. Vereinbarkeit mit dem mehrjährigen Finanzrahmen

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

– ☒ Der Vorschlag/Die Initiative erfordert eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens.

Der Vorschlag erfordert eine Anpassung der Rubrik 09 02 03 wegen der Neufassung des Mandats der ENISA, durch die der Agentur neue Aufgaben übertragen werden, u. a. im Zusammenhang mit der Umsetzung der NIS-Richtlinie und dem europäischen Rahmen für die Cybersicherheitszertifizierung. Dabei geht es um die folgenden Beträge:

Jahr	Geplant	Beantragt
2019	10,739	16,550
2020	10,954	20,646
2021	entfällt	22,248
2022	entfällt	23,023*

* Hierbei handelt es sich um eine Schätzung. Der EU-Finanzbeitrag für die Zeit nach 2020 ist im Rahmen einer kommissionsweiten Diskussion aller Vorschläge für den Zeitraum nach 2020 zu prüfen. Dies bedeutet, dass die Kommission, sobald sie ihren Vorschlag für den nächsten mehrjährigen Finanzrahmen unterbreitet hat, unter Berücksichtigung der Schlussfolgerungen der Folgenabschätzung[58] einen geänderten Finanzbogen zu Rechtsakten vorlegen wird.

– ☐ Der Vorschlag/Die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des mehrjährigen Finanzrahmens[59].

3.2.5. Finanzierungsbeteiligung Dritter

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

– ☒ Der Vorschlag/Die Initiative sieht folgende Kofinanzierung vor:

[58] Link zu der Seite mit der Folgenabschätzung.

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

	Jahr **2019**	Jahr **2020**	Jahr **2021**	Jahr **2022**
EFTA	p.m.[60]	p.m.	p.m.	p.m.

3.3. Geschätzte Auswirkungen auf die Einnahmen

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

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

  – ☐ auf die Eigenmittel

  – ☐ auf die sonstigen Einnahmen

[60] Der genaue Betrag für die Folgejahre kann erst vorliegen, wenn der EFTA-Proportionalitätsfaktor für das betreffende Jahr festgesetzt wurde.